CHAPTER 1

1.INTRODUCTION

1.1. Overview

Cartoon images are fully human's creativity. We can witness cartoons into millions of characters whether in kid's tv programmes or advertisements, they are now present everywhere. Nowadays, cartoons are not only considered as a form of entertainment but also helpful in attracting customers in the malls or for the purpose of sharing some important information on the roads on which we generally don't want to waste our time. Image cartoonification has now become easy with discoveries in techniques and it has now become an important part of computer graphics. Cartoons has now taken the form of digital arts. We can now convert a simple raw image into cartoon with the help of some lines of code but creating these lines of code is something out of knowledge for general public as it requires deep knowledge of computer science and its processes. Thus, we came up with the idea of developing a software to make this technique available to the public using our knowledge. This project aims to convert a raw image and do all the required steps for conversion into cartoon form in a simple and efficient way.

1.2. Project Description

"Cartoonifying Image" is a project which converts a normal image taken as input from user into its own cartoon character. This project is developed by the combination of OpenCV and some Python libraries e.g., NumPy to get the desired output. A technique, which is used to conceal the secret image into transparencies (which will vary with the user) and these transparencies are distributed to the intended recipients. The transparencies are embedded into the meaningful images so that the intended recipient will have a transparency, which is a meaningful image. Without much computation, only the qualified set of participants can reveal the secret image by simply stacking transparencies. The tool can be used in both ways, to encrypt the secret image into transparencies and to decrypt the embedded images. User can send encrypted images that are in the format of GIF and PNG. The encrypted transparencies can be saved in the machine and can be sent to the intended person by other means. Experimental results reveal that the tool works with grey-scale images in the format of .png and .gif.

CHAPTER 2

2.THE PROBLEM STATEMENT

2.1. Problem Description

In today's world there are many encryptions and decryption algorithms, used especially in the communication system provided in variety of applications. People are still finding ways to secure the transmission of data among different channels. Our project is used to perform secret data transmission by performing encryption of text on images the sender uses a key to perform encryption and the same key is given to the receiver to decrypt and obtain the data. An attack that affects the confidentiality of information often presents for the integrity of such information to be compromised intercepted information on transit would make little or no sense to an interceptor if he is not able to decipher the content of the information.

Encryption and decryption are particularly impacted in the field of military communications and reliable security data to protection and transmitting used to send the information such as direction, strategy, and secret code and other information. This also implies where there is a strong need to transfer some confidential data which when anyhow falls into wrong hands can cause massive security issues. For example, let's consider a scenario where a biochemical industry has developed some new formula which needs to be presented to senior authorities present at distinct locations, thus there is a risk of data manipulation or stealing if not transferred securely, here encryption and decryption plays a role. He will use the algorithm to encrypt the data and transfer it safely to the authorized persons and the receiver will decrypt the encrypted file using some key provided to him. Thus, we got an idea to develop a new algorithm for encrypting and decrypting the data using over an image using the techniques of image processing. The main issue arises here is the process of receiving data for the encryption and decryption processes as it will be a matter of confidentiality for the client to share the data with us, not being the authorised personalities to view the confidential data.

2.2. Problem Solution

We all know that today every bit of data being shared over the internet is under the eyes of hackers if not proper security methods are used. There are several techniques available for the purpose of encryption and decryption. Texts can be simply encrypted using these algorithms and using the same key can be decrypted. This gave us the idea of doing encryption and decryption of data by using images. Instead of encryption and decryption method of transferring data we can use image processing for hiding the data into an image. Each image is represented using some pair of combinational nodes over a machine. Thus, we can use these nodes to store some bit of hidden information hidden behind them. Greyscale is a technique used to convert the image in a Gray shade. This Grey scaling technique is useful in the process of hiding the data behind an image as it is nearly impossible to drag out hidden data in this colour. It is better method to hide the information and is reliable as compared to other techniques.

