# PROJECT REPORT

**on**

# VISUAL CRYPTOGRAPHY

**(IMAGE ENCRYPTION & DECRYPTION)**

**(CSE V Semester Mini project)**

**2020 - 2021**


**Submitted to:**

Mr. Saumitra Chattopadhyay

(CC-CSE-E-V-Sem)

**Mentor:**

Ms. Preeti Choudhary

**Submitted by:**

Mr. Priyansu Bisht

Roll. No.: 1918571

CSE-E-V-Sem

Session: 2020-2021

**DEPARTMENT OF COMPUTER SCIENCE AND INFORMATION TECHNOLOGY**

**GRAPHIC ERA HILL UNVERSITY, DEHRADUN**

# CERTIFICATE

Certified that Mr. Priyansu Bisht (Roll No.- 1918571) has developed mini project on “Visual Cryptography ( Image encryption & decryption )” for the CS V Semester Mini Project Lab in Graphic Era Hill University, Dehradun. The project carried out by Students is their own work as best of my knowledge.

Date: 17-December-2021

( Mr. Saumitra Chattopadhyay )
**Class Co-ordinator**
**CSE-E-V-Sem**
(CSE Department)
GEHU Dehradun

Ms. Preeti Choudhary
(Mentor)
(CSE Department)
GEHU Dehradun

# ACKNOWLEDGMENT

We would like to express our gratitude to The Almighty Shiva, the most Beneficent and the most Merciful, for completion of project.

We wish to thank our parents for their continuing support and encouragement. We also wish to thank them for providing us with the opportunity to reach this far in our studies.

We would like to thank particularly our class Co-ordinator Mr. Saumitra Chattopadhyay and our respected mentor Ms. Preeti Choudhary for his patience, support, and encouragement throughout the completion of this project and having faith in us.

At last, but not the least We greatly indebted to all other persons who directly or indirectly helped us during this work.

**Mr. Priyansu Bisht**

**Roll No.- 1918571**

**CSE-E-V-Sem**

**Session: 2020-2021**

**GEHU, Dehradun**

# ABSTRACT

## Cryptography

Cryptography also knows as cryptology, is the study and practice of techniques which are used for securing data over a network or on a system. It is all about creating, developing, testing, and using certain techniques caller 'cypher' to convert useful, important and data in-need-to-be protected into something which any other normal user will consider something that can called a noise, or simply waste data which is of no use until and unless a proper decrypting 'cypher' along with its key are provided.

ENCRYPTING-CYPHER ( useful data, Pseudo-random key(k) ) ⟶ cypher text

DECRYPTING-CYPHER ( cypher text , k ) ⟶ useful data

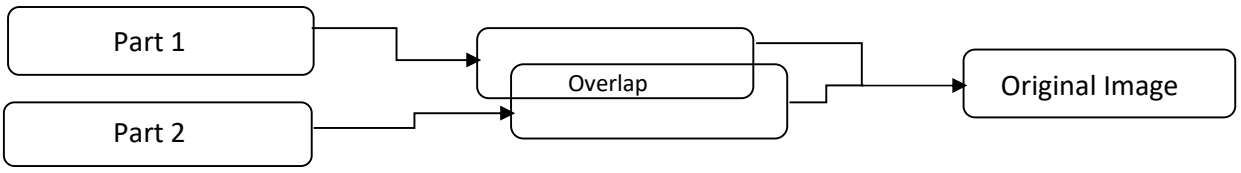
## Most used Cyphers

- AES (Advanced Encryption Standard) Cypher
- ECDSA (Elliptic Curve Digital Signature Algorithm)
- DES (Data Encryption Standard) Cypher, etc.

## Visual-Cryptography

Visual Cryptography is a cryptographic technique which make use of cryptography techniques to encrypt visual information (pictures, text, etc.) in such a way that decryption can be done mechanically, visually by overlapping images or by decrypting using a computer.

It was introduced by Moni Naor and Adi Shamir at EUROCRYPT 1994. They broke an image into 'n' parts such that only by having all 'n' parts can one decrypt the image. To decrypt an image, one has to overlap all the images and the hidden information is visible.




