INFORMATION HIDING IN IMAGES

A MINI PROJECT REPORT

Submitted by

BARATH P	**(731619104008)**
KEERTHIRAJAN M	**(731619104024)**
PRATHAP D	**(731619104044)**
YUVARAJ A	**(731619104063)**

in partial fulfillment for the award of the degree

of

BACHELOR OF ENGINEERING

IN

COMPUTER SCIENCE AND ENGINEERING

KSR INSTITUTE FOR ENGINEERING AND TECHNOLOGY

TIRUCHENGODE – 637215

ANNA UNIVERSITY : CHENNAI 600 025

JUNE 2022

ANNA UNIVERSITY: CHENNAI 600 025

BONAFIDE CERTIFICATE

Certified that this project report **"INFORMATION HIDING IN IMAGES"** is the bonafide work of **" BARATH P (731619104008) , KEERTHIRAJAN M (731619104024) ,PRATHAP D (731619104044) , YUVARAJ A (731619104063)** who carried out the project work under my supervision.

SIGNATURE

Dr. M. VIMALA DEVI M.E.,Ph.D.,

HEAD OF THE DEPARTMENT

Associate Professor & Head

Computer Science and Engineering,

K S R Institute for Engineering and Technology,

Tiruchangode-637215

SIGNATURE

Mr. V. GOPINATH M.E.,

SUPERVISOR

Assistant Professor

Computer Science and Engineering,

K S R Institute for Engineering and Technology,

Tiruchangode-637215

Submitted for the Project work Viva-Voce held on _____

INTERNAL EXAMINER **EXTERNAL EXAMINER**

ACKNOWLEDGEMENT

We express our deep sense of gratitude to our beloved founder and chairman, **Lion Dr. K. S. RANGASAMY, MJF** , KSR Educational Institutions.We thank our vice chairman **Thiru . R . SRINIVASAN B.B.M . , M.I.S.T.E. ,** KSR Institute for Engineering and Technology, for his inspiration and moral support.

We express our heartfelt thanks to our principal, **Dr. M. VENKATESAN M.E., Ph.D.,M.I.S.T.E.,** of KSR Institute for Engineering and Technology for his Valuable support.

We express our sincere thanks to **Dr. M.VIMALADEVI M.E.,Ph.D.,** Head of the Department of Computer Science and Engineering , KSR Institute for Engineering and Technology, for her valuable guidance and constant motivation.

We express our extreme gratitute to our project coordinators **Mr. V. PRAKASHAM M.Tech.,** Assistant professor **, Mrs.A.SUHANA M.Tech.**, Assistant professor Department of Computer Science and Engineering , for providing us kind advice during the development of the project.

We wish to express our profound gratitude and thanks to our Guide **Mr.V.GOPINATH M.E.**, Assistant Professor , Department of Computer Science and Engineering , KSR Institute for Engineering and Technology , for his invaluable guidance , immense help , encouragement and providing us necessary facilities throughout this project.

ABSTRACT

Information security purported, yet another retrospected technique for secret sharing highlighted by image encryption . Encryption of images is proven a successful method to communicate confidential information for which countless procedures are unearthed. Still , it attracting researchers as usage of images in every means of digital communication has increased Cryptography embraces various encryption methods and offers four chief modes where each one found its place in many journals. This study takes cryptographic Cipher Block Chaining (CBC)mode as the fundamental footing which is manipulated in a unique fashion to achieve the goal. This script is coalescing of both Steganography and Cryptography thus ensuring enhanced security. Tentative results testify the routine and thus making it more upright of previously existing image encryption techniques.

Security is one of the core areas of study in recent days. Encryption of the image is widely known as an effective method for its secure transmission. The objective of any image encryption method is to obtain a top quality hidden image in order to keep information secret . In this paper , the procedures and schemes of different image encryption techniques that provide privacy and security are reviewed.

TABLE OF CONTENTS

LIST OF FIGURES

CHAPTER 1

INTRODUCTION

As the data exchange in electronic way is rapidly increasing, it is also equally important to protect the confidentiality of data from unauthorized access. The breaches in security affect user's privacy and reputation. The data exchanged can be text, image , audio , video etc. Each type of data has its own features different techniques are used to protect confidential image data from unauthorized access. Hence encryption of data is done to confirm security in open networks such as the internet where the multimedia applications are ever growing. Cryptography is the study of techniques for secure communication in the presence It deals with problems like encryption, authentication and key distribution to name a few. Image encryption is a technique that provides security to images by Converting the original image into an image which is difficult to understand. Applications of image encryption can have extended to military communication, multimedia systems, medical science, telemedicine, internet communication etc. for encryption of image is to consider a 2D image as a 1D data stream and this stream is encrypted with any textual based cryptosystem. This approach is called nave approach. For text, small bit rate audio, image and video files that can be sent over a fast-dedicated channel, this approach is suitable. Unfortunately, these encryption algorithms may not satisfy for different image data types like JPEG, PNG, BMP, etc...An image when decrypted contains small distortion and is usually acceptable because of the characteristic of human perception.