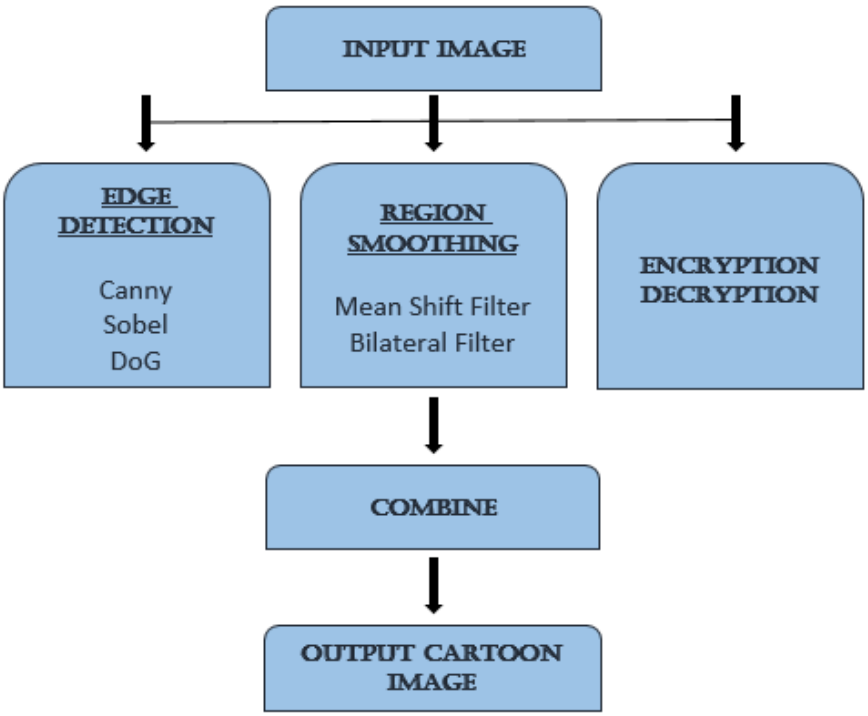
CHAPTER 3

3.EXISTING SYSTEM

3.1. Introduction

Designing an encryption/decryption system, amongst other things, requires decision on the basic functionality of the software, and the choice of cryptographic algorithm to be used. While the functionality supports the attractiveness of the system, the type of cryptographic algorithm determines how much security the system would provide. Our project allows the user to Encrypt image processing data step by step firstly it encrypts the data at sender side using simple steps and method. The interface is very interactive and easy user and understand GUI. Then it is decrypt at receiver side.

3.2. DFD for Present System



3.3. What's New In The System To Be Developed

Our Project Encryption and decryption refers to the process of scrambling information so that the observer cannot be detecting the data. We can use image processing by hiding data into image it is better method to hide the information.

CHAPTER 4

4.PROBLEM ANALYSIS

4.1. Product Introduction

Our project to make a cartoon image we gate a picture-based methodology. Is the process of translating plain image data into something that appears to be random and meaningless? To decrypt a particular piece of cipher image the key that was used to encrypt the data must be used.

4.2. Feasibility Analysis

Basically, this is the phase which plays an important role in deciding whether it is optimum to go for the project or to drop the idea of it. It tells us about the success potential of the project is in all the aspects i.e., technically as well as economically and enhances the success rate of the project because a complete study has been done on the project.

The constraints in feasibility studies were:

1. Technical
2. Economical
3. Behavioral
4. Operational

4.2.1. Technical

All the technical requirements were feasible and well supported over a vast scope of systems. The project was developed on an open-sourced platform developed by google named “colab” and is supported over all the browsers. The technology required for the working was done using the features of Python and OpenCV which is easily accessible to the developers as well as users.

4.2.2. Economical

As all the major requirements of the project were covered using open-source technologies, it became much economical using these resources available all over the web.

4.2.3. Behavioural

Project will be developed to give the client a total user-friendly experience. The outcome of the project is completely positive as there will be less consumption of time and a total interaction between the user and system.

4.2.4. Operational

All the working environment is available on the google colab platform at a single click. The project will get completely operational without setting up an external environment as everything will be performed using browser only.

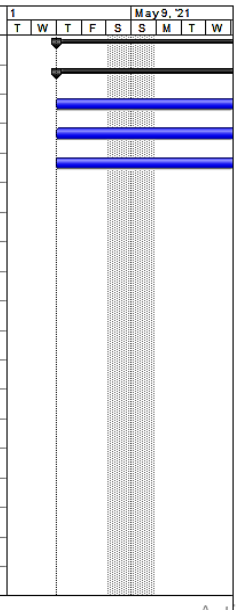
4.3. Project Plan

Project plan describes all the activities and their duration. It also summarizes the activity planning about all the tasks and processes including the designation of every member. This phase defines the responsibilities of the members, time required to perform various tasks in a well representative manner. A proper project planning can boost the success rate of project by allowing the members proper utilization of time and do the required changes needed during the production phase.

We created a proper working schedule for the development using Microsoft project tool:

.

ID	Task Name	Duration	Predecessors
1	**CAPSTONE PROJECT**	**98 days**	
2	**Requirement Analysis**	**10 days**	
3	Open end questonaries	10 days	
4	surveys	10 days	
5	online research work	10 days	
6	**Requirement Gathering**	**10 days**	**2**
7	**Feasibility studies**	**7 days**	**6**
8	technical	7 days	
9	economical	2 days	
10	behavioral	2 days	
11	operational	3 days	
12	**Design**	**15 days**	**7**
13	**coding**	**20 days**	**12**
14	**Testing**	**7 days**	**13**
15	error debugging	7 days	
16	**Implementation**	**15 days**	**14**
17	**Documentation**	**14 days**	**16**
18	Research Paper	7 days	
19	Project Report	7 days	18



CHAPTER 5

5. SOFTWARE REQUIREMENT AND ANALYSIS

5.1. Introduction

The technology is increasing gradually but security is main concern of any technology that has been implemented on any machine. When we are implementing any security feature to our server, or any machine data protection is our main concern. For that data would be safe we have implemented encryption decryption features on google colab. The project has design on image processing means encryption and decryption being done on image not at plane text. As we all know that encryption and decryption are always the better option for providing user security. So, as we have two types of cryptography techniques here, first one is symmetric and second one is asymmetric cryptography. Talking about symmetric technique, here only one key is used for both encrypt and decrypt electronic information whereas if look at the asymmetric where a pair of keys, one public and one private is used to encrypt and decrypt the information. But if we look as in of security basis asymmetric one is more secure than symmetric. Symmetric encryption is faster than the other one. They both are important and effective indifferent ways, depending on the task at the hand, either may be both deployed together or alone.

