<u>governmgnhbhgjnjj</u>

CONTENTS

ABSTRACT

The word steganography literally means covered writing as derived from Greek. Steganography is the art of concealing the existence of information within seemingly innocuous carriers. In broad sense, term Steganography is used for hiding messagewithin an image.

The art and science of hiding information by embedding messages within other, seemingly harmless messages. Steganography works by replacing bits of useless or unused in regular computer (such as graphics, sound, text, or even floppydisks) with bits of different, invisible information. This hidden information can be plain text, cipher text or even images.

**Steganography (literally meaning covered writing) dates back to ancient Greece, where
common practices consisted of etching messages in wooden tablets and covering them
with wax, and tattooing a shaved messenger's head, letting his hair grow back, then
shaving it again when he arrived at his contact point.**

INDRODUCTION

Steganography is the art and science of communicating in a way which hides the existence of the communication. In contrast to cryptography, where the "enemy" is allowed to detect, intercept and modify messages without being able to violate certain security premises guaranteed by a cryptosystem, the goal of steganography is to hide messages inside other "harmless" messages in a way that does not allow any "enemy" to even detect that there is a second secret message present. Steganography is in the (especially military) literature also referred to as transmission security or short TRANSEC.

This basic design principle of steganographic systems, i.e. replacing high entropy noise with a high entropy secret transmission, is quite obvious. There have a number of simple software tools been published for e.g. hiding files in the least significant bits of digital

Steganography vs cryptography

Steganography can be viewed as akin to cryptography. Both have been used throughoutrecorded history as means to protect information. At times these two technologies seem to converge while the objectives of the two differ.Cryptographic techniques "scramble"messages so if intercepted, the messages cannot be understood.Steganography, anessence, "camouflages" a message to hide its existence and make it seem "invisible" thusconcealing the fact that a message is being sent altogether. An encrypted message may draw suspicion while an invisible message will not.
In an ideal world we would all be able to openly send encrypted email or files to each other with no fear of reprisals. However there are often cases when this is not possible,either because you are working for a company that does not allow encrypted email or perhaps the local government does not approve of encrypted communication (a reality in some parts of the world). This is where steganography can come into play.

A good steganography system should fulfill the same requirements posed by the"Kerckhoff principle" in cryptography. This means that the security of the system has to
be based on the assumption that the "enemy" has full knowledge of the design and implementation details of the steganographic system. The only missing information for the "enemy" is a short easily exchangeable random number sequence, the secret key, and without the secret key, the "enemy" should not have the slightest chance of even becoming suspicious that on an observed communication channel hidden communication might take place.
Steganography cannot be detected. Therefore, it is used when encryption is not permitted.

Or, more commonly, steganography is used to supplement encryption. An encrypted file may still hide information using steganography, so even if the encrypted file is deciphered, the hidden message is not seen.

EVOLUTION OF STEGANOGRAPHY

CODE BREAKERS : David Kahn's The Code breakers and Bruce Norman’s Secret Warfare: The Battle of Codes and Ciphers recounts numerous tales of steganography .
INVISIBLE INK : An innocent letter may contain a very different message written between the lines with invisible ink. Common sources for invisible inks are milk, vinegar, fruit juices and urine. All of these darken when heated. Later on, more sophisticated inks were developed which react to various chemicals.
MICRODOTS: The Germans developed microdot technology. Microdots are photographs the size of a printed period having the clarity of standard-sized typewritten pages. The first microdots were discovered masquerading as a period on a typed envelope carried by a German agent in 1941.
The message was not hidden, nor encrypted. It was just so small as to not draw attention to itself (for a while).

TYPES OF STEGANOGRAPHY

1.MESSAGES IN TEXT program is called SPAM MIMIC. Secret messages can be hidden in text format by reframing the text of the carrier file, while maintaining the context. On e form of steganography is a program called Spam Mimic.
Based on a set of rules called a mimic engine by Peter Wayner, it encodes your message into what looks like your typical, quickly deleted Spam message. However, hiding a message in plain text is a thing of past, as people are suspicious of irrelevant text.

2.MESSAGES IN STILL IMAGES most popular tool is outguess.

