**ABSTRACT**

This project explores the use of steganography to hide data within images. Steganography is the practice of concealing a message within another message or object. This project specifically looks at using images as a means to hide data. The use of images for steganography offers a few advantages over other methods, such as being able to hide a large amount of data within a single image, and the fact that images are ubiquitous and easily shared. There are a few challenges that come with using images for steganography as well, such as the need for specialized software to encode and decode the hidden data, and the fact that the hidden data can be easily detected if the image is scrutinized. Despite these challenges, steganography offers a powerful tool for hiding data in plain sight, and this project seeks to explore the use of images for steganography.

Information can be concealed in digital audio and picture files using steganography. It functions by inserting invisible data into empty spaces in ordinary digital files. Two files are required to embed concealed information into an image: the secret message file and the cover image file. A communication could be in cypher text or plain text (or another image). The cover image and the secret message form a stego image when merged. The message may be concealed and decoded using a stego-key or password. For steganography, specialised software is required. We will examine two programmes that conceal text behind graphics in this lesson.

**KEYWORDS:** Steganography and cryptography, File Cryptography, Image Steganography, Audio Steganography, Base64 Steganography, Encryption and Decryption

**CHAPTERS CHAPTER NAME PAGE NO**

**ABSTRACT v**

**LIST OF FIGURES viii**

**LIST OF ABBREVIATIONS ix**

**1 INTRODUCTION 1**

1.1 Introduction 1

1.2 Statement of problem 1

1.3 Problem statement is of interest 2

1.4 Objective of the study 3

1.5 Research of questions 3

**2 LITERATURE SURVEY 4**

2.1 Literature Review- Ⅰ 4

2.2 Literature Review- ⅠI 5

2.3 Literature Review- Ⅲ 6

2.4 Literature Review- Ⅳ 7

2.5 Literature Review- Ⅴ 8

**3 SYSTEM ANALYSIS 10**

3.1 Existing System 10

3.1.1 Disadvantages 11

3.2 Proposed System 11

3.2.1 Advantages 12

**4 REQUIREMENTS SPECIFICATIONS 13**

4.1 Html 13

4.2 Bootstrap 13 4.3 Css 14

4.4 Python 14

4.5 Javascript 15

4.6 Hardware Requirements 15

**5 METHODOLOGY 16**

5.1 Selecting type of Encryption 16

5.2 File Encryption and Decryption 17

5.3 Image Encryption, Decryption 18

5.4 Audio Encryption, Decryption 20

5.5 Base64 Encryption, Decryption 22

**6 SYSTEM DESIGN 24**

6.1 Architecture Diagram 24

6.1.1 File Encryption 24

6.1.2 Image Encryption 25

6.1.3 Audio Encryption 26

6.1.4 Base64 Encryption 27

6.2 How overall system works 28

**7 Result and Discussion 30**

**8 Conclusion & Future work 33**

**9 APPENDICES 36**

9.1 Appendix A-Source Code 36

**10 Reference 47**

**LIST OF FIGURES**

### **Fig No** **TITLE Page No**

5.1 Main page 9

5.2.1 File main page 21

5.2.2 File Encoder 25

5.3.1 Image page 25

5.3.2 Image encode 26

5.3.3 Image decode 26

5.3.4 Image encrypt 27

5.4.1 Audio page 28

5.4.2 Audio encoder 29

5.4.3 Audio decoder 29

5.5.1 Base64 main page 30

5.5.2 Base64 Example 32

5.5.3 Base64 Example 32

6.1 Block diagram of file 35

6.1.2 Block diagram of image 36

6.1.3 Block diagram of audio 37

6.1.4 Block diagram of base64 38

6.2 System design 39

7.1 Home site 40

7.2 File site 41

7.3 Image site 42

7.4 Audio site 43

7.5 Base64 site 44

**LIST OF ABBREVIATIONS**

|  |  |  |
| --- | --- | --- |
| **S NO** | **ABBREVIATIONS** | **DESCRIPTION** |
| 1 | Opencv | Computer Vision |
| 2 | Stego | Steganography |
| 3 | DB | Database |
| 4 | HTML | Hyper Text Markup Language |
| 5 | CSS | Cascading Style Sheets |