## Types

- X-OR (2 out of 2 scheme, 2 subpixels) Visual Cryptography
- Extensions - Extended VC
- **'k'** out of '**n'** sharing scheme
- **'n'** out of '**n'** Scheme, etc.

# ABOUT PROJECT

## Aim

To create a desktop application capable of doing all basic cryptographic actions like encrypting text, images, files & decrypting them, visual cryptography, etc.

## Introduction

- This is a project which comes under the branch of Cyber Security.
- Name of application: CryptFunct
- Language Used: Java
- Platforms Used: Apache NetBeans, VS Code, GitHub, Paint 3d, justcolourpicker.

This project is for creating a desktop application which can currently implement Text encryption & decryption. This a project which uses concepts of cryptography for securing our data. It used the cypher of AES for encryption and decryption of text.

XOR (2 of 2 scheme) is used for visual cryptography.

Can be divided into parts:

- Front End
    - Contain all the user intractable options in the projects.
    - Files include all the frames in: *com.cryptoproject.GUIFranes*
    - Every view is divided into frames, each having their own display like sign In page is showed using BaseFrame, Home page in HomeFrame.
- Back End
    - Contain all the functions that are used in background to give the desired result.
    - Files include classes under: *com.cryptoproject.FunctionalClasses*
    - Every functionality have their own Java Class like, Text Encryption and Decryption functions are all stored in TextEnDe.java file
- Resources
    - Contain all fonts, icons, images used in the project.
    - All comes under the package: *Resources.fonts, Resources.Images, Resources.Icons*

# METHODOLOGY

STEP 1: Created a blueprint using SDLC

SPEP 2: created front end Using Apache NetBeans & Java.

STEP 3: Applied AES for text encryption

AES: Advanced Encryption Standard

AES is a block cipher. The key size can be 128/192/256 bits. Encrypts data in blocks of 128 bits each. That means AES takes 128 bits as input (block) of data at a time and outputs 128 bits of encrypted cipher text corresponding to the input as output or cypher data. AES is performed using series of linked operations which in turn are used for replacing and shuffling of the input data and presentation it in the form of encrypted data.

Code Snippets:

*x = encrypt("AES/CBC/PKCS5Padding", plainText, secretKey, IV);*

*Cipher cipher = Cipher.getInstance(algorithm);*

*cipher.init(Cipher.ENCRYPT_MODE, key, iv);*

*byte[] cipherText = cipher.doFinal(input.getBytes());*

*return Base64.getEncoder().encodeToString(cipherText);*

STEP 4: Applied XOR (2 by 2 scheme) for visual Cryptography

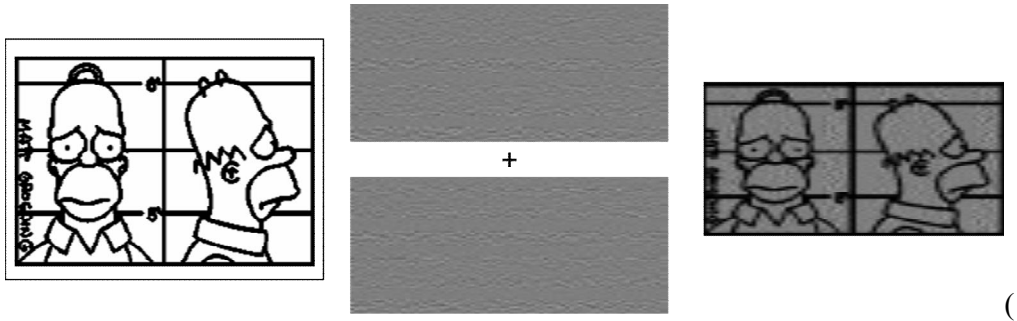
X-OR Visual Cryptography : 2 out of 2 Scheme (2 subpixels)

In k out of k, the image is visible only if all the shares are stacked together. If any share in k is lost, and remaining shares are stacked together, it will not form the image. Thus, in k out of k, all the shares are important to construct the image.