1.1 PROBLEM STATEMENT

To assess the security needs of an organization effectively, the manager responsible for security needs some systematic way of defining the requirements for security an characterization of approaches to satisfy those requirements. One approach is to consider three aspects of information security:

Security attack – Any action that compromises the security of information owned by an organization.

Security mechanism – A mechanism that is designed to detect, prevent or recover from a security attack.

Security service – A service that enhances the security of the data processing systems and the information transfers of an organization. The services are intended to counter security attacks and they make use of one or more security mechanisms to provide the service.

1.2 OBJECTIVES

Nowadays , information security is becoming more important in data storage and transmission . Images are widely used in different - different processes . Therefore , the security of image data from unauthorized uses is important. Image encryption plays a important role in the field of information hiding.Image encryption method prepared information unreadable . Therefore, nohacker or eavesdropper , including server administrators and others, have access to original message or any other type of transmitted information through public networks such as internet.

Ability to get the pixels of the original image. Create a strong encryption image such that it cannot be hacked easily . Faster encryption time such that encrypted image is transferred faster to the person. Perfection in the original image we obtain after decrypting it.

Cryptography supports a number of security aims to provide the privacy of information , non - alteration of information and so on. Because of the high security benefit of cryptography it is broadly used today . There are the various goals of cryptography which are as follows :

Confidentiality : Information in computer is sent and has to be approached only by the authorized party and not by anyone else . The principle of confidentiality represent that only the sender and the intended recipient(s) should be able to make the content of a message. Confidentiality have negotiated if an unauthorized person is able to make a message.

Authentication: Authentication is any process by which it can test that someone is who they claim they are.This generally includes a username and a password, but can contain some other approach of demonstrating identity, such as smart card, retina scan, voice identification, or fingerprints . Authentication is same as showing the drivers license at the ticket counter at the airport.

Integrity : It can only the authorized party is enables to change the transmitted information . No one in between the sender and receiver are enabled to modify the given message.

Non-Repudiation : It provides that neither the sender , nor the receiver of message should be capable to decline the transmission. Non-repudiation defines that a person who sends a message cannot decline that sent it and, conversely, that a person who has received a message cannot decline that received it. Furthermore these technical components, the conceptual reach of information security is broad and multifaceted.

Access Control : The principle of access control determines who should be capable to access what. For instance, it should be able to represent that user A can view the information in a database, but cannot update them . User A can be enables to create updates as well.

CHAPTER 2

LITERATURE SURVEY

2.1 IMAGE ENCRYPTION WITH BLOCK SHUFFLING AND CHAOTIC MAP

A novel image encryption based on row-column, masking and main diffusion processes with hyper chaos. (2015) In this paper, a novel algorithm for image encryption based on the hyper-chaotic system is proposed.The algorithm consists three main sections. In the first Section the rows and columns of the image are encrypted using a row-column algorithm.In the Second section employs masking Process which is applied to each quarter of the image that is to be encrypted,using that sub-image data and one of the other sub-images and the average data of other quarters of image. Finally , in the last diffusion section , the four most significant bit planes will be encrypted.

2.2 FOUR DIMENSIONAL HYPERCHAOTIC FINANCE SYSTEM

An image encryption scheme based on a new hyperchaotic finance system. (2015) In this paper, a new four-dimensional hyperchaotic finance system based on a chaotic finance system is presented. The chaotic sequence is generated Runge–Kutta method, the key sequence is generated by chaotic sequence comparison. The key sequence is used for image encryption with relation to plaintext

2.3 2D SINE LIGISTIC MODULATION MAP

2D Sine Logistic modulation map for image encryption. (2015) In this paper, introduce a new two dimensional Sine Logistic modulation map (2D-SLMM) which is derived from the Logistic and Sine maps. To investigate its applications, they propose a chaotic magic transform to efficiently change the image pixel positions. 2D-SLMM with CMT,we further introduce a new image encryption algorithm . They use the trajectory , Lyapunov exponent, Lyapunov dimension and Kolmogorov entropy to evaluate its chaotic performance.

2.4 COLOR BYTE SCRAMBLING TECNIQUE

A colour byte scrambling technique for efficient image encryption based on combined chaotic map: Image encryption using combined chaotic map. (2016) In this paper, an image encryption scheme based on colour byte scrambling technique is proposed by using Logistic map and Ikeda map.The proposed scheme is using Logistic map for generating permutation sequence to shuffle the colour bytes (confusion) and used for generating maskingsequence to change the value of the colour bytes (diffusion) of the 24-bit colour image.

2.5 IMAGE ENCRYPTION WITH BLOCKSHUFFLING AND CHAOTIC MAP

(2015) In the first step, they scramble image blocks to achieve initial encryption. In the second step , generate a set of secret matrices by a chaotic map and Arnold transform.They adopt the skew tent chaotic map for randomized secret matrix generation. Finally, encrypt each block by calculating exclusive OR operation between the corresponding elements of a random secret matrix and the image block.