**CHAPTER 1**

**INTRODUCTION**

**1.1 Introduction**

Steganography is a technique for obfuscating secret information by enclosing it in a regular, non-secret file or safeguard data. Greek roots steganos (hidden or covered) and graph are combined to get the word steganography (meaning to write). By using codes, cryptography is a technique for encrypting data and communications so that only the intended audience can read and comprehend it.

## In computer science, the term "cryptography" refers to safe information and communication methods that use mathematical principles and a system of calculations based on rules, or "algorithms," to change messages in ways that are challenging to read. These deterministic algorithms are employed in the creation of cryptographic keys, digital signature, online browsing on the internet, and private communications like email and credit card transactions.

**1.2 STATEMENT OF THE PROBLEM**

The main goal of this problem is to establish a secure transfer of information between two users. The data is secured by encrypting the data. In contemporary digital steganography, information is first encrypted or otherwise obscured, and then it is inserted using a special algorithm into information that is part of a certain file format, such a JPEG image, audio file, or video file. There are numerous techniques to insert the hidden message into regular data files. One method is to conceal data in bits that correspond to consecutive rows of the same colour pixels in a picture file. The output will be an image file that looks just like the original image but has "noise" patterns of regular, unencrypted data. This is accomplished by applying the encrypted data to this redundant data in some covert manner.

**1.3 WHY THE PROBLEM OF INTEREST**

With an ever-increasing amount and variety of data to be kept and transferred in multiple mediums, the security specification that must be created at various levels of medium access, as well as the associated issues of authentication and authorization, has become a significant consideration. Various stenographic, watermarking, and data-embedding algorithms have typically manipulated the actual data in order to either conceal or provide some level of access control over the medium. The mediums are typically photos, video, music, and so on, with selected areas or the entire space being "corrupted" with "significant" data. This research attempts to highlight the significance of steganographic techniques used in information processing algorithms for data security. It addresses the issue of data security, with a focus on images, and attempts to explain the many traits and characteristics that steganographic methods should have.

The increased use of the Internet has resulted in an increase in the volume of data transferred and stored in various digital mediums. This has resulted in several surprising examples involving both benign and malignant uses of digital data. Security and authentication approaches such as digital watermarks, stenographic methods, and other data embedding algorithms have made significant contributions to improving various security characteristics and preserving intellectual property. In this regard, stenographic techniques have shown to be the most effective in assisting in the concealment of crucial information in ways that avoid the detection of hidden signals. Steganography hides the data so that it cannot be noticed, whereas cryptography scrambles the message so that it cannot be comprehend.

**1.4 OBJECTIVE OF THE STUDY**

The main goals to be achieved upon completion of this study are:

* **To hide messages** in such a way that no one apart from the intended recipient even knows that a message has been sent.
* To secure the sensitive information.
* Hide data in different types of encryptions and decryptions of different forms.
* Make it so strong that no one can break the encryption of the sensitive data and access it.

**1.5 RESEARCH QUESTIONS**

* Why should everyone use Steganographic and Cryptographic methods to secure their sensitive information.
* What are the methods involved in implementing steganography and cryptography.
* What challenges does users face while encrypting their information.
* Which is the suitable encryption algorithm for the current project.
* How does it secure from cyber-attacks.
* How to make it strong from decrypting by the wrong people to get access.

**CHAPTER 2**

**LITERATURE REVIEW**

**2.1 LITERATURE REVIEW – I**

# **TITLE:** A Review on Data hiding using Steganography and

# Cryptography.

**AUTHOR:** [Jeba Nega Cheltha C](https://ieeexplore.ieee.org/author/37089035468), [Manik Rakhra](https://ieeexplore.ieee.org/author/37086409223), [Rajan Kumar](https://ieeexplore.ieee.org/author/37089032592),

Himdweep Walia.