3.MESSAGES IN AUDIO data is hidden in layer III of encoding process of MP3 file.Messages in audio are always sent along with ambient noise. The data is hidden in the heart of the layer III encoding process of MP3 file, namely the inner loop during
compression. The inner loop limits the input data and increases the step size until the data can be coded with the available number of bits. The data is compressed, encrypted and then hidden in MP3 bit stream.

4.MESSAGES IN VIDEO embedding information into multimedia data has gained
increasing attention lately. The method of encryption is the same as in audio
steganography. Video files are generally very good carrier files since they have a lot of
irrelevant bits.

AN EXAMPLE

Fishing freshwater bends and saltwater coasts rewards anyone feeling stressed.Resourceful anglers usually find masterful leapers fun and admit swordfish rankoverwhelming anyday.

“Send lawyers guns and money”

Steganography is closely related to the problem of "hidden channels" in secure operating system design, a term which refers to all communication paths that can not easily be restricted by access control mechanisms (e.g. two processes that communicate by modulating and measuring the CPU load). Steganography is also closely related to spread spectrum radio transmission, a technique that allows to receive radio signals that are over 100 times weaker than the atmospheric background noise, as well asTEMPEST,techniques which analyze RF transmissions of computer and communication equipment in order to get access to secret information handled by these systems.Most communication channels like telephone lines and radio broadcasts transmit signals which are always accompanied by some kind of noise. This noise can be replaced by a secret signal that has been transformed into a form that is indistinguishable from noise .

DISSECTING STEGANOGRAPHY

Steganography is a term used for hiding messages within an image. Any color pixel is made of a combination of red – green-blue mode(RGB) wherein each RGB component consist of 8 bits. If letters in ASCII are to be represented within the color pixels, the rightmost digit, called the least significant bit (LSB), can be altered. Any variation in the value of this bit leads to very minimal variation in color. If we have to hide the word'digit' in the image, we take the LSB of every color_and hide each bit of the word in its RGB combination. To insert the letter 'D' we modify three color pixels with three bits in each color pixel, we utilize 14 color pixels to hide the entire word with only 1 bit in the 14th pixel.

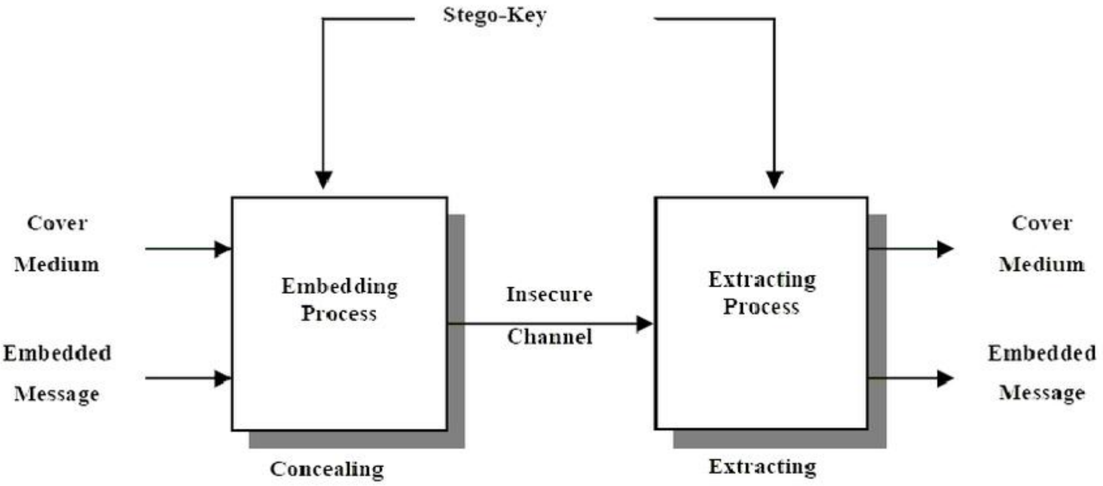

Fig. 1: The General Steganography System

AMOUNT OF DATA STORED INSIDE A PICTURE

Suppose we have a 24-bit image 1024 x 768 (this is a common resolution for satellite images, electronic astral photographs and other high resolution graphics). This may produce a file over 2 megabytes in size (1024x768x24/8 = 2,359,296 bits). All color variations are derived from three primary colors, Red, Green and Blue.Each primary color is represented by 1 byte (8 bits). 24-bit images use 3 bytes per pixel.If information is stored in the least significant bit (LSB) of each byte, 3 bits can be a

stored in each pixel. The "container" image will look identical to the human eye, even if viewing the picture side by side with the original.