CHAPTER 3

SYSTEM ANALYSIS

3.1 EXISTING SYSTEM

- There is no option to try all the algorithms together in one system.
- There is no privilege for the user to send the encrypted message to other person as a mail.
- There is no database storage for the existing system. Further retrieval of the code is not possible.
- The system do no t check for any authentication . Any user can encrypt and decrypt.
- It is easy for an intruder (third party) to access the text and he can make his ownChanges in it.

DISADVANTAGES

- Pixels obtained after Gaussian elimination is fully distorted , so the key is needed to obtain original image because it's hard to crack that encrypted form.
- Both encryption and decryption have been processed by clicking the encryption button. there will be no availability for decryption button.
- Efficiency of our algorithm is 2/3 * O(n^3). Decryption takes 4 times larger the time taken by Encryption.

3.2 PROPOSED SYSTEM

- It hides the message and your privacy is safe.
- You can write whatever you want and however you want (any theme any symbol for the code) to keep your code a secret by using encryption .
- The system CRYPTO corner contains a data base and the data can bestored and retrieved easily and also system provides email facility.
- The person who got the mail has to login to the CRYPTO corner and decrypt it.
- The system checks for security . If the user type incorrect password for three time. Then the system will automatically block the user and the user gets messageas unauthorized access.

ADVANTAGES

- Simplicity: It's simpler, cheaper.
- Ratio: Encryption takes ¼ th time the decryption process takes.
- Robust: The encrypted image is hard to hack to obtain the original image.
- Pixels obtained after Gaussian elimination is fully distorted , so the key is needed to original image because it's hard to crack that encrypted form.
- We have reduced time taken by encryption by smartly by updating rowexchanges using another matrix. So basically it's a Space for time tradeoff.

CHAPTER 4

SYSTEM SPECIFICATION

4.1 HARDWARE REQUIREMENTS

This section gives the details and specification of the hardware on which the system is expected to work.

Processor	:	Intel dual core processor
RAM	:	2 GB SD RAM
Monitor	:	17” Color
Hard disk	:	500 GB
Keyboard	:	Standard 102 Keys
Mouse	:	Optical mouse

4.2 SOFTWARE REQUIREMENTS

This section gives the details of the software that are used for the development.

Operating System	:	Windows 10 Pro
Environment	:	JUPYTER
Language	:	React JS

CHAPTER 5

SYSTEM TESTING

TESTING

Software testing is an investigation conducted to provide stakeholders with information about the quality of the product or service under test. Software testing can also provide an objective, independent view of the software to allow the business to appreciate and understand the risks of software implementation. Test techniques include various types of testing, but are not limited to the process of executing a program or application with the intent of finding software bugs (errors or other defects).

TYPES OF TESTING

1. Unit testing
2. Integration testing
3. System testing
4. Acceptance testing
5. Validation testing

5.1 UNIT TESTING

Unit testing is a level of software testing where individual units/ components of software are tested. The purpose is to validate that each unit of the software performs as designed. A unit is the smallest testable part of any software. It usually has one or a few inputs and usually a single output. Unit testing increases confidence in changing/ maintaining code. Codes are more reusable.

5.2 INTEGRATION TESTING

Integration testing is the phase in software testing in which individual software modules are combined and tested as a group. Integration testing takes as its input modules that have been unit tested, groups them in larger aggregates , applies tests defined in an integration test plan to those aggregates, and delivers as its output the integrated system ready for system testing.

5.3 SYSTEM TESTING

System testing of software or hardware is testing conducted on a complete, integrated system to evaluate the system's compliance with its specified requirements. System testing is performed on the entire system in the context of a Functional Requirement Specification(s) (FRS) and/or a System Requirement Specification (SRS).

5.4 ACCEPTANCE TESTING

Acceptance testing is a level of software testing where a system is tested for acceptability. The purpose of this test is to evaluate the system's compliance with the business requirements and assess whether it is acceptable for delivery.

5.5 VALIDATION TESTING

Verification and Validation (V&V) is the process of checking that a software system meets specifications and that it fulfills its intended purpose. It may also be referred to as software quality control. It is normally the responsibility of software testers. Software validation checks that the software product satisfies or fits the intended use (high-level checking), i.e. The software meets the user requirements, not as specification artifacts or as needs.