**PUBLISHER**: IEEE

**YEAR:** 2021

**CONTEXT:**

Nowadays we are sending lot of data through internet. The data can be image file, video file, text file and audio file. Some of the data which is transferred through internet might be confidential or may not be confidential data. However everyone expects their data should be secured and it should not be hacked by others. There are lots of techniques to defend from unauthorized users. One of the techniques to protect the data from unlicensed user is cryptography. In cryptography, the data will be converted to encrypted data on the sender side. Encryption means converting original message to scribbled message, which is not in the readable format. The encrypted data will be sending through communication channel. If any unauthorized person access the data, the original data will not be visible. Only the receiver can decrypt the data. Steganography is another technique, in which the original data will be embedded into Cover file. The cover file can be text file or video file or image file. If any unauthorized person, try to access the message, the original data will not be visible instead cover file will be visible. Various steganography and cryptographic technique is presented in this literature review. Among those few are steganography based and few use both steganography and cryptography. The methodology in which both steganography and cryptography gives the best performance.

**2.2 LITERATURE REVIEW – II**

# **TITLE:** Digital Image Steganography

**AUTHOR:**  [Aditya Saxena](https://ieeexplore.ieee.org/author/37089472824) , [Ganga Maheshwari](https://ieeexplore.ieee.org/author/37089472399)

**PUBLISHER**: IEEE

**YEAR:** 2021

**CONTEXT:**

Various applications have various prerequisites of the steganography strategy utilized. As an example, a couple of applications may require outright imperceptibility of the restricted data, while others require a much bigger mystery message to be covered up. During this venture named “Image Steganography”, we’ve zeroed in on least huge piece change methods of spatial area. We’ve broke down and analyzed the variations of this calculation regarding viability and concealing limit. Adequacy of the calculation is estimated by client assessments deciding so, all things considered modification to the photographs got evident. In modern world, Internet one of the most important factor of information technology and communication has been the security of information. Cryptography was created as a technique for securing the secrecy of communication and many different methods have been developed to encrypt and decrypt data in order to keep the message secret. Unfortunately it is sometimes not enough to keep the contents of a message secret, it may also be necessary to keep the existence of the message secret. The technique used to implement this, is called steganography. That is in need to tackle this issue has prompted the improvement of steganography plans. Steganography is a ground-breaking security mechanism that gives a significant degree of security, especially once it's joined with cryptography. Steganography varies from cryptography, cryptography focuses on keeping the contents of a message secret, steganography focuses on keeping the existence of a message secret.

**2.3 LITERATURE REVIEW – III**

# **TITLE:** An Efficient Audio Steganography Technique to Hide Text in

# Audio

# **AUTHOR:** [Shital P. Rajput](https://ieeexplore.ieee.org/author/37086454241) , [Shital P. Rajput](https://ieeexplore.ieee.org/author/37086454241) , [Girish K. Patnaik](https://ieeexplore.ieee.org/author/37997397900)

**PUBLISHER**: IEEE

**YEAR:** 2018

**CONTEXT:**

Information security is the biggest challenge in recent digital communication era. Audio steganography is one of the information security techniques, which hides secret data in audio media. The traditional LSB based Audio steganography techniques are easy to implement but suffers from low embedding rate and low robustness. This paper introduces the new efficient audio steganography technique where two data bits of secret message are embedded at the time on LSB positions of carrier audio based on the compliment of 3 MSBs of carrier audio. In proposed work, two algorithms have been proposed. In Proposed Algorithm-I two data bits of secret message are embedded at a time on LSB positions of carrier audio based on the 3 MSBs of carrier audio and in Proposed Algorithm-II those two data bits are embedded on LSB positions of carrier audio but based on the compliment of 3 MSBs of carrier audio. Proposed Algorithm-I improves the embedding capacity by embedding two data bits at a time and Proposed Algorithm-II increases the robustness against attacks, because in conventional algorithms the embedding of the secret bit value is in linear fashion, therefore a hacker can easily extract the secret message. As complement operation is used in Proposed Algorithm-II extraction of data bits from complement 3 MSB's is not that much of easy than extraction of data bits from traditional algorithm. Moreover, additional security is provided with the help of secret key without knowing the valid secret key it is difficult to access the data.