5.2. General Description

The project has design with python programming for encryption decryption. There is various module are used to perform encryption decryption. As we know python is not compiled language and it is open source and free so we can run on any operating system like Window, Linux, MacOS. We designed project with google collab. Google colab is free cloud service and now it supports free GPU also. We can write out pyhton code there. Plus, it is an online IDE so we don't have to create environment and all before starting our ML or DL projects. Colab makes it more interesting for the coders to code more in python. It is more focussed on making work easier and reducible. It is considered as an excellent tool for ML task also.

5.3. Specific Requirements

To perform encryption decryption, we need few software and environment. First, we need an operating system whether its Linux or windows, after that we need to install python on system and few modules that have being used in our project. Like

The following module being used:

- Cryptography
- Simple-Crypt

1. Encryption of Data
2. Decryption of Data
3. Libraries used for Cryptography

CHAPTER 6

6. DESIGN

Design is a process which includes multiple steps following a respective order. Although these steps can be developed individually but must be in coordination for a system to work in an efficient manner. This project is designed with the help of google colab, Python and OpenCV for image processing.

6.1. Research Regarding Project Design

A lot of research work was done in order to extract the knowledge about the project being considered. Selecting Python as the coding language was based upon the facts that it has several libraries which are required for the image processing in machine learning. Python has a very simple and clear syntax to write the code. We read several articles regarding the topic from the neptune.ai blogs which helped us to understand the process of developing this project and made our requirements crystal clear. From here we came to learn about the OpenCV, which is an open-source library developed by Intel systems. OpenCV along with the TensorFlow mechanism allowed us to deal with all the issues which showed up in the image processing phase. TensorFlow mechanism is compiled of many different models and algorithms to implement in image processing. The next area of concern was to find out the platforms which could help us to integrate all the above functionalities without creating major issues and thus we selected google colab for the implementation of this project. As it provided us with all the requirements of integrating TensorFlow mechanism with OpenCV for image processing and implementing Caesar-Cipher mechanism for encryption decryption phase using Python.

6.2. Introduction to Google Colab

Colab has been proved to be one of the finest research in the field of artificial intelligence. Since it works on the tensor flow mechanism, it has become easy to develop projects on this platform as it gives you freedom to develop and modify the interface as well. Another important feature provided in this is the option to switch between normal CPU or high performing GPU of your system to deal with heavier projects which require machine learning algorithms. Python being our first choice of coding, Colab was very helpful in development of this project as there were no additional configuration requirements to be set up. One can write arbitrary python code and import its libraries on the browser itself. It also provides free access to the cloud storage for sharing purpose.

6.3. OpenCV & Its Uses

OpenCV could perform from basic to all the major image processing functions like image segmentation, object analysing and recognition, etc. It involves conversion of images into greyscale method to extract the information from the different pixels which could be useful in hiding data under the images as in the process of encryption and decryption. This module has its own functions to read the image using their path as argument in imread() function and imshow() function to show the output image.

6.4. Encryption and Decryption

As the core idea of our project is to provide encryption and decryption of the input data in form of images. This is done at the end of the image processing. It is highly important plus required also in these client-based project. Encoding performs task to encode the data so that the data will get hidden or not be accessed by the unauthorized users. It helps in protecting the private information, sensitive data and it also enhances the security between client and the server. And if suppose your data is encrypted and then also some unauthorized users get access to your data, they will not be able to read your file.

Now talking about the decryption, so if we have encrypted that data then it's obvious, we must decrypt it also. After decrypting the data, it will come in its original form. In short it is a reverse process of encryption. Here the encrypted information is decoded so that the authorized user can access data by using a key or password because decryption needs a key.

6.5. Functional and Operational Requirements

This requirement outlines the functional/operational capability that the system can be able to provide and reaction to a particular problem. The data encryption and decryption system have the following functional requirements:

1. The system shall be able to identify documents with .PNG AND .GIF extension, for encryption.
2. The system shall be able to generate public and private keys to be used by registered users for both encryption and decryption.
3. The system shall be able to encrypt and decrypt image files stored in the computer system.
4. The system shall be able to save the encrypted plain image as .png and .gif files
5. RAM: 4gb, windows 7 or above.
6. Proper internet connectivity to connect and install the online libraries.

6.6. Security Requirements

The security requirement entails the capacity to control user access, manage data and support the three-security concept (E.g., confidentiality, integrity and availability of data). The security requirements of the new data encryption and decryption Systems are listed below:

1. The system shall be able to authenticate users.
2. The system must be able to deny access to illegitimate users to the system
3. Only the authorized personalities should be given access.
4. System must be running on secure configuration
5. System must be free of malwares, viruses or any trojan horses

CHAPTER 7

7. TESTING

Testing has major role to check our project that it is working properly or not. This is the phase which checks that before the deployment of software testing is required so that it could don't create further technical issues. Testing is very important in many ways, one of the most important one is cost-effectiveness. It can save money in long run. Most sensitive and vulnerable part testing can provide is security. But then the question come up that how testing help in security so here they are, the user gets the trustworthy software to rely on, keep use's personal information and data safe, problems and risk are resolved beforehand, saves a lot of problems later.