CHAPTER 6
SYSTEM FLOW DIAGRAM

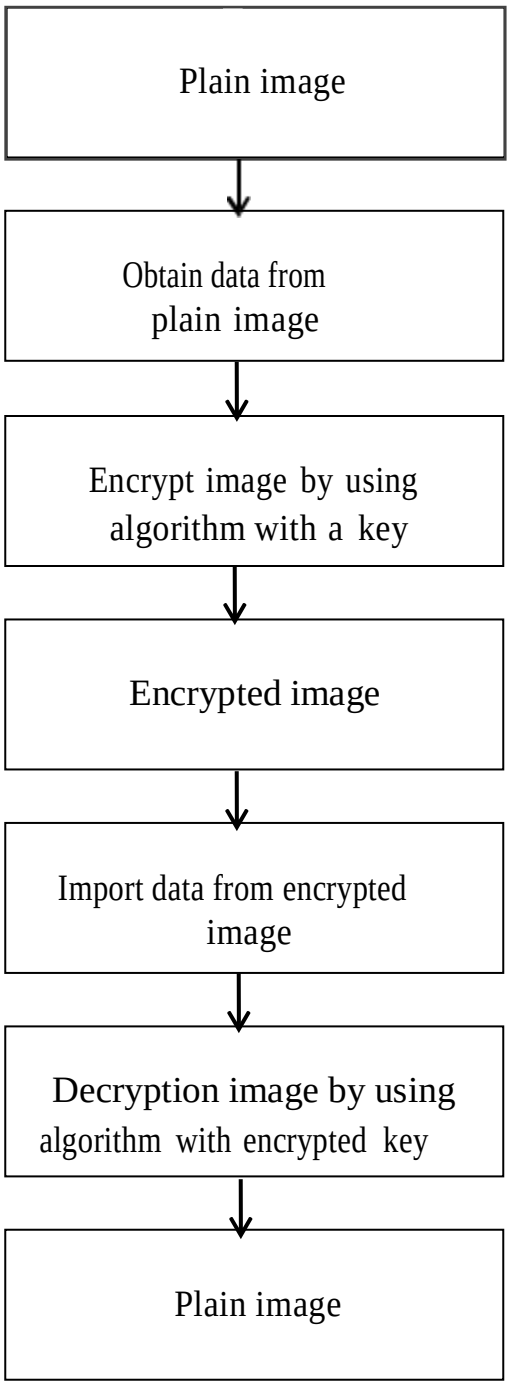


FIGURE 6.1

CHAPTER 7

IMPLEMENTATION

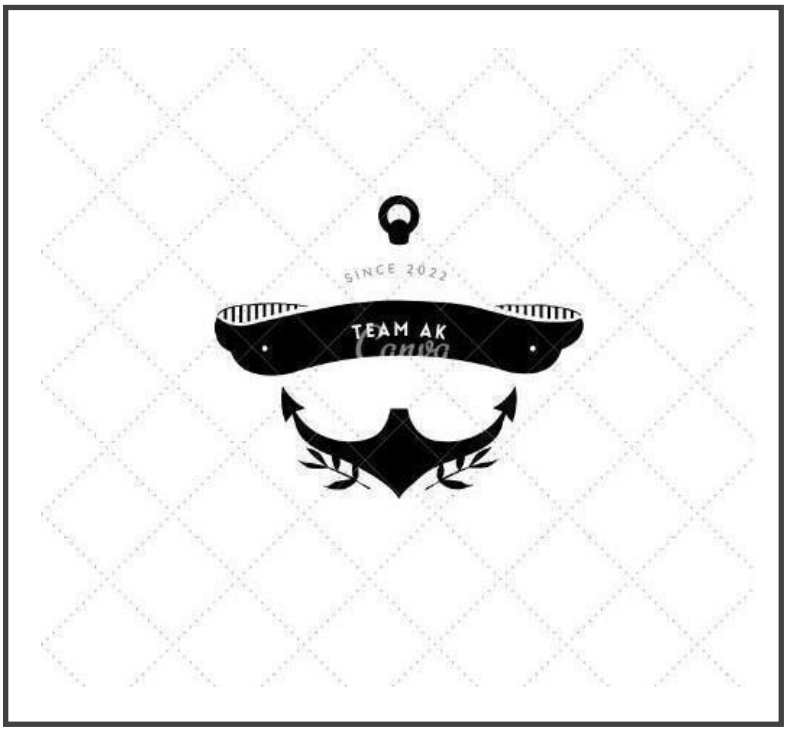
7.1 SOURCE CODE

```
from tkinter import *
from tkinter import filedialog
root=Tk()
root.geometry("200x200")
def encrypt_image():
    file1=filedialog.askopenfile(mode='r',filetype=[('jpg    file','*.jpg')])
    if file1 is not None:
        file_name=file1.name
        key=entry1.get(1.0,END)
        print(file_name,key)
        fi=open(file_name,'rb')
        image=fi.read()
        fi.close()
        image=bytearray(image)
        for index,values in enumerate(image):
            image[index]=values^int(key)
        fi1=open(file_name,'wb')
        fi1.write(image)
        fi1.close()
```

