GRAPHICAL PASSWORD AUTHENTICATION

Mentors: Dipanshu Barnwal, Pranav Viswanath and O. Sai Sharan

Team Members: Akash A and Bharath S. N.

AIM AND INSPIRATION

- To build a user login interface with image as password
- Graphical image is broken down into grids of variable size which user must re-arrange correctly to access the application
- Lot of ongoing research in graphical image authentication systems since images can be easily remembered and passwords are difficult to crack
- Motivation to explore areas of image processing and cryptography related to security systems

EXISTING APPROACHES

- Two types of passwords used nowadays - recognition based and recall based
- In recall based, person is required to regenerate password stored at the time of registration. Thus, chances of someone replicating the same password.
- In recognition-based, a set of images consisting of a group of pass images is given to the user which he must select correctly chosen at the time of registration
- Useful in devices with good color display

METHOD AND WORKING

- At the time of registration, user specifies username, uploads image and specifies number of fragments
- Uploaded image is segmented into specified number of fragments. After segmentation, it is compressed and encrypted and stored into database
- At the time of authentication, fragments corresponding to username are displayed after jumbling them. User must reorder images correctly by drag and drop and then click Submit
- If images are correctly reordered, authentication is granted otherwise access is denied

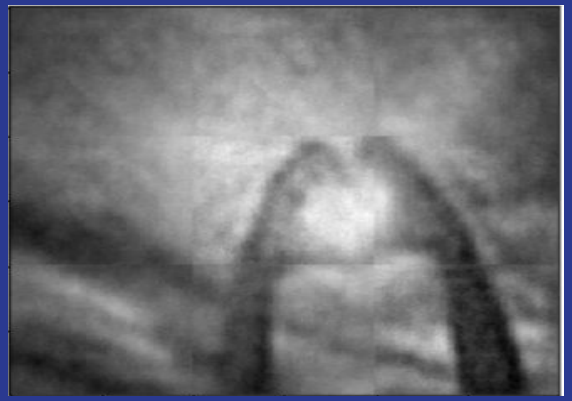
TECHNIQUES EMPLOYED

- Cryptographic methods (DES algorithm) for encryption
- Deep learning for image compression
- Web Development
- Programming Languages used for the database: Python and sqlite

RESULTS

1. Image Compression (8:1) using single hidden layer

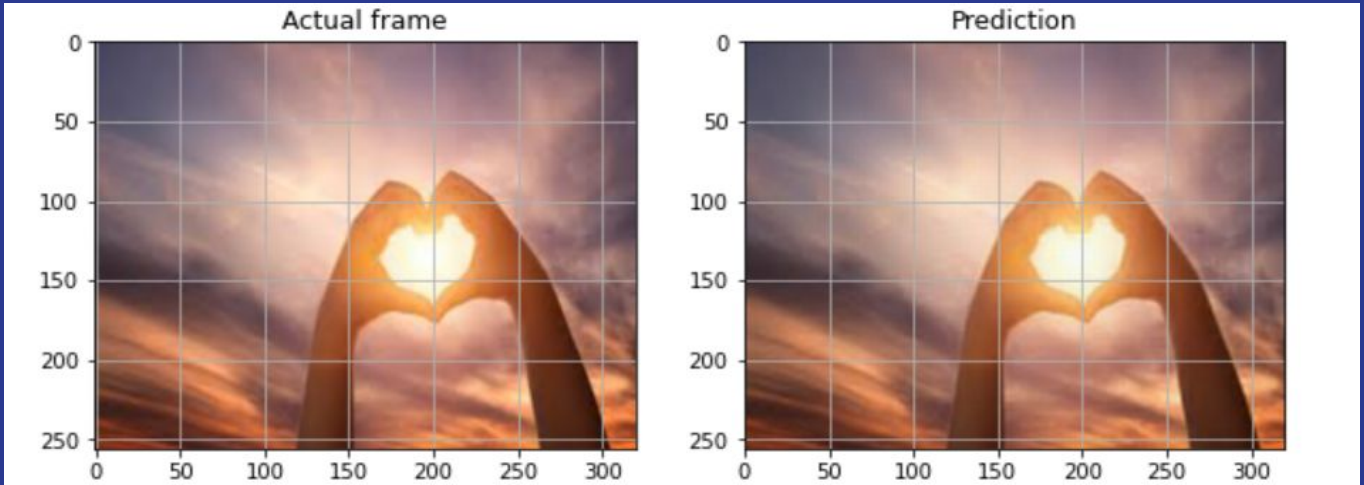
Before Compression



After Compression

RESULTS (contd.)