7.1. Functional Testing

Functional testing is a kind of quality assurance process and a type of black box testing that bases its test case on the speciation of the software component under test. Some types of functional testing's are unit testing, component testing, smoke testing, integration testing and many more. The main aim of functional testing is it ensures that the customer or end user is satisfied. It produces a defect free software.it ensures that all requirements should be met.

Now talking about our project so,

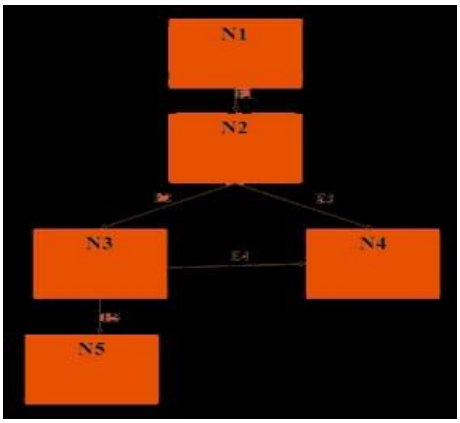
As we use cryptography techniques for that we have taken an image that is converting in unreadable or imaginary that normal user cannot be understand or a meaningless image. Testing of image is to check image is loaded or not properly testing of function we are using to load. The function path should be valid. The module we are using we test that all modules is installed properly or not; like we used OpenCV, NumPy should be installed and import.

7.2. Structural Testing

Structural testing is the type of testing carried out to test the structure of code. It is also known as White Box testing or Glass Box testing. This type of testing requires knowledge of the code. Basically, it is used to test the internal design of the software, or we can say the code part of the dataset

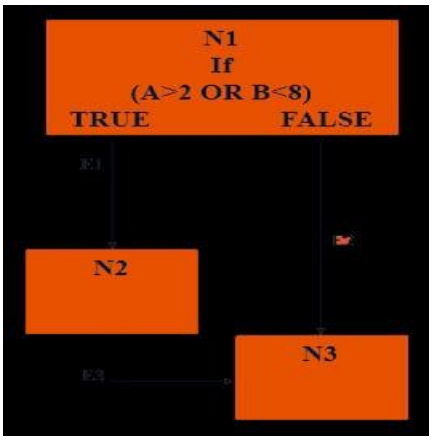
7.2.1 Techniques of Structural Testing

1.Statement coverage:



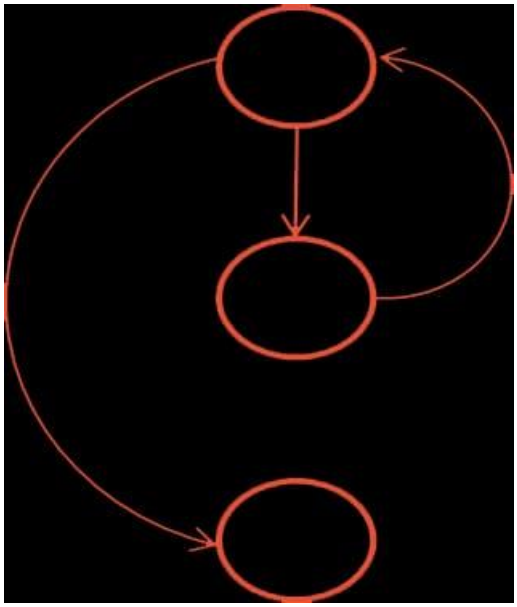
It ensures that the privilege of statement that has implement to perform that specific part should be not beyond that, suppose we have imported an image by using img. Load function than it should work on loading of image only. There are so many statements that are involved in the programming of the specific software. And it's obvious also that those statements can have error too, hence the statement coverage is aimed at checking all the statements by calling them in practice. It also aims at carrying few tests if possible.

2. Branch coverage:



It is known as decision covering test. It is aiming to test all the branches or edges at least once in the test suite or to test each branch from a decision point at least once. It provides solution for the problem faced in Statement coverage. It is slightly different from statement coverage. It does not focus on the test, but it just takes care that each test carried out at least once if not more than once.

3. Path coverage:



As the name suggest path coverage focuses on all the paths that can be involved in the codes. Pathe coverage has the maximum number of the test to be carried out, out of three techniques. It covers both branch coverage and statement coverage. When every path is tested it is automatic that every statement is also checked.

4. Condition coverage:

S.No.	A	B	A/B
1	0	0	0
2	0	1	1
3	1	0	1
4	1	1	1

Individual conditions can be put to test with Boolean inputs. The process offers better coverage and problems that were discussed under branch coverage can be rectified in this process.

CHAPTER 8

8. Implementation

Python provides various module to perform various operation so here we cryptography module that python provide. It is very helpful to perform entire encryption decryption process. We used cryptography techniques to perform encryption decryption.

8.1. Implementation of project

Computer vision may be is the stuffy area in Artificial Intelligence with a wide array of uses that pre-owns python. Python is a group of libraries. It has numerous libraries for authentic applications. One such library is Open CV [9]. Open CV is the most famous library used in computer visions with so much fascinating stuff. Open CV is a cross platform library that assimilates application like video and picture taking and producing media. It is importantly used in image conversion, face recognition, object detection, and numerous other shocking applications. We will follow the following steps in this article to convert the image to cartoon.

