**Title-** Ensuring secure data transfer through steganography and steganalysis using deep learning.

**Objective-**

1. To develop a deep learning model for maintaining the secrecy and integrity of multiple secret images and protecting them from unauthorised access.
2. To hide the secret images in such a way that their existence itself gets hidden, unlike cryptography which hides only the meaning of the data.
3. To hide the existence of the secret images, steganography is used and then to retrieve the secret images at the receiver's end steganalysis has been done, in a way that there is minimum loss in reconstruction of the cover image and the hidden images.

**Brief description of the project-**

1. In the proposed work, a convolutional neural network-based model for hiding two secret images within a cover image and then retrieving the hidden image from the cover image has been developed.
2. The dataset used has been picked from the “Tiny images dataset”.
3. The model consists of three sections (Preparation Network, Hiding Network and Reveal Network).
4. The preparation network increases the dimensions of the secret images to match the size of the cover image.
5. The hidden network section takes as input the outputs of the preparation network and the cover image and then combines the three to create the carrier image or container image.
6. The reveal network is the final section of the model. It is used by the receiver of the container image. The section is used by the receiver to extract the secret data in the form of an image from the container image.

**Is the project related to any local problem?**

1. In the current scenario, the e-commerce transactions are secured by a username and a password, which does not verify if the card is being used by the actual card holder at the particular instance of time or not.
2. Businesses have difficulty in hiding the secret data from unauthorised access using cryptography as in cryptography the fact that the meaning of some secret data is hidden is known.

**Commercial Application:**

1. For E-commerce transactions, the current session ID embedded into the fingerprint image of the user can be used to verify if the transaction is being done by the actual card holder or not.
2. Business establishments can have concerns regarding trade secrets or new product data, steganography can be used to accomplish hidden exchanges of such secret data.
3. Steganography can also be used for invisibly watermarking the data to verify the authenticity of the data.