References


References


References


References


References


References


References


References


References


Appendix A

Definition of Terms

Artifact: Artifacts are the irregularities that may be present in an image after processing. They are not related to the details of the image and sometimes accompany transmitted signals.

Bit-plane: The bit-plane of an image is a set of bits corresponding to a given bit position in each of the binary numbers representing the image.

Carrier: Carriers are the digital media that are used as a medium to carry the secret data. It is the medium into which the secret data is hidden.

Ciphertext: It is the translated text which is formed by encrypting the secret data. It is the unordered or substituted text created by changing its readability and meaning.

Coefficient: Coefficients are formed when a signal is transformed from an image representation into a frequency representation by using discrete transformation.

Cover-image: The image which is taken as a medium of covering the secret data. It is the original image into which the secret data is inserted into its redundant bits.

Cryptanalysis: It is the study of attacks on the cryptography to find weaknesses in them, without necessarily knowing the key or the algorithm.

Decibel: The decibel (dB) is a logarithmic unit used to express the ratio between two values of a physical quantity. It is used to measure signal level after processing and is widely used in electronics, signals and communication.

Decryption: Decryption is the process of taking encoded or encrypted text and converting it back into original plaintext which are understandable.

Eavesdropper: Eavesdroppers are the attackers (unauthorized person) who try to break a signal through communication channel to check if the signal contains any secret data.
Encryption: The process of transformation from plaintext (secret message) to ciphertext (unreadable format) to create a data that is not understandable.

Entropy coding: Entropy coding encodes an image by rounding the coefficient values to integer to reduce the size. Entropy coding is lossless compression.

Fidelity: Fidelity is the perceptual similarity between images before and after processing.

Keystream generator: It generates random sequence of numbers by partitioning the stego-key into random sequences. These sequences allocate positions of the secret bits.

MSE: Mean squared error (MSE) shows variation between the cover-image and resultant (stego) image. A high quality image should have less MSE value.

Payload: In steganography, payload relates to the amount of secret data that can be hidden into digital media.

Pixel indices: Pixel indices are the random locations of the pixels which are formed using random number generator.

Plaintext: It is the original secret message that is transformed into unordered state using encryption process.

PRNG: The pseudorandom number generator (PRNG) generates sequence of random numbers using a stego-key which is used to select random pixels of the cover-image for hiding the secret data. The key is used as seed for the random number generation.

PSNR: The Peak-Signal-to-Noise Ratio (PSNR) is the performance measurement criteria that show the relationship between the bit- or detection-error of two similar signals. A high quality image should have higher PSNR value.

Randomization: It is the process of scattering the secret bits in different pixel position of the cover-image that makes the secret data to be in random order.

Seed: The seed defines the starting point of a random number generator. It initiates the process of random number generation.
**Steganalysis**: Steganalysis is the technique to detect whether a given digital media contains hidden data. The steganalysis plays a role in the selection of features or properties of the digital media to test for suspicious data.

**Steganalyst**: Steganalyst is the individual (attacker) who performs the steganalysis with the purpose of detecting suspicious or secret data into a medium when transmitted.

**Stego-image**: The resultant image formed as a result of the steganography algorithm which contains secret data embedded into it.

**Stego-key**: The secret key used in the steganographic method to choose the random pixel position in the image. The security of a stego-key

**Target character**: It is the last character that is embedded into the cover-image. The target character terminates the embedding and extraction process.

**Zigzag**: Zigzag order is performed to group similar frequencies together by sorting the coefficients in zigzag ordering.