- Ship in library
- Studying Input Image
- Detecting edges in the image

It is the main process in which "all the functionalities required are loaded and the project inputs are completely processed to get the output on the basis of algorithm applied." Implementation phase involves:

8.1.1. Loading the functionalities

Loading functionalities here refers to the various objects of the project being linked up together so that the project works fine without giving any error. This phase also involves making the arrangements required for the operations. It is the starting stage of project implementation where it includes all the resources.

8.1.2. Activation of the project

Project activation is nothing but making the required arrangements to have the project that need to be started. It is the starting stage of project implementation where it includes the allocation of resources so that the project becomes operational, and coordination sets up between the different elements of the project.

8.1.3. Operation of the project

The whole project flows in a sequential manner from the early stages of the working, taking inputs from the client and performing the operations needed to attend the desired outputs. The whole processing of the input is done within a specific timeframe so that there is no mishandling of the information occurs. The total time taken to process the input is also monitored to fix the further complications if any occurs during the operations.

8.2. Encryption Process

Firstly, we will read a colour image from files with specific path

```
#Reading image
img = cv2.imread("/content/drive/MyDrive/download.jpg")
from skimage import io
io.imshow(img);
#open source python pkg(skimage) and is used for image processing
```

We are loading the image in img variable from specific path and skimage will import (io) and we check with whether image is loaded or not with help of io.imshow().

This process makes use of greyscale method to hide the data behind the image. Here, cv2.COLOR_BGR2GRAY shell is used to convert the images in greyscale which provides the base for encryption. This phase also makes use of some bitwise operations too like bitwise XOR.

```
encryption = cv2.bitwise_xor(cv2.cvtColor(img, cv2.COLOR_BGR2GRAY), key) # encryption
decryption = cv2.bitwise_xor(encryption, key) # decryption

io.imshow(encryption) # Display ciphertext image
```

```
<matplotlib.image.AxesImage at 0x7f60c9c17d50>
```

8.3. Decryption Process

After applying the encryption algorithm and successful completion of the encryption phase a key is generated. This key is used in the decryption phase to decrypt the data and the image from greyscale.

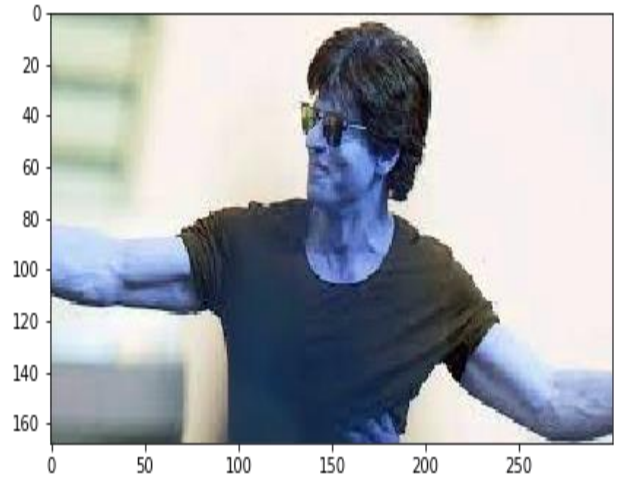
```
io.imshow(decryption) # Display the decrypted image
```

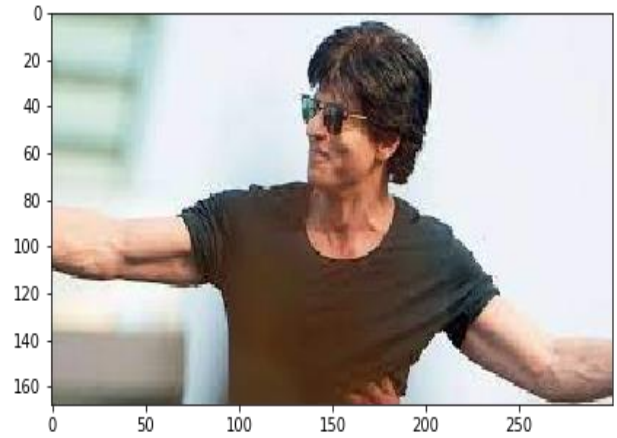
```
#Cartoonifying the image
color = cv2.bilateralFilter(img, 9, 250, 250)
cartoon = cv2.bitwise_and(color, color, mask=edges)
```

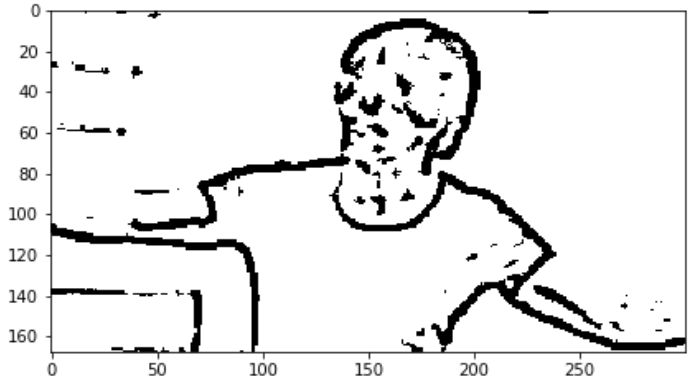
8.4. Conversion Plan

The project is flexible for any types of images like we are taking colour image then it will generation different shape it means if we change the image any type of image whether coloured or black