Black and white image: each pixel divided in 2 sub-pixels

Randomly choose between black and white.

The two subpixels per pixel variant can distort the aspect ratio of the original image




( Image 1 )

# ANALYSIS

## CURRENT WORKING

- A basic signup page.
- Home page which Gives access to all the functionalities in the Application
- Text Encryption: Encrypt Text Entered by AES Algorithm.
- Text Decryption: Decrypt Cypher text created in previous step by using AES Algorithm, previously used key, & IV.
- Visual Cryptography: Encryption
    - Ask for Image to be Encrypted
    - Generate Key Image based of the inserted Image
    - Encrypt both using XOR visual cryptography
    - Download Both Images to File System

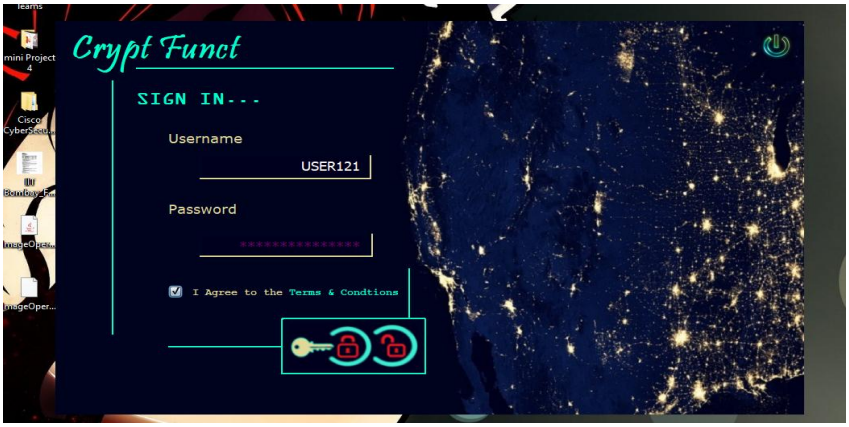
- Visual Cryptography: Decryption
    - Select both Images from File System
    - Use XOR visual Cryptography to decrypt image
    - Display & download decrypted and Overlayed Image.

## FUTURE WORKS

- Add Functionality of Image & file encryption and Decryption using AES cypher
- Add Steganography Functions
- Connect Application to a NOSQL database
- Prepare a exe setup file for application

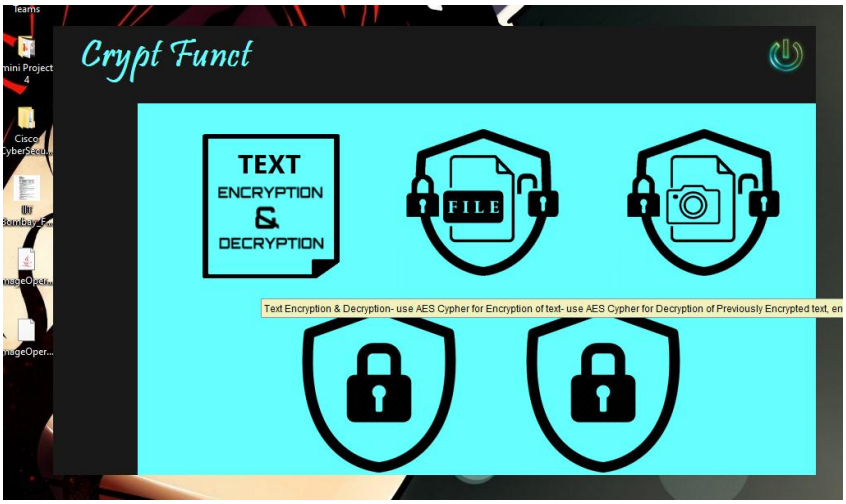
# SCREENSHOTS

- **First Sign-In page for application**




( Image 2 )

- **Home Page of Application showing different functionalities**




( Image 3 )

