APPLICATIONS OF SYSTEM

8.1 Advantages of Image Steganography.

1. Image Steganography is a method that makes it easy to conceal a message within another to keep it secret. The result is that the hidden message remains hidden. A steganography approach can benefit images.
2. Unlike other methods, Image steganography has the added benefit of hiding communications so well that they receive no attention.
3. However, in countries where encryption is illegal, sending an encrypted message that you can easily decipher will raise suspicion and may be risky.
4. Image Steganography is a form of encryption that protects the information within a message and the connections between sender and receiver.
5. You can store an encrypted copy of a file containing sensitive information on the server without fear of unauthorized parties gaining access to the data.
6. Government and law enforcement agencies can communicate secretly with the help of steganography corporations.
7. The Image stenographic technique enables the concealment of the fact that messages are being transmitted through digital media, such communication techniques are invisible between the sender and the receiver, while cryptography obscures the integrity of the information so that it is not understood by anyone.
8. **Perceptual Transparency:** Perceptual transparency is an important feature of Image steganography.
9. **Hiding Capacity:** This feature deals with the size of information that can be hidden inside the cover file. A larger hiding capacity allows use of a small cover and thus reduces the band-width required to transmit the stegomedia.
10. **Tamper Resistance:** Of all the features, this feature is very important. This is because, if the attacker is successful in destroying the steganographic technique then the tamper–resistance property makes it difficult for the attacker or pirates to alter or damage the original data.

11. **Robustness:** Robustness is the ability of the hidden message to remain undamaged even if the stego–media undergoes transformation, sharpening, linear and non-linear filtering, scaling and blurring, cropping and various other techniques.
12. This approach featured security, capacity, and robustness, the three needed element of steganography that creates it beneficial in hidden exchange of data through text files and creating secret communication.

8.2 Disadvantages of Image Steganography.

1. The major disadvantage of steganography is that, unlike cryptography, it needed a lot of overhead to hide associatively few bits of information.
2. Image Steganography can be inefficient and time consuming, and it still requires you to have a secure channel where you can communicate which steganographic technique is being used, and where the data is hidden. Encryption is much simpler and far more data can be encoded in the same space.
3. If there are large number of information, huge file size, therefore someone can suspect about it.
4. If this approach is gone in the wrong hands such as hackers, terrorist, criminals then this can be very much critical.
5. Most data hiding approach take advantage of human perceptual deficiency, but they have deficiency of their own. However, these can be independently rectified.
6. The major disadvantage of Image steganography is that, unlike cryptography, it needed a lot of overhead to hide associatively few bits of information. Because the steganographic system is found, it is rendered useless. However, it fares no worse than cryptography and is still the preferred medium.
7. Hackers using steganography techniques for malware transmission.
8. The main limitation is the maximum size of the embedded data compared to the total data. If a piece of data is already very compressed it might be wholly impossible to embed additional data in it. And even under ideal conditions you will rarely get more than 20% out of the carrier data.
9. In multilevel security systems one wants sometimes to declassify some information from ‘top secret’ to ‘confidential’ or even ‘public’.

10. Image steganography is not easy as it seems, especially if you want to downgrade images.
11. The whole purpose for image steganography is to make sure the message is hidden. So, container media is too broken(picture) this might unveil the message.
12. Image Steganography is not without its disadvantages. However, these can be rectified and once it is performed and it can strengthen the element of steganography.

8.3 Applications of Image Steganography.

1. Secure Private Files and Documents.
2. Hide Passwords and Encryption Keys.
3. Transport Highly Private Documents between International Governments.
4. Transmit message and data without revealing the existence of available message.
5. To allow communication within an underground community. There are several reports, for example, of persecuted religious minorities using steganography to embed messages for the group within images that are posted to known Web sites.
6. Confidential communication and secret data storing.
7. Protection of data alteration.
8. Access control system for digital content distribution.
9. Media Database systems.
10. Defense and intelligence.
11. Medical.
12. Online Banking.
13. Other financial and commercial purposes.
14. For self-communication, image steganography is used to hide one-time passwords (OTPs) in images that are stored on a mobile device.
15. Image Steganography can be used to enhance the security of various applications, including secure communication.
16. Different approaches to secure communication, as discussed in the next section, entail different implementations of steganography.