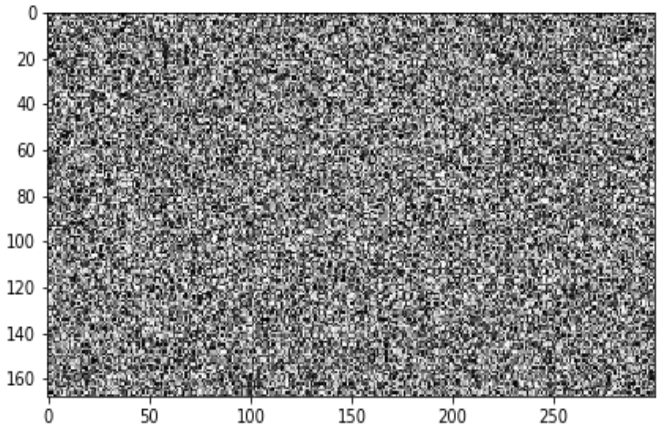
It will generate distinct figure after every phase as shown below:

1. 

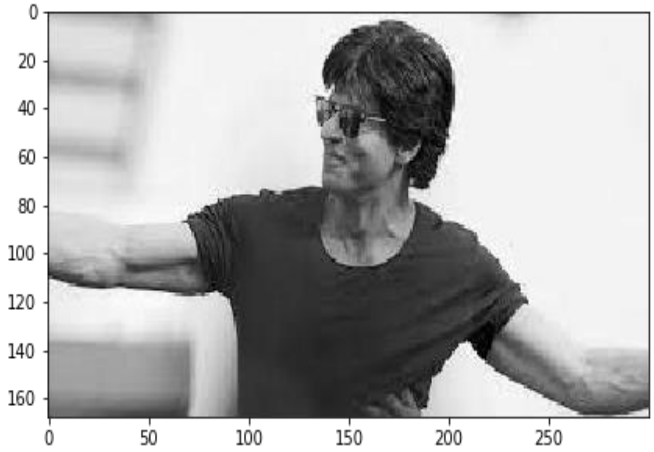
2. 

3. 

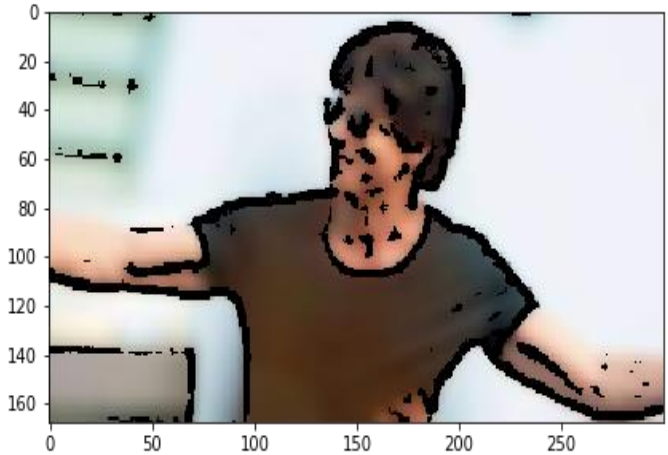
4.



5.



6.



All the images shown above are results of steps involved in the process of converting the images and applying the encryption decryption methods. These images are produced as output for every consecutive processes. The final output is given to the client in form of a cartoon image which is the cartoonified form of image provided as input to the system.

CHAPTER 9

9. PROJECT LEGACY

9.1. Current Status of the project

This project is currently focused on encryption and decryption on raw image data only. The input of the project is any raw image in applicable format on which the encryption and decryption is processed. The encryption and decryption happen in a way that data is concealed behind the pixels of the image and the output is given in a cartoonified image. The client is able to do encryption as well as decryption on the single platform. These days data is the only wealth and with so many attacks going on the server it is getting difficult to transmit he data in a safe and secure manner, thus we came with the idea of developing this project so that one could feel safe while transmitting data to different locations.

9.2. Remaining Areas of concern

As the technology is growing, we are witnessing keys to every problem and sometimes these keys come into hands of unauthorized persons who aim to steal the data for their personal uses. The project works fine with the image encryption, but we need to focus on every aspect of the data processing. The remaining area of concern includes applying much safer algorithms which are impossible to break in case any attack occurs in future. The software should work on any kind of data not only gets specific to image encryption and data should reach safely to the authorized person only.

9.3. Technical and managerial lessons learnt

Developing this project played a very significant role in making us understand the basics of image processing and the process of encryption and decryption. This project was aimed to develop an encryption decryption website and with some sort of knowledge clearance we were able to upgrade the project to image processing along with the process of encryption and decryption.