**2.4 LITERATURE REVIEW – IV**

# **TITLE:** StegoCrypt Scheme using LSB-AES Base64

# **AUTHOR:** [Fahmi Anwar](https://ieeexplore.ieee.org/author/37087130193) , [Eko Hari Rachmawanto](https://ieeexplore.ieee.org/author/37086046813) , [Christy Atika Sari](https://ieeexplore.ieee.org/author/37086536435)

**PUBLISHER**: IEEE

**YEAR:** 2019

**CONTEXT:**

Many people use the internet in their daily communication. But the risks of data theft on the internet are quite high, so sending security is a very important thing for data. Cryptography and steganography is a technique used to secure data to minimize data theft and access by unauthorized people. Combination of Least Significant Bit (LSB) - Advanced Encryption Standard (AES) - Base64 is proposed in this study to provide protection for messages and various file formats embedded in digital images. Secret messages are encrypted with the AES and Base64 methods before being inserted into the image using the LSB method. The study also analyzed the performance of the LSB-AES-Base64 combination of algorithms on various files and the size of the cover image. Cover images used an image with RGB channels. For measurement of imperceptibility performance used Peak Signal to Noise Ratio (PSNR), Mean Square Error (MSE), and histogram analysis. Based on the results of testing, the proposed method can work well with the value of PNSR and MSE in a very good category. The stego image histogram is also identic to the original image.The development of internet technology makes it easy for the information exchange process. This exchange process cannot guarantee that the files sent will be free from access by unauthorized people. Files that can be accessed by unauthorized people can be misused so that they will be detrimental, therefore file security techniques are important and needed to prevent this . Security can be applied with cryptography and steganography mechanisms. In this case, cryptography and steganography can help someone to secure the information data sent. Cryptography is a science and art that learns how to secure a file. How to secure this by encrypting files with certain keys. Before the encrypted file is called plaintext, after being encrypted, it is called ciphertext. Whereas steganography is the science and art of hiding secret messages where messages are contained in the media but are not known to exist with the human senses.

This study proposes a combination of Least Significant Bit (LSB) - Advanced Encryption Standard (AES) - Base64 to safeguard messages and various file formats contained in digital images. Before being placed into the image using the LSB method, secret messages are encrypted using the AES and Base64 methods.

**2.5 LITERATURE REVIEW – V**

**TITLE:** A Proficient and secure way of Transmission using Cryptography and

Steganography

# **AUTHOR:** G Diwakara Reddy, Yaddanapudi VSSRR Udai Kiran, Prabhdeep Singh, Shubhranshu Vikram Singh, Sanchita Shaw, Jitendra Singh

