COMPARISION

9.1 Cryptography VS Steganography

STEGANOGRAPHY	CRYPTOGRAPHY
The term Steganography is derived from the Greek word “steganos”, meaning hidden or covered.	The term Cryptography is originally derived from the two Greek words “kryptos” and “graph”, meaning hidden and writing.
Steganography means covered writing. The process of hiding digital information in a carrier signal.	Cryptography means secret writing. The art and science of studying methods of protecting data.
Steganography hides the trace of communication.	While cryptography uses the encryption to make the message incomprehensible.
Attack’s name in steganography is steganalysis.	While in cryptography, Attack’s name is Cryptanalysis.
In steganography, structure of data is not usually altered.	While in cryptography, structure of data is altered.
Steganography supports confidentiality and authentication security principles.	While cryptography supports confidentiality and authentication security principles as well as data integrity and non-repudiation.
In steganography, the fact that a secret communication is taking place is hidden.	While in cryptography only secret message is hidden.
In steganography, not much mathematical transformations are involved.	Cryptography involves the use of number theory, mathematically etc., to modify data.
Its goal is to assist in secret communication, it conceals the occurrence of any exchange between the sender and receiver.	Its goal is to encrypt the contents of the visible message to save the data.
It relies on the confidentiality of the method of embedding.	It relies on the confidentiality of the key.

Spatial domain, Transform Domain, Distortion, Model-based and ad-hoc are the techniques present in Steganography.	Transposition, Substitution, Stream cipher, Block ciphers are the techniques present in Cryptography.
It is implemented on Audio, Video, Image and Text Files.	It is implemented only on Text Files.
Its objective is to maintain survival of a message secret, Secret communication.	Its objective is to maintain contents of a message secret, Data protection.
It is used to carry several digital media.	It is used to carry text-based data.
Its key is optional.	Its key is necessary.
Input Files are at least two.	Only one input File.
Broken when attacker reveals that steganography has been used known as Steganography.	Broken when an attacker can understand the secret message known as Cryptanalysis.
The final result obtained is known as stego media.	The final result obtained is known as cipher text.
It is used for securing information against potential eavesdroppers.	It is used for securing information against potential eavesdroppers
Counter Steps: Use of data refining, rigid protocol specifications, observe data exchanges, carry out analyses which involve looking for structural indications of manipulation.	Counter Steps: Use of reverse engineering to split difficult algorithms execute cryptography export laws which disallow the transmission of such technology or devices between countries.
The message which is embedded is invisible to an unaware viewer.	The encrypted message which is encrypted is unreadable to everyone without the decryption key.
The goal of secure steganographic methods is to prevent an observant intermediary from even obtaining knowledge of the mere presence of the secret data.	The goal of a secure cryptographic is to prevent an interceptor from gaining any information about the plaintext from the intercepted cipher text.
It is hidden but not scrambled.	It is scrambled and unreadable.
No one can percept the hidden message.	No one can read the message without knowing the key.

Robustness: Against detecting the existence of secret data payload.	Robustness: Against breaking ciphers.
Main Challenges are Imperceptibility, embedding payload, and robustness.	Main challenges are complexity of encryption and key management.
Once it has been discovered anyone can get the secret data.	Once it has been discovered no one can easily get the secret data.
Steganography prevents discovery of the very existence communication.	Encryption prevents an unauthorized party from discovering the contents of a communication.
Technology still being developed for certain formats.	Most of algorithms are known by all and are developed.
Steganography requires a parameter like key.	Cryptography may not need any key.
Steganography is less popular than cryptography.	Cryptography is more popular than steganography.
It does not involve the role of mathematics.	It highly uses mathematical formulas and theories.
In Steganography, only the sender and the receiver know the existence of the message.	In Cryptography the existence of the encrypted message is visible to the world.
The Structure of data is not usually modified.	The Structure of data is modified.
Steganography is used from ancient time to modern era.	Cryptography is used in this modern era.
In steganography once detected, message is known easily.	Strong current algorithm are resistant to attack and larger expensive power is needed to crack those algorithms.
Modern steganography refers to hiding information in digital picture files and audio files.	Modern cryptography operates on binary bit sequences.
Adversary has no idea about your hiding something.	Adversary knows about your message but can't read it.
The structure of the data remains unchanged in the steganography.	The structure of the data remains changed in the cryptography.