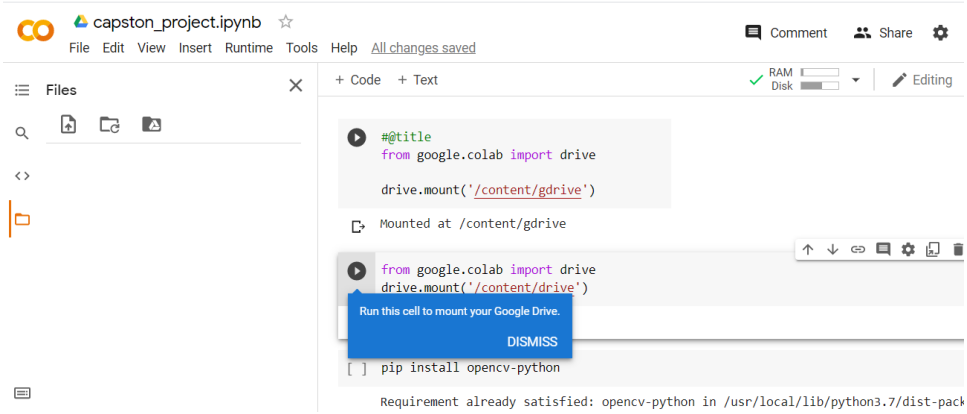
This project helped us to learn about the various features of google colab and how to develop projects on these online executable platforms. The project has a vast operational and functional properties which could have been difficult to develop but with proper distribution of the tasks among all the members we were able to develop it in a more learning manner. Fixing the errors and glitches are one of the toughest parts of a software and we were able to learn some of the error fixing strategies as well.

CHAPTER 10

10. USER MANNUAL

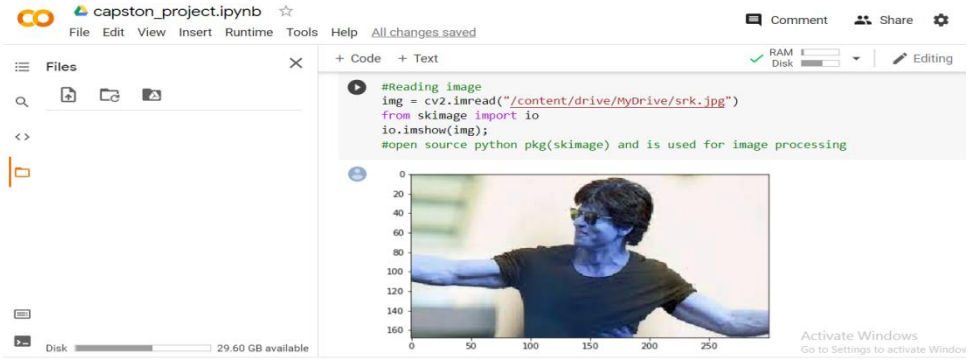
The project was developed in a very simple way so that user faces no complexions and gets a true user-friendly experience. This project elements are classified according to their working in separate sections from very first step of connecting the drive, taking inputs, processing of image to get the desired output. Every step follows in a continuous manner to provide the best user experience and complete view of the operations going on. we have used google colab research platform and the python programming for the internal coding. Python provides us several high-power inbuilt features and libraries which made the development of project easier. A client should follow these steps to get the desired output from the host site:

10.1. Mounting of drive: connecting your google drive to the server as the input data should be taken from drive and there is no need to upload your critical data on server site. Here, one needs to connect his personal drive to the system and mount it. After connecting your drive, you need to click on the play button or press "SHIFT+ENTER" drive will get mounted and gets to the next step.



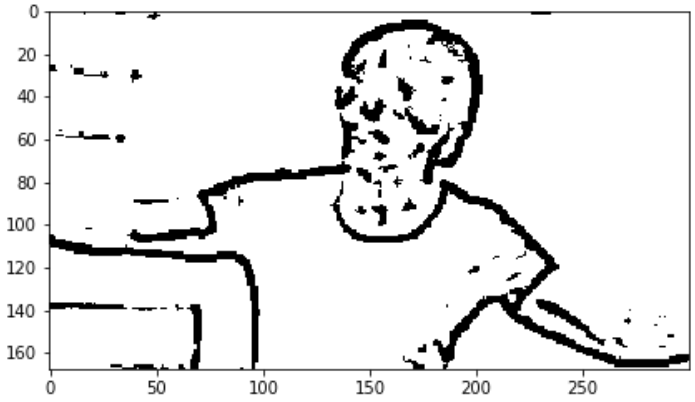
10.2. Importing the libraries: After the path of image is provided ,activation of the functionalities is to be done. This step requires importing all the libraries which are cv2[6], NumPy[7], cv2_imshow[8]. These libraries are required to process the input image.

10.3. Specifying the path: Next step involves providing the correct path of the image on which encryption has to be performed and serves as the input. From the drive you need to get the path of the image and enter it into the reading image section [9] of the interface.