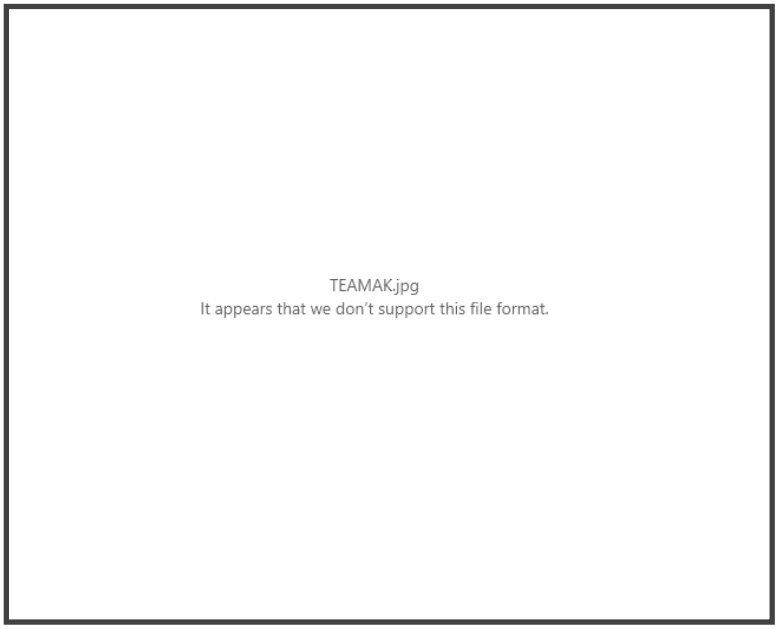
```
def     decrypt_image():
    file1=filedialog.askopenfile(mode='r',filetype=[('jpg  file','*.jpg')])
if file1 is not None:
        file_name=file1.name
        key=entry1.get(1.0,END)
        print(file_name,key)
        fi=open(file_name,'rb')
        image=fi.read()
        fi.close()
        image=bytearray(image)
        for index,values in enumerate(image):
            image[index]=values^int(key)
        fi1=open(file_name,'wb')
        fi1.write(image)
        fi1.close()
b1=Button(root,text="Encrypt",command=encrypt_image)
b1.place(x=50,y=10)
b2=Button(root,text="Decrypt",command=decrypt_image)
b2.place(x=100,y=10)
entry1=Text(root,height=1,width=10)
entry1.place(x=50,y=50)
root.mainloop()
```