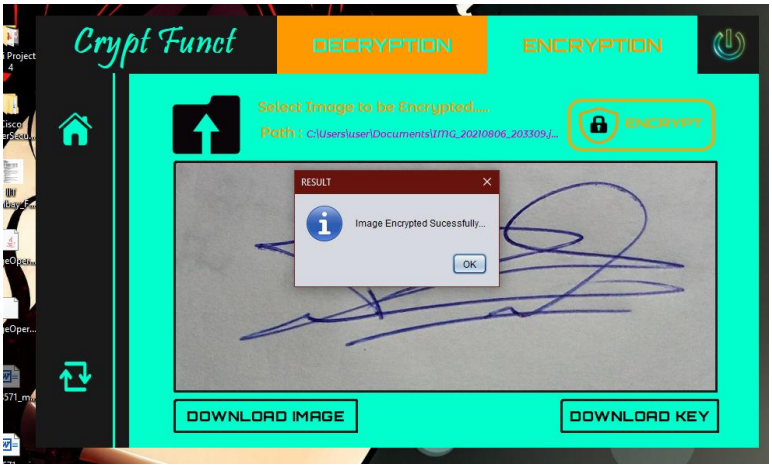
- **Opened Text Encryption Functionality**


( Image 4 )

- **Visual Cryptography Functionality, image selected and ready to encrypt.**

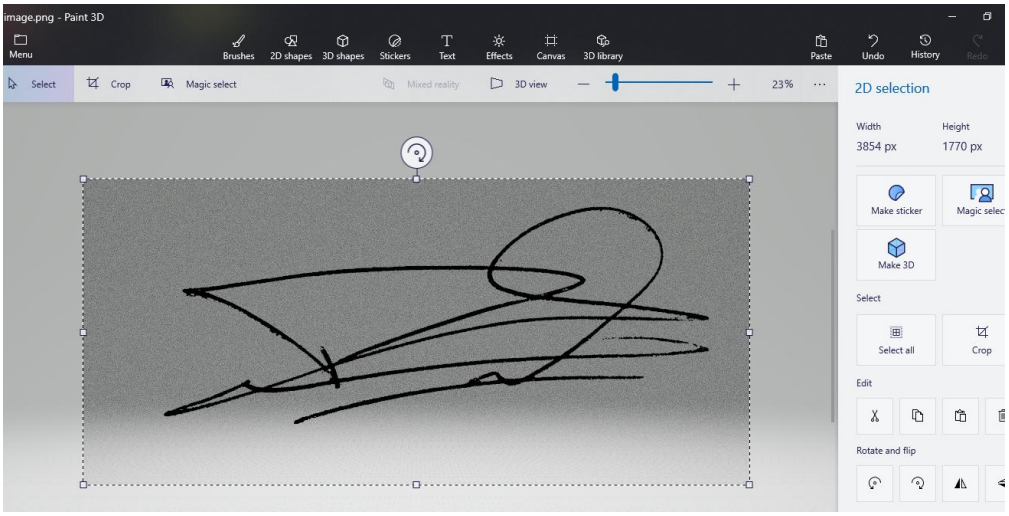

( Image 5 )

- **Visual Cryptography Performed Image and Key ready to be downloaded**




( Image 6 )

- **Original Image(b/w) obtained if key & encrypted image are Overlapped**




( Image 7 )

# REFERENCES


- Naor and Shamir, VisualCryptography, in Advances in Cryptology-Eurocrypt '94
- http://homes.esat.kuleuven.be/~fvercaut/talks/visual.pdf
- http://www.cse.psu.edu/~rsharris/visualcryptography/viscrypt.ppt
- http://netlab.mgt.ncu.edu.tw/computersecurity/2002/ppt/%E5%BD%A9%E8%89%B2%E8%A6%96%E8%A6%BA%E5%AF%86%E7%A2%BC%E5%8F%8A%E5%85%B6%E6%87%89%E7%94%A8.ppt
- http://163.17.135.4/imgra/PPT/200500022.ppt
- https://stackoverflow.com/
- https://www.w3schools.com/
- https://www.github.com
- https://www.baeldung.com/java-aes-encryption-decryption
- http://successprojects-in.blogspot.com/2013/10/visual-cryptography-schemes-for-secret.html
- https://www.freeiconspng.com/images/reload-icon