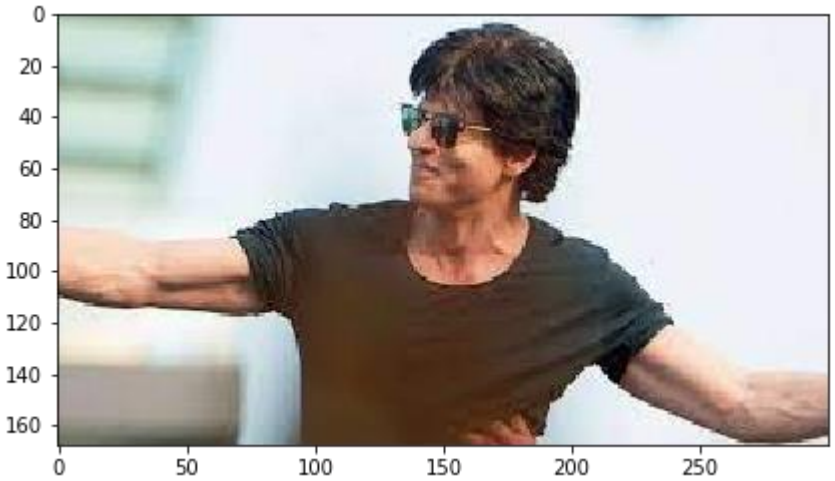


10.4. Output Generation: This is the final step where one only needs to press the play buttons of different sections in a respective manner. This is the step where all the image processing and system operations are performed. This step involves following processes:

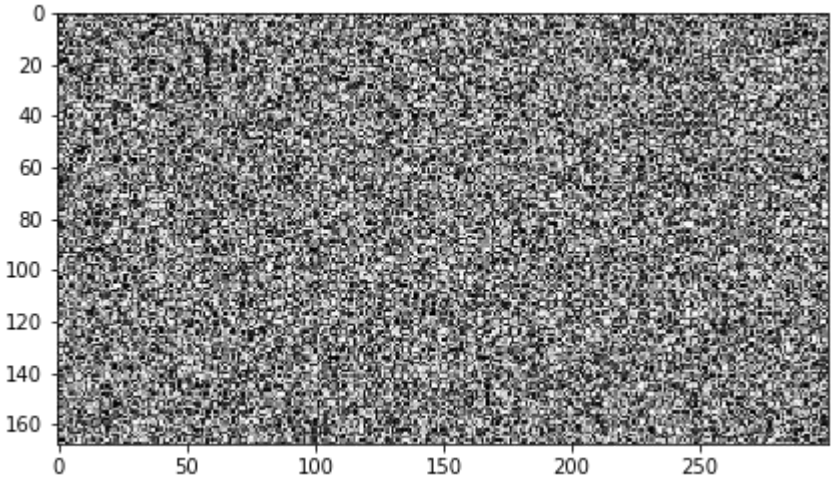
→ Converting input image to RGB [10]
→ Detecting edges of the input image [11]



→ Measurement of the size of image I.e., height and width [13]

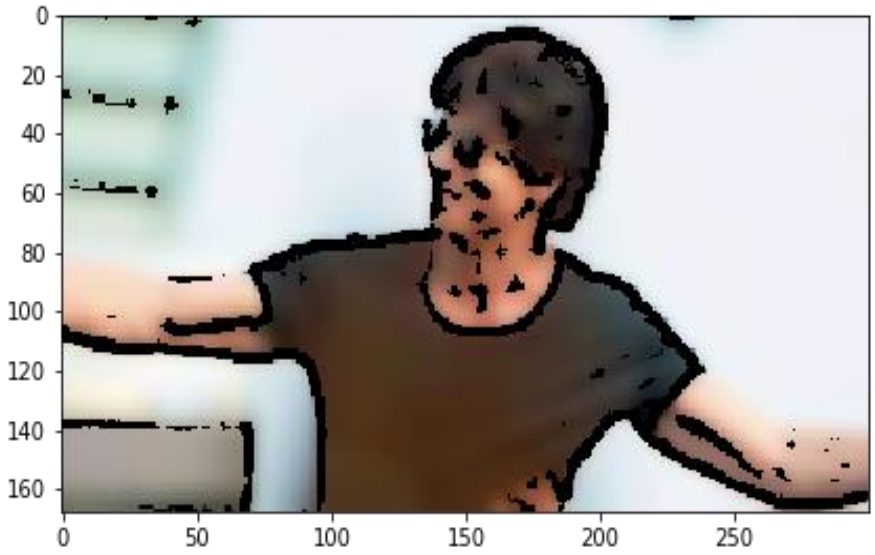


→ Displaying the key image as encrypted from using greyscale method [14,15]



→ Performing encryption and decryption using the cipher text [16]

→ Output as a cartoon image with all the encryption and decryption texts [18]



→

Thus, we see how the image provided by client is processed to give the desired output. We only needed to get the path of user image and all the encryption and decryption were performed on this image only using the cipher text algorithms. Client can perform all the needed operations on a single platform without any exchange of original data so that security does not get compromised. After doing edge detection, region smoothening, we performed encryption and decryption for providing security to the user, So, in the early stages of the operation we stored the keys. The output we get after is in greyscale method. This is further converted into a cartoon form of image.

CHAPTER 11

11. BIBLIOGRAPHY

- Cryptography - Wikipedia
- Caesar Cipher in Cryptography - GeeksforGeeks
- Digital Image Processing Basics - GeeksforGeeks
- Cartooning an Image using OpenCV - Python - GeeksforGeeks
- https://en.wikipedia.org/wiki/Python_(programming_language)
- Image encryption and decryption in public key cryptography based on MR | IEEE Conference Publication | IEEE Xplore
- Welcome To Colaboratory - Colaboratory (google.com)
- Image processing in Python? (tutorialspoint.com)
- Image Recognition in Python with TensorFlow and Keras (stackabuse.com)
- youtube.com
- neptune.ai