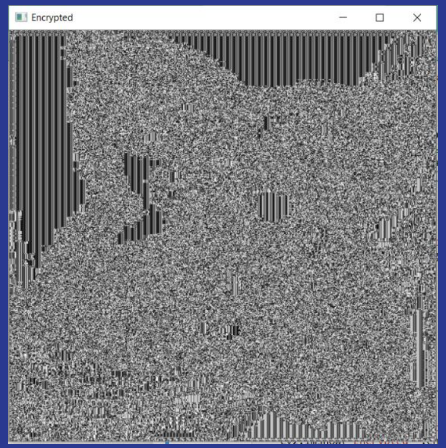
Image Compression using the UNET architecture



RESULTS

2. Image Encryption and Decryption

Original Image

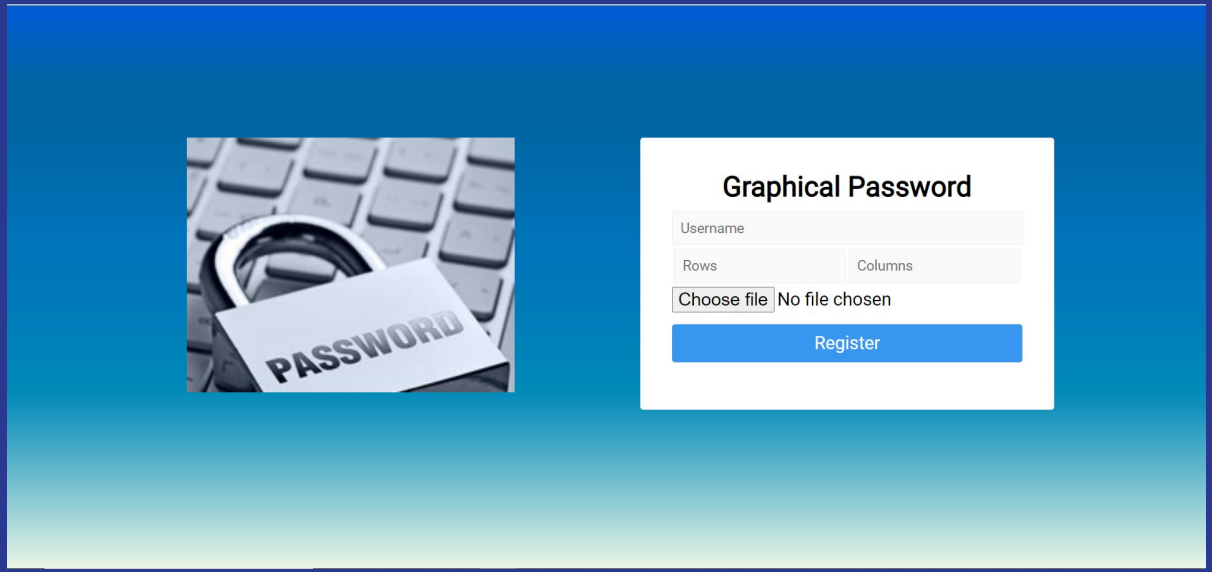


Encrypted Image

Decrypted Image

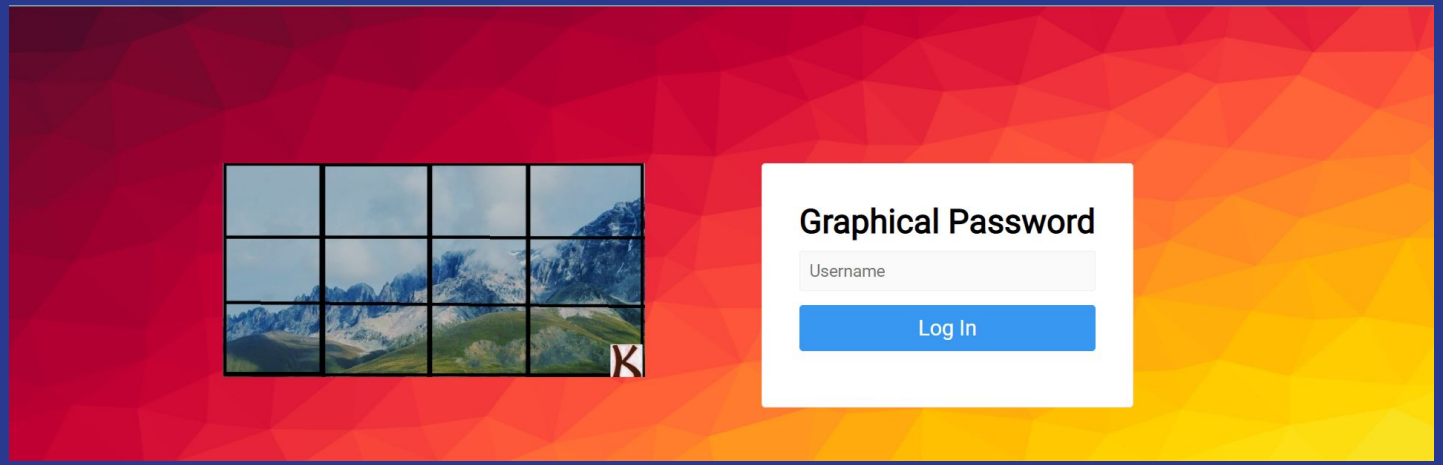
RESULTS

3. Web Page



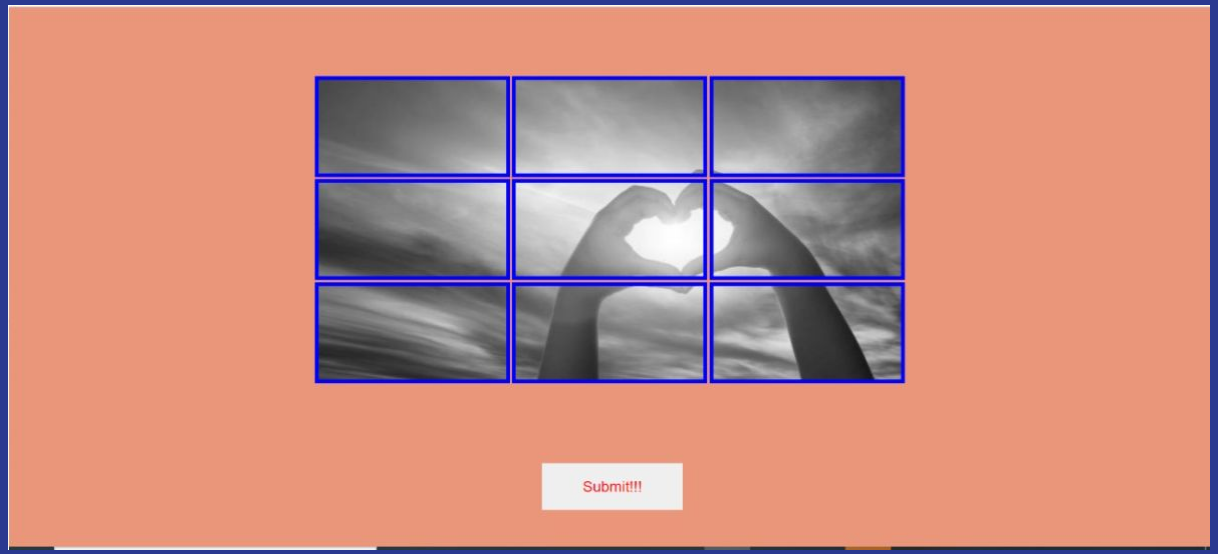
RESULTS (contd.)

Login Page



RESULTS (contd.)

Authentication Page



CHALLENGES FACED

- Images had a large size when stored as BLOBs and needed to be compressed
- Image compression using a single hidden layer gave blurred images
- Encryption and decryption of image using DES took time so size was reduced and then again resized after decryption.

FUTURE WORK

- To develop efficient crypto-compression methods and various combinations of CE, EC and JCE could be analyzed
- The image compression and encryption modules could be optimized so that the overall application could be used with improved processing time
- Current system is still immature. Much more research and user studies are needed to achieve higher levels of usefulness

REFERENCES

- Image Encryption: https://www.commonlounge.com/discussion/20f56c5cfff24d5d87f8a583505bb122
- Image Compression: https://www.hindawi.com/journals/js/2016/3184840/
- Papers:
  - https://www.ijitee.org/wp-content/uploads/papers/v8i6s4/F10950486S419.pdf
  - http://ijcat.org/IJCAT-2017/4-12/Authentication-by-Image-Segmentation-and-Shuffling.pdf