STEPS FOR HIDING AN IMAGE USING STEGANOGRAPHY

1.start s-tool and window explorer using the later as drag and drop interface for the
software.
2.drag and drop the image to be used as the carrier file from the explorer onto the actions
window in s-tool.
3.drag and drop the data file on the carrier file.
4.give pass phrase and encryption algorithm when prompted. Pass these to receiver too.
5.the hidden file is ready. Receiver has to click on the “reveal” button to extract the data.
Steganography simply takes one piece of information and hides it within another.
Computer files (images, sounds recordings, even disks) contain unused or insignificant

DIGITAL WATERMARKING

Usually carrier file carry hidden data unrelated to the content in which it is embedded, but digital watermarking holds information about its carrier medium. Information such as a number or a text into a multimedia file can be added to carrier file through slight data modification. this process has gained huge acclaim from the media for enabling copyright for their products. Video steganography is more suited to avoiding piracy and is mostly used for digital watermarking.

Types of digital watermarking

ROBUST DIGITAL WATERMARKING :- A robust watermark is embedded in the file in such a way that even if the file is later transformed, the watermark will not be removed. A robust digital watermark is concealed message that identifies the source of data. It is called robust because it is designed to survive modifications of the data that result from resizing, cropping or photographing the image to capture only the part of the image that doesn't have the watermark or even from re-sampling or making an analog recording of an audio stream. Its application includes copyright protection, labeling, monitoring, tamper proofing and conditional access.

FRAGILE DIGITAL WATERMARKING is similar to fragile analog watermarks-if the data is altered or copied in exactly, the watermark is corrupted. If changes are made to the file containing a fragile watermark, the originator of the watermark will be able to detect and identify the areas where the alterations have been made and maybe even determine what the data was before modification. This scheme serves at proving the authenticity of the data.

For ensuring the integrity of data, digital signatures are preferred but fragile digital
watermarking can detect data tempering without alerting the culprit. Compatible players
refuse to play content that does not bear a valid watermark.

WHAT IS “STEGANALYSIS”?

The art of detecting, decoding and altering messages hidden via steganography is called steganalysis. It is easiest when before as well as after steganography copies of file are present. Steganalysis can make the hidden data work against the creator. Any malicious interceptor could alter as carrier file without the knowledge of sender or the intended receiver. Hence inaccurate or wrong data could be passed under identity of the original sender.

SOME OUTSTANDING FACTS

1. steganos security suite 4 uses powerful 128-bit encryption. It would take 1 billion powerful computers million of years to try every combination to gain access to your
personal information. this software uses steganography along with encryption to completely secure your data.

2. Blindside is an application of steganography that allows you to conceal a single file or set of files within a standard computer image. The new image looks identical to the original, but can contain up to 50k of data. The hidden files can also be password encrypted to prevent unauthorized access.

3. Mp3stego hides information in mp3 files during the compression process. The data is first compressed,encrypted and then hidden in the mp3 bit stream. Although mp3stego

was written with steganographic applications in mind, it can also be used as a copyright marking system for mp3 files.

APPLICATIONS

1.Like many security tools, steganography can be used for a variety of reasons, some good, some not so good.

2.Legitimate purposes can include things like watermarking images for reasons such as copyright protection. Digital watermarks (also known as fingerprinting, significant especially in copyrighting material) are similar to steganography in that they are overlaid in files, which appear to be part of the original file and are thus not easily detectable by the average person.

3. Steganography can also be used as a way to make a substitute for a one-way hash value (where you take a variable length input and create a static length output string to verify that no changes have been made to the original variable length input).

4.Steganography can be used to tag notes to online images (like post-it notes attached to paper files)

5.Steganography can be used to maintain the confidentiality of valuable information, to protect the data from possible sabotage, theft, or unauthorized viewing.

6.Steganography can also be used for illegitimate reasons.