7.2 SCREENSHOTS

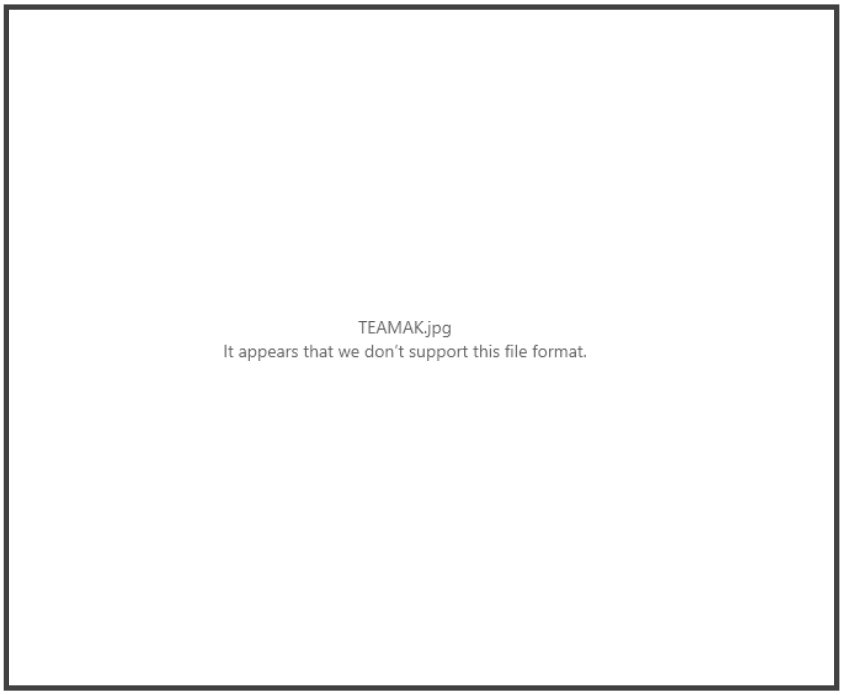
7.2.1 IMAGE BEFORE THE ENCRYPTION



7.2.2 IMAGE AFTER THE ENCRYPTION

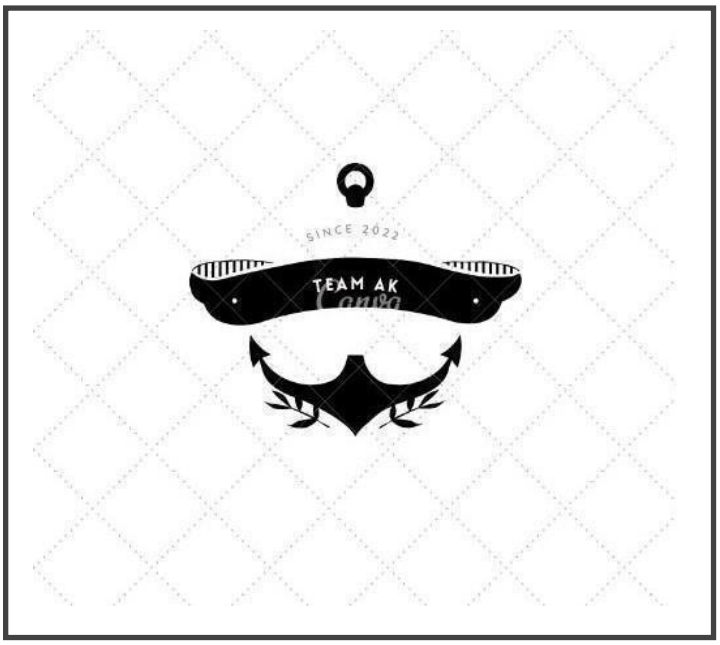


7.2.3 IMAGE BEFORE THE DECRYPTION

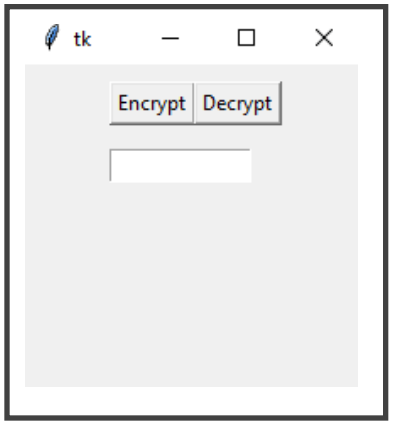


7.2.4 IMAGE AFTER THE DECRYPTION

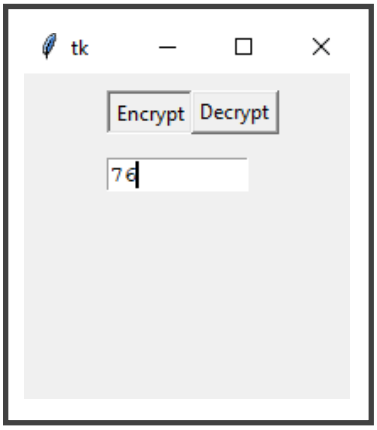
7.2.5 ENCRYPTION PROCESS SCRENSHOTS:



