[Project Report Final.pdf](https://my.plagramme.com/accset/chreportview/hypGLj4H)

[(https://my.plagramme.com/accset/chreportview/hypGLj4H)](https://my.plagramme.com/accset/chreportview/hypGLj4H)

Originality Risk of the plagiarism

Diagram

Description automatically generatedLOWEST

Paraphrase

### 2%

Improper Citations

### 0%

Matches

### 11

A

PROJECT Report on File Camouflage

Submitted for partial fulfillment of award of BACHELOR OF TECHNOLOGY

Degree In

Information Technology By

STUDENT

Naveen Kumar Varshney-1900300130063 Arun Kumar-1900300130008 Md Sadique Rashid-1900300130057 Nikhil Saini -1900300130064

Under the Supervision of Ms. Jasneet Kaur

INDERPRASTHA ENGINEERING COLLEGE, GHACZlIAicBkADo,nDrt. hAeP rJeAdBDaUrLeKaALtAoMinTEsCpHeNcICtAL UNIVERSITY

# the source of plagiarism

LUCKNOW, UTTAR PRADESH

(SESSION:2022-23)

## Plagramme

This is to certify that the Project Report entitled “…… File Camouflage”

which is submitted by Naveen Kumar Varshney, Nikhil Saini, Arun Kumar, Md Sadique Rashid…in partial fulfillment of the requirement for the award of degree

B. Tech. in Department of ....Information Technology of Dr. A.P.J. Abdul Kalam Technical University, Lucknow, is a

record of the candidate's own work carried out by him under my supervision. The matter embodied in this thesis is original and has not been submitted for the award of any other degree.

Date: 22-12-2023

(Ms. Jasneet kaur ) Designation: Assistant Professor Address: IPEC, Ghaziabad

Acknowledgement

We take this opportunity to thank our teachers and friends who helped us throughout the project.

First and foremost, I would like to thank my guide for the project (Ms. Jasneet kaur, Assistant professor, Information Technology Department) for her/his valuable advice and time during development of project.

We would also like to thank Dr. Pooja Tripathi (HOD, Information Technology Department) for his constant support during the development of the project.

Name: Naveen Kumar VarshneyName: Nikhil Saini Roll No. 1900300130063Roll No. 1900300130064

SignatureSignature

Name: Md Sadique RashidName: Arun Kumar Roll No. 1900300130057Roll No. 1900300130018

SignatureSignature

Declaration

I hereby declare that this submission is my own work and that, to the best of my knowledge and belief, it contains no material previously published or written by another person nor material which to a substantial extent has been accepted for the award of any other degree or diploma of the university or other institute of higher learning, except where due acknowledgment has been made in the text.

Name: Naveen Kumar VarshneyName: Nikhil Saini Roll No. 1900300130063Roll No. 1900300130064

SignatureSignature

Name: Md Sadique RashidName: Arun Kumar

# Click on the red area to inspect

Roll No. 1900300130057Roll No. 1900300130t0h18e source of plagiarism

SignatureSignature

## Plagramme

The word steganography means” covered in hidden writing”. The object of steganography is to send a message through some innocuous carrier (to a receiver while preventing anyone else from knowing that a message is being sent to all. Computer based steganography allows changes to be made to what are known as digital carriers such as images or sounds.

The changes represent the hidden message, but result if successful in no discernible change to the carrier. The information may be nothing to do with the carrier sound or image or it might be information about the carrier such as the author or a digital watermarking or fingerprint.

In steganography information can be hidden in carriers such as images, audio files, text files, and video and data transmissions. When message is hidden in the carrier a stego carrier is formed for example a stego- image. Hopefully it will be perceived to be as close as possible to the original carrier or cover image by the human senses.

Images are the most widespread carrier medium. The are used for steganography in the following way. The message may firstly be encrypted. They are used for steganography in the following way. The message may firstly be encrypted. The sender embeds the secret message to be sent into a graphic file. This results in the production of what is called stego-image. Additional secret data may be needed in the hiding process e.g. a stegokey etc. This stego-image is then transmitted to the recipient.

KEYWORDS:

Stegnography, Images, Hiding, Web application, Online, Text Files, Message, Encryption, Extraction. Role and Responsibility:

The growing use of the Internet has led to a continuous increase in the amount of data that is being exchanged and storage in various digital media. This has led to some unexpected cases involving both benevolent and malevolent usage of digital data.

With the ever increasing amount and variety of data to be stored and transmitted in various mediums, the specification of security which has to be established at various levels of medium access and the accompanying issues of authentication and authorization has become a critical factor.

Various stenographic, watermarking and data-embedding algorithms have usually manipulated the actual data in order to either hide any coveted information or to provide some level of access control over the medium. The mediums are usually images, video, audio etc., wherein specific portions or the overall space is usually ‗corrupted‘ with

‗significant‘ data. This paper is an attempt to bring out the significance of the steganographic techniques that are employed in information processing algorithms for data security. It deals with the problem of data security, focusing mainly on images, and tries to state the various properties and characteristics that the steganographic algorithms should possess.

# Click on the red area to inspect the source of plagiarism



2011-2022 © All rights reserved by plagramme.com

## Plagramme