**PUBLISHER**: IEEE

**YEAR:** 2022

**CONTEXT:**

People are concerned about the security of their data over the internet. The data can be protected in many ways to keep unauthorized individuals from accessing it. To secure data, steganography can be used in conjunction with cryptography. It is common for steganography to be used for hiding data or secret messages, whereas cryptography encrypts the messages so that they cannot be read. As a result, the proposed system combines both cryptography and steganography. A steganographic message can be concealed from prying eyes by using an image as a carrier of data. In steganography, writing is done secretly or covertly. The digital steganography algorithm uses text, graphics, and audio as cover media. Due to recent advancements in technology, steganography is challenging to employ to safeguard private data, messages, or digital photographs. This paper presents a new steganography strategy for confidential communications between private parties. A transformation of the ciphertext into an image system is also performed during this process. To implement XOR and ECC (Elliptic Curve Cryptography) encryption, three secure mechanisms were constructed using the least significant bit (LSB). When sending personal data over the internet, data security is crucial. Copyright, ownership, and harmful data identification are all aided by steganography and stegan analysis tools. Steganography, which does not alter the content, is used to conceal sensitive data, and stegan analysis is used to unearth hidden material. In this article, we describe steganography, stegen analysis, and machine learning frameworks. It also demonstrates how the latter can be utilized to uncover buried textual information using steganographic methods. Today, secure communications are established using mathematical models in conjunction with cryptography and steganographic methods. As the number of users increases effectively, steganography is the effective method to provide secure data transmission over the network. Data via networks can also be secured using cryptography, however transmission of secured messages might be detected by third parties. Steganography, from the perspective of security, does not permit the detection of the presence of a hidden secret over the communication channel, other than the user. In this study, we build a system that combines steganographic and cryptographic features, using the TCP/IP header as a steganographic carrier to conceal encrypted data. A helpful tool that enables covert information transmission via the communications channel is steganography.

**CHAPTER 3**

**SYSEM ANALYSIS**

**3.1 EXISTING SYSTEM**

Steganography is the practice of enclosing information in another message or physical item in a way that prevents human scrutiny from revealing its presence. A message, image, or video is hidden within another file, message, image, or video in computing and electronic environments. Steganography can be applied both positively and negatively. Steganography is used, for instance, by organizations in the corporate and educational sectors, as well as by the military, intelligence services, and law enforcement, to hide sensitive communications and data.

However, malicious hackers use steganography to tamper with data files or conceal malware in otherwise good-looking documents. For instance, hackers can utilize Word and Excel documents to conduct automated assaults using BASH and PowerShell scripts. When one of those documents is opened by a careless, unwary user, the concealed, secret script is activated, and chaos results. This form of ransomware delivery is popular. At their most basic level, steganography and cryptography both work to protect communications and data from prying eyes. They do, however, use a different form of security.

Cryptography transforms data into incomprehensible ciphertext. The use of encryption was obvious to everyone who read this message after it was intercepted. Steganography, on the other hand, conceals a message without changing its original structure. While obfuscation and steganography both involve concealing information, the former method intentionally makes the message difficult to understand, read, or decode. That makes sense because to obfuscate something is to make it unclear, difficult to understand, or obscure. Obfuscation is a technique used by cyber security experts to safeguard sensitive data, such as programming codes. As a result, hackers are prevented from accessing the codes in the first place and using the data for their own purposes. In conclusion, obfuscation is a type of steganography, but the reverse is not true.

**3.1.1 DISADVANTAGES**

* Someone may have suspicions because there is a lot of material and a significant file size.
* This method can be extremely dangerous if it falls into the hands of hackers, terrorists, or criminals.
* If the original file's size is already known or estimated, that might pose a risk to the excess memory that would be evident in its attributes.
* High availability, one of the essential elements of information security, cannot be ensured by cryptography. To combat threats like denial of service (DoS) attacks and complete information system failure, more defence tactics are needed.

**3.2 PROPOSED SYSTEM**

Although steganography and cryptography are different, combining the two can increase the security of the information that is protected and keep the secret communication from being discovered. Data that has been steganographically concealed may still be secure if it is encrypted, but the security of the channel will be compromised. Comparing steganography with encryption to encryption-only communication has benefits.

The main benefit of steganography over encryption for data concealment is that it makes it more difficult to identify the sensitive information that is being concealed within a file or other piece of content. Using steganographic techniques helps to hide the existence of the secure channel, whereas an encrypted file, communication, or network packet payload is plainly indicated and traceable as such. Steganographic messages may first be encrypted and then a cover message is modified to contain the encrypted message, resulting in stego text. Only those who know the technique used can recover the message and, if required, decrypt it and so on.