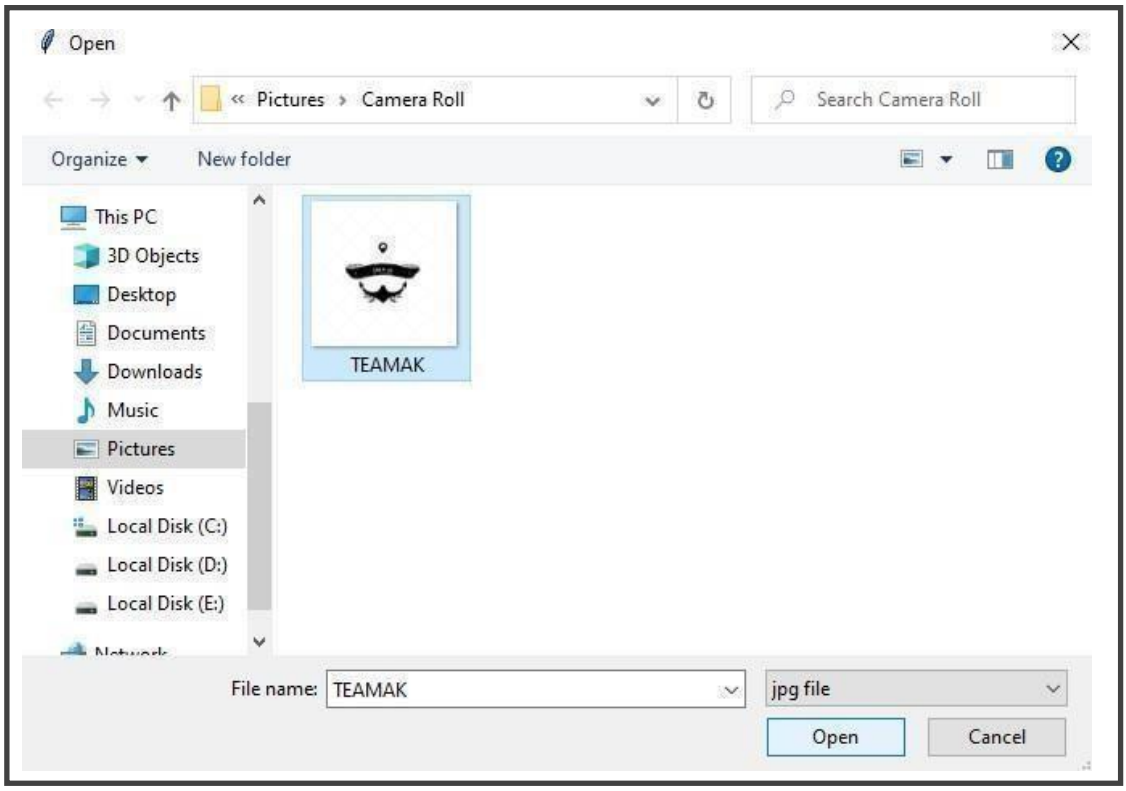
7.2.5.1 Image before encryption



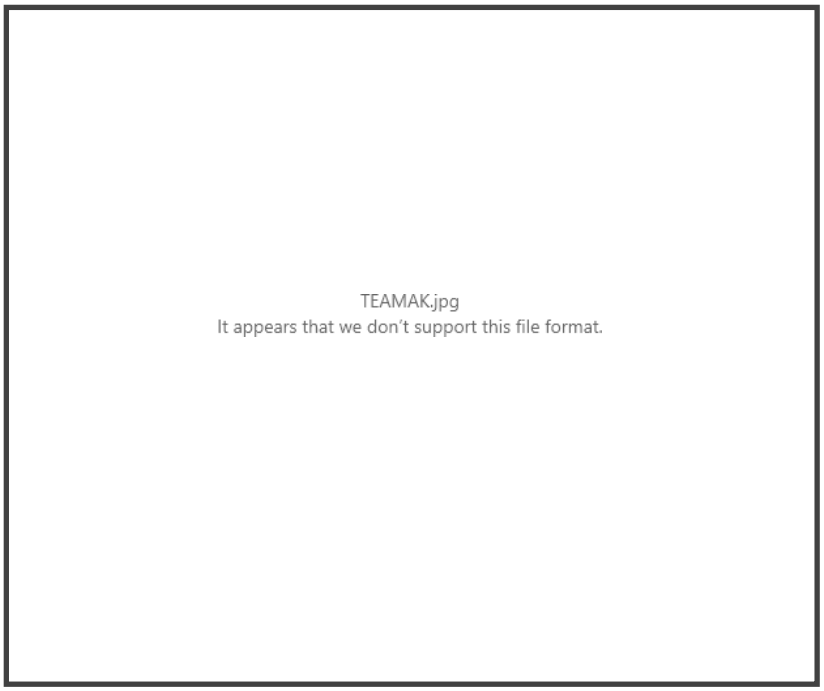
7.2.5.2 Input entering box for encryption and decryption