LIMITATIONS

1.There are limitations on the use of steganography. As with encryption, if Alice wants to communicate secretly with Bob they must first agree on the methodbeing used. Demeratus, a Greek at the Persian court, sent a warning to Sparta about an imminent invasion by Xerxes by removing the wax from a writing tablet,writing the message on the wood and then covering it in wax again. The tablet appeared to be blank and fooled the customs men but almost fooled the recipient too since he was unaware that the message was being hidden

2.With encryption, Bob can be reasonably sure that he has received a secret message when a seemingly meaningless file arrives. It has either been corrupted or is encrypted. It is not so clear with hidden data, Bob simply receives an image, for example, and needs to know that there is a hidden message and how to locate it.

3.Another limitation is due to the size of the medium being used to hide the data. In order for steganography to be useful the message should be hidden without any major changes to the object it is being embedded in. This leaves limited room to embed a message without noticeably changing the original object. This is most obvious in compressed files where many of the obvious candidates for embedding data are lost. What is left is likely to be the most perceptually significant portions of the file and although hiding data is still possible it may be difficult to avoid If someone was trying to steal data, they could conceal it in another file or files and send it out in an innocent looking email or file transfer.

4.Simple spread spectrum techniques are able to survive amplitude distortion and noise addition but are vulnerable to timing errors.

Synchronization of the chip signal is required in order for the technique to work so adjusting the synchronization can cause the embedded data to be lost.

NEED OF PROPOSED SYSTEM

The previously had many drawbacks such as more manual processing of data which resulted in a time consuming process.Besides this cost of maintaining a manually was more as compared to the computerized process. Besides this there were complexities but not the least there was minimal amount of data security.

USERS

Sender

Sender who make a stegano image. Sender is an authorized person who sends important information with the help of an image to receiver

Receiver

Receiver is an authorized person who extracts important information from image in a secure way. Receiver receives information from sender

SCOPE OF STEGANOGRAPHY

Encryption

The object file which is supposed to be proceeding will be encrypted in some binary codes. This binary code depends on the nature of the object file.This encryption is different for different files. As, example the encryption is made of text file which is absolutely different from any audio file or image files.

Data Chucking

In this process the encrypted file is chunked in various parts and then this file is to Be proceed for the further streganography. The aim of this step is to reduce the stenography time and increase the effectiveness of this procedure.

Steganography

In this process the steganography is done on the chunked encrypted files. In this Process the binary codes of the encrypted files are to be changed by
any of the method as mentioned below.
Specific method changes the specific binary numbers.

ADVANTAGES OF STEGANOGRAPHY

1. It can be used for safeguarding data, such as in the field of media where copywriting ensures authenticity.

2. It can be used by intelligence agencies for sending their secret data.

3. messages do not attract attention to themselves. Plainly visible encrypted messages—no matter how unbreakable—will arouse suspicion,
and may in themselves be incriminating in countries where encryption is illegal.

4.Altered picture closely resembles original. Not susceptible to attacks such as rotation and translation.

DISADVANTAGE OF STEGANOGRAPHY

1. Many a terrorist and anti humanist activities have been carried out cloaked under this technique.

2. Message is hard to recover if image is subject to attack such as translation and rotation.

3. Significant damage to picture appearance. Message difficult to recover.

4.Image is distorted. Message easily lost if picture subject to compression such as JPEG.

CONCLUSION

Steganography can protect data by hiding it but using it alone may not guarantee total protection. It is possible that by using a steganocryption technique,enemy detects presence of text message in the image file and then he/she may succeed in extracting information from the picture, which can be disastrous in real life situations. This is same for plain encryption. In this case by seeing the meaningless appearing sequence of bits enemy can detect that some illegal message is being sent (unless he/she is a fool),and we may land –up in a problematic situation.However, if one uses both methods, this will lead to ‘security in depth’. The message should first be encoded using a strong encryption algorithm and then embedded into a carrier.

REFERENCE

1. "Definition of STEGANOGRAPHY". *Merriam-webster.com*. Retrieved 14 December 2021*.*
2. Petitcolas, Fabien A.P.; Katzenbeisser, Stefan (2016). Information Hiding. Artech House Publishers.
3.Johnson, Neil; Duric, Zoran; Jajodia, Sushil (2001). Information hiding: steganography and watermarking: attacks and countermeasures.
4.**Steganography** **at** **Curlie**