Social Media Image Tracker System Using Image Steganography and Perceptual Hashing

Team Members:

Parikshit Patil (2016BTECS00003)

Farhan Jamadar (2016BTECS000052)

Jinesh Nadar (2016BTECS00061)

Objective/Aim:

Real World Objective is to find out the main culprit for spreading false rumored image on social media and to enhance security over Social Media.

Technical Objective is to Prevent any kind of intrusion of hacker from changing any information and to create a Strong Steganographic Algorithm.

Significance:

- Steganography and cryptography are cousins in spy-craft family. Cryptography scrambles a message so it cannot be understood. Steganography hides the message so it cannot be seen.
- A message in cipher text for instance might arouse suspicion on the part of the recipient while an "invisible" message created with steganographic methods will not.
- In this way, we can say that steganography completes cryptography, and actually there are usually two ciphers to break when trying to extract the embedded message: one is the one with which the message was embedded, and the other is the one with which the

Technical Details:

The underlying technology used in this project is Image Steganography and Perceptual Hashing.

Image Steganography is the process of storing the data into images by bit manipulation in such a way that it is unknown to others. The stronger steganographic algorithm prevents the hacker from retrieving the information. The information can be retrieved only by the admin, who knows the actual decryption algorithm. In this project, the name of creator of image as well as of the users who forward the image in social media will be stored in the bits of pixel. Whenever some catastrophic event happens due to any of image circulated in social Media, the creator of the image as well as the forwarders of image can be traced out with the help of the data stored in the image. This will be the reason for the justice if something bad happens due to the image.

There may be a case that image is edited by the user by applying some filter or by re-sizing the image. In this case, the concept of Perceptual Hashing is used to check if the image received to the user is somewhat similar to the image send by the user. If the algorithm finds the images same, then the chain of information present in the image is continued. By this way, the user cannot get away by changing the pixels bits.

Innovativeness and Usefulness:

The usefulness and innovativeness of the project lies in the fact that image steganography is amalgamated with Perceptual Hashing. Following points prove the uniqueness of our project:

- Steganographic Algorithm is highly secure and less prone to error.
- Enhance security over Social Media.
- Prevent any kind of intrusion of hacker from changing any information.
- Storing information in the image doesn't change the image altogether.
- Strong encryption algorithm is used.

Market Potential and Competitive Advantage:

As far as WhatsApp is concerned, they are not acquainted with this feature of tracking the image.

The reason is because WhatsApp Server never store data and images of Users.

If this feature is added to WhatsApp, it will be a great boon for the Cyber Security Purpose.