7.2.5.3 Giving key value for encryption

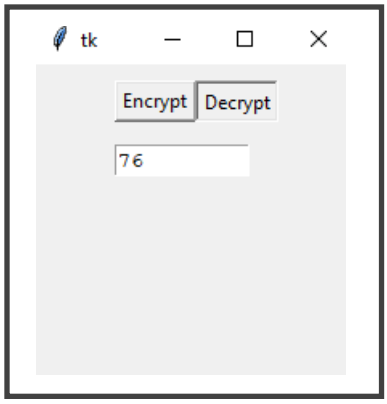


7.2.5.4 File selection for Encryption

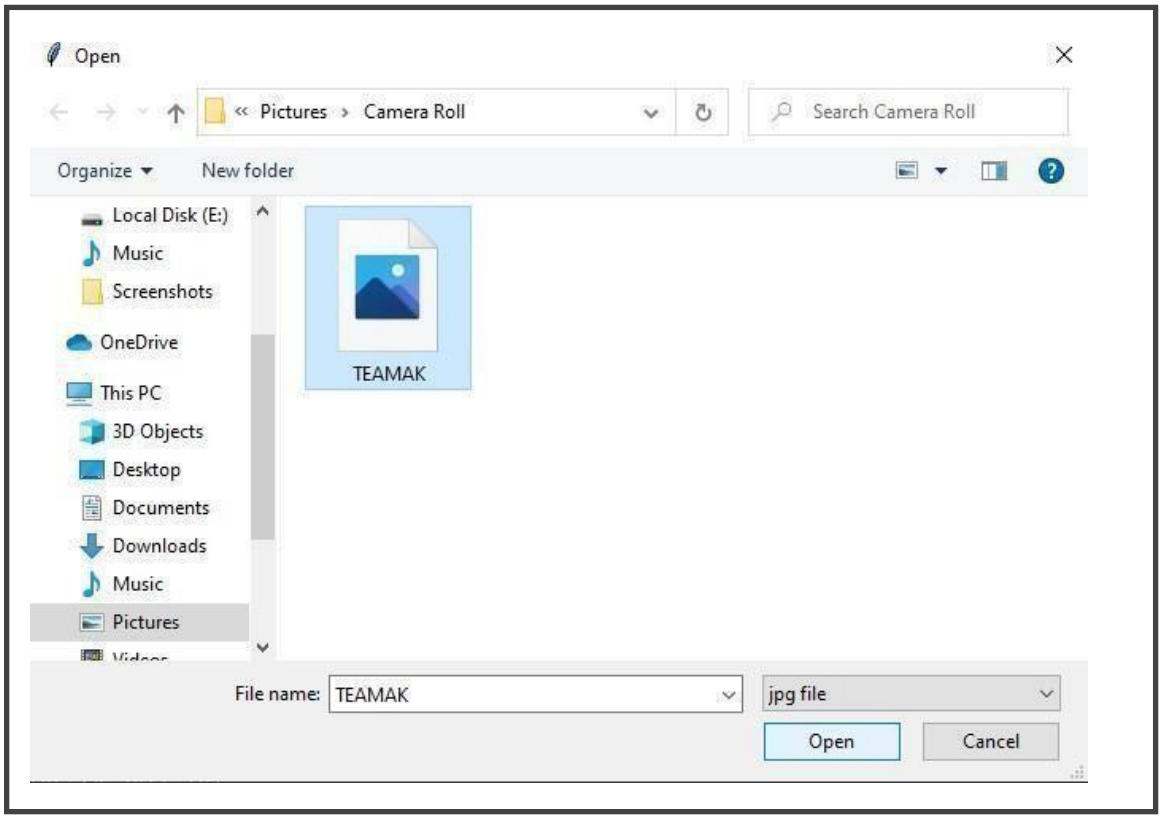


7.2.5.5 Image after the encryption process

7.2.6 DECRYPTION PROCESS SCRENSHOTS:



7.2.6.1 Giving key value for decryption



7.2.6.2 File selection for Decryption

7.2.6.3 Image after the decryption process

CHAPTER 8

CONCLUSION

In this paper,large portions of the current essential image encryption methods have been exhibited and examined. In this review report , at first the stress have been made on officially existing image encryption algorithms in light of the fact that the most ideal method for ensuring media information like images is by method for the gullible algorithm; i.e., by scrambling the whole sight and sound bit succession utilizing a quick conventional cryptosystem. A great part of the past and momentum exploration targets scrambling just a deliberately choose piece of image bit - stream keeping in mind the end goal to decrease the computational burden and yet keep the security level high. Huge numbers of the proposed plans could just accomplish moderate to low level of security , which may discover applications in which quality debasement is favored over outright security. Then again, just few of the proposed strategies guarantee to attain considerable security, which is the prime prerequisite in numerous media applications . Secondly, we evaluated a wide-run of image encryption algorithms and ordered them on the premise of full and partial image encryption procedures under spatial space, frequency domain and hybrid domain categories.

In the process, of this survey, a few perceptions were made , which are that full encryption plan guarantees high state of security of encoded information because of the way that they encode the whole image , however much time is used in such a procedure . On account of selective image encryption , just a locale or some piece of the image is scrambled . The time used in encoding the region of investment is less in contrast to the full encryption procedures.

Hence , the partial encryption scheme is more suitable for constant applications . Therefore , partial image encryption scheme proved to be encouraging in term of encryption time, attaining an encryption procedure that adjusts security with transforming time for ongoing applications is still a challenge for researcher in image encryption . On the other hand, some key elements , for example , the sort of information to be encoded, the rate of the information that must be ensured and the measures put set up to ensure the information from cryptanalytic attack, when considered in the configuration of a continuous image encryption procedure might be a reasonable answer for ongoing image encryption issues.

REFERENCES

i. Norouzi, Benyamin, et al. "A novel image encryption based on row-column, masking and main diffusion processes with hyper chaos." Multimedia Tools and Applications 74.3 (2015):781-811.

ii. Tong, Xiao-Jun, et al. "An image encryption scheme based on a newhyperchaotic finance system." Optik-International Journal for Light and Electron Optics 126.20 (2015): 2445-2452.

iii. Hua, Zhongyun, et al. "2D Sine Logistic modulation map for image encryption." Information Sciences 297 (2015): 80-94.

iv. Suri, Shelza, and Ritu Vijay. "An implementation and performance evaluation of an improved chaotic image encryption approach. " Advances in Computing , Communications and Informatics (ICACCI), 2016 International Conference on. IEEE, 2016.

v. Zhang, Xuanping, et al. "A chaos-based image encryption scheme using 2D rectangular transform and dependent substitution." Multimedia Tools and Applications 75.4 (2016): 1745-1763.

vi. Parvees, MY Mohamed, et al. " A colour byte scrambling technique for efficient image encryption based on combined chaotic map: Image encryption using combined chaotic map." Electrical , Electronics, and Optimization Techniques (ICEEOT) , International Conference on. IEEE, 2016.

vii. Tong, Xiao-Jun, et al. "A fast encryption algorithm of color image based on four dimensional chaotic system . " Journal of Visual Communication and Image Representation 33 (2015): 219-234.

WEB REFERENCE

.

- https://1000projects.org/cryptography-project-report.html
- https://scialert.net/fulltextmobile/?doi=jai.2014.123.135
- https://www.sciencedirect.com/science/article/pii/S1877050915013782
- https://www.researchgate.net/publication/338548874_Image_Cryptography_A_Survey_towards_its_Growth