**3.2.1 ADVANTAGES**

* Sensitive data can be hidden via steganography, making it harder for unauthorized people to access or steal it.
* Enables covert communication between parties by enabling the transmission of secret messages.
* Can be used to hide sensitive information inside of seemingly innocent files, preventing it from being deleted or altered.
* For persons who live in nations with strong internet regulations, steganography can be used to get around censorship by masking the substance of a message.

**CHAPTER 4**

**REQUIREMENT ANALYSIS**

**4.1 SOFTWARE REQUIREMENTS**

**4.1.1 HTML**

Hyper Text Markup Language, also known as HTML, is a programming language used to build websites and online applications. Simply put, hypertext is "Text within Text." A text that contains links is a hypertext. A hypertext link is one that when you click on it opens a new webpage for you. Two or more web pages (HTML documents) can be linked together via hypertext. A text document can be formatted and laid out using a markup language, which is a computer language. Text is made more interactive and dynamic using markup language. It can convert text into graphics, tables, links, and other formats. A web browser will transform a document that is typically written in HTML into a web page. An URL can be used to locate a web page. A web page can be either dynamic or static. Only HTML can be used to construct static web pages.

**4.1.2 BOOTSTRAP**

A suite of free and open-source tools called Bootstrap is used to build websites and online apps that are responsive. The framework is the most well-liked combination of HTML, CSS, and JavaScript for creating responsive, mobile-first websites. The websites of today are ideal for all modern browsers, including IE, Firefox, and Chrome, as well as for displays of all sizes, including desktop, tablets, phablets, and smartphones. All credits to the creators of Bootstrap, Mark Otto and Jacob Thornton from Twitter, even if the project later became open-source. All websites created today are responsive. Responsive web design is design that adapts to all screen sizes. Adjust the design according to the screen size. So the same applications can be opened on the laptops, tabs, smartphones, etc. The size changes according to the screen size. This mean your web design can run on any screen size. There is no need to create separate applications for laptops, tablets, smartphones, etc. Bootstrap is known as an open source front-end development framework for building websites and web applications and creating website icons etc.

**4.3 CSS**

CSS, or cascading style sheets, is an acronym. It is a language for creating style sheets that describe the layout and appearance of markup-language documents. It gives HTML an additional feature. Typically, it works with HTML to modify the look and feel of web pages and user interfaces. Any XML document type, including plain XML, SVG, and XUL, can be used with it. To construct user interfaces for web apps and many mobile applications, most websites combine CSS, HTML, and JavaScript.

**4.4 PYTHON**

A high-level, all-purpose programming language is Python. Its design philosophy places a strong emphasis on code readability through the use of off-side rule-based considerable indentation. Python uses garbage collection and has dynamic typing. It supports a variety of programming paradigms, including procedural, object-oriented, and functional programming as well as structured programming (especially this). Due to its extensive standard library, it is frequently referred to as a "batteries included" language.

Python was created by Guido van Rossum in the late 1980s to replace the ABC programming language, and it was originally made available as Python 0.9.0 in 1991. In 2000, Python 2.0 was made available. The 2008 release of Python 3.0 was a significant update that was only partially backwards compatible with previous iterations. The final Python 2 release was Python 2.7.18, which was made available in 2020.

**4.5 JAVASCRIPT**

Along with HTML and CSS, JavaScript frequently referred to as JS, is a programming language that is a fundamental component of the World Wide Web. 98% of websites will utilize JavaScript on the client side by the year 2022 to control webpage behavior, frequently integrating third-party libraries. A dedicated JavaScript engine is available in every major web browser and is used to run the code on users' devices. JavaScript is an ECMAScript-compliant high-level, frequently just-in-time compiled language. It features first-class functions, prototype-based object orientation, and dynamic typing. It supports event-driven, functional, and imperative programming paradigms and is multi-paradigm. For working with