DocLock Application for Secure Document Sharing

Nayan Jain[1], Vishal Wadhwani[2], Bhavik Jain[3]

[1,2,3]*B.E.:Computer Engineering Dept., VESIT, Mumbai, India.*

Abstract - *The framework proposed in this paper provides an effective method for secure document sharing. The suggested method is based on Facial Recognition, Self-Destruct Timer and Screenshot Prevention Mechanism. With the Screenshot Prevention Mechanism, you can prevent recipients from forwarding, copying or even saving your file. In this paper we use Convolutional Neural Network for Facial Recognition so that only the intended receiver can open the file. This secure application will be suitable to work on android platform. The designed method provides confidentiality of a file and the integrity.*

Key Words: CNN, Screenshot Prevention Mechanism, Self-Destruct Timer, FLAG_SECURE, Two Stream CNN.

1. INTRODUCTION

Misuse of personal information is a serious problem for all individuals. The current process for transferring important documents or files between electronic devices is achieved by the means of e-mail or general chat applications. These data are sent in PDF, DOCX or image format. This mode of transfer can be vulnerable if the data sent is accessed by a person other than the intended receiver. The problem mentioned can be solved if no other user is given access to open the document other than the intended one. The proposed system uses face detection technique to detect and grant access to only the intended receiver. Also the information sent to the receiver must be deleted after use and not redirected to someone else, but sometimes the information is misused for purposes other than what an individual desires. This issue is resolved by the proposed framework by preventing the receiver from taking screenshot of the data or downloading it. The self destruct feature will allow the data to be persistent only for two days on the receiver's device.

2. EXISTING SYSTEM

Existing system refers to the traditional framework that was followed till now for transferring documents or other sensitive information. It was a one layer secured framework with pin or password protection. Using these frameworks an individual could send any file as a message to the receiver. The receiver would then download the file and use it. The respective file is then opened in the editor for further use. The disadvantages of the existing system are:

- In the traditional framework the only protection available are pattern and pin protection.
- The problem is that if any individual gets hold of this then security can be compromised.
- Receiver can still take a screenshot of the given file which makes this framework redundant.
- Also if a person forgets his/her password then opening the document again can be really difficult.
- After completion of a task keeping a file with an individual makes no sense.
- If other apps are given access to our app then security can be compromised.
- User interface is complex to be used by a novice.
- The algorithms used are time consuming and the low efficacy is undesirable.
- The content of the app is visible in the recent activities tab.

3. PROPOSED SYSTEM

The proposed system will eliminate all the anomalies of the existing system by having the following features:

- All users while registering will have to provide their face ids along with their basic information. When the user uploads a document, it will automatically be converted to an image format and then it will be sent.The sender needs to add the email address of the receiver.
- On receiving the images of the document, the receiver will be allowed to open the application but not the images directly.
- The face ids of the receiver will be verified in order to view the images.

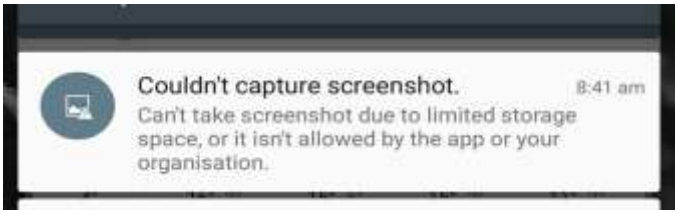

FIGURE 1. Result of trying to take a screenshot on using FLAG_SECURE in application.

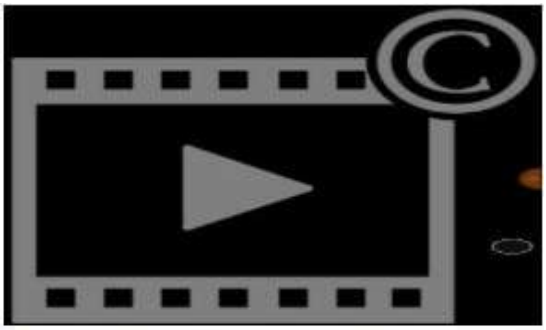

FIGURE 2. Result of trying to record screen on using FLAG_SECURE in application.

- Each time when the file is accessed, face id will be verified.
- While accessing the file, screen capture will be restricted.
- The received file will disappear within two days.
- The content of the app will not be visible in the recent activities tab.

The advantages of the proposed system are:

- By preventing screen capturing, the images can't be misused.
- The application will display a blank display in the recent activities tab which mean not even a slight detail will be visible to other people through the recent activities tab.
- The self destruct feature will ensure that the information doesn't remain with the receiver after two days.
- The features will ensure complete security of the information of a user.

4. SCREEN CAPTURE BLOCKING

It is possible to block users from taking screenshot in android application. The WindowManager.LayoutParams class in Android provides a constant FLAG_SECURE to restrict screen capture of the present window. It treats the content of the window as secure, preventing it from appearing in screenshots or from being viewed on non-secure displays.

Android's FLAG_SECURE also blocks users from recording the screen using a third party screen recorder application.

```
protected void
onCreate(Bundle
savedInstanceState)

 {
  super.onCreate(savedInstanceState);
getWindow().setFlags(WindowManager.Layout
Par ams.FLAG_SECURE,
WindowManager.LayoutParams.FLAG_SECUR
E)
; setContentView(R.layout.activity_main);

}
```

Table 1: Sample Code to use FLAG_SECURE:

5. FACIAL RECOGNITION

A Convolutional Neural Network consist of network made up of neurons with weights and biases that can be changed. Every neuron performs a dot product with the input and forwards it. The network on whole takes an image as an input and gives a single differentiable score function as an output. We take the explicit assumption that an image is given as an input as it allows us to encode certain properties into the architecture. These then make the forward function

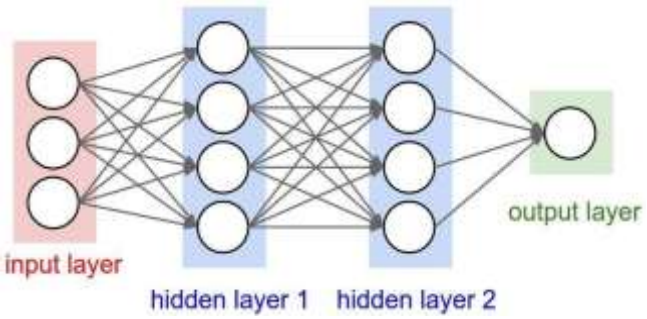

FIGURE 3. A regular 3-layer Neural Network. Right: A ConvNet arranges its neurons in three dimensions (width, height, depth), as visualized in one of the layers. Every layer of a ConvNet transforms the 3D input volume to a 3D

more efficient to implement and vastly reduces the amount of parameters required by the network. For the project, we developed our face detection methods using the following approaches: First, we developed a model called Two Stream CNN, which specializes in classification and localization for a single face detection. With an input image, this Two Stream CNN method is capable to output whether it contains a human face or not, and if there is a human face, it would also output the identity of that human (classification) as well as the coordinate and the size of the bounding box (localization). We also try to perform our multi-object detection with a cascade of Region of Interest Network and Two Stream CNN. This ROI Network helps in eliminating the number of repetitions required.

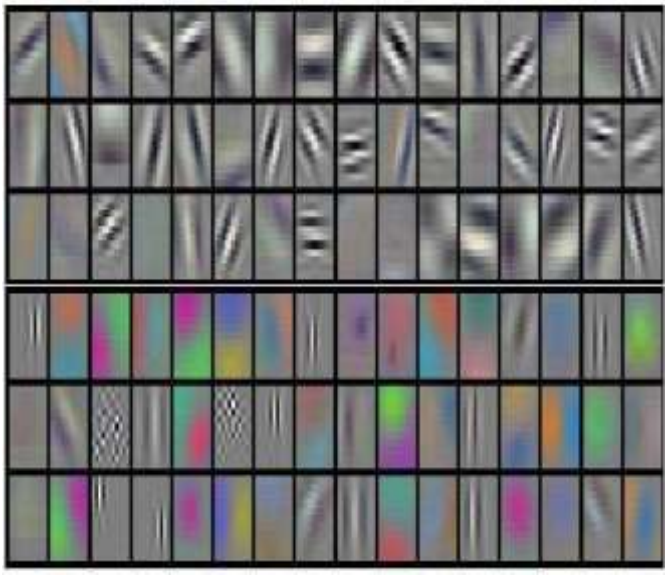

FIGURE 4. Filters learned by Krizhevsky et al. Each of the 96 filters shown here is of size [11x11x3], and each one is shared by the 55*55 neurons in one depth slice.

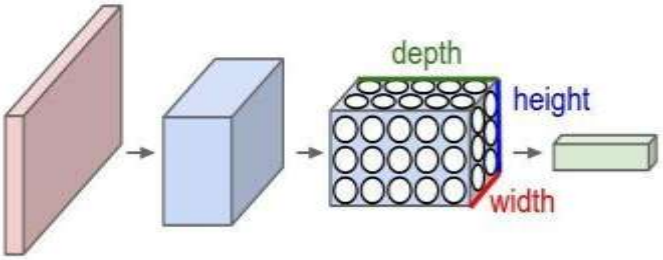

FIGURE 5. The red input layer represents an image with the height, width and breadth represented by the the three colours.

6. CONCLUSIONS

The proposed framework describes the way important documents or files can be securely transferred between two android devices. The framework uses face detection and screen capture blocking technique for security of the data. Users will be able to transfer information with the assurance that it reached the intended person.

Considering the complexity of data security there is a need for a lot of research on this subject in the future. In the following paragraph we would thus like to list few open research issue associated with security.

- Encryption: If a miscreant tries getting the file from the network then end to end encryption will safeguard the data from being accessed.
- iOS: Our system considers only Android OS but we can develop this application for iOS too in the future.
- Facial Recognition: Our application only uses images to verify user but we can also add support for a combination of light projectors and sensors to take several images of users facial features and train our network.
- Other risk: We should remember that one can always point a camera on the screen to steal the content. We cannot stop someone from from doing that but we can assign every file sent with some key unique to that user so that he may be deterred to do it.

REFERENCES

1) Yicheng An, Jiafu Wu, Chang Yue(2016). CNNs for Face Detection and Recognition. 2016 CVPR J. Clerk Maxwell," A Treatise on Electricity and Magnetism", 3rd ed., vol. 2. Oxford: Clarendon, 1892, pp.68-73.

2) Justin Johnson(2017). Derivatives, Backpropagation, and Vectorization. 2017 CVPR

3) Yoshua Bengio (2012). Practical Recommendations for Gradient-Based Training of Deep Architectures.

4) CS231n: Convolutional Neural Networks for Visual Recognition. Retrieved Spring 2017, from http://cs231n.stanford.edu/syllabus.html

5) Vinothkumar Arputharaj. Disabling screen shot capture in Android application (2015, June18), Retrieved from https://stackandroid.com/tutorial/disabling-screen-shot-capture-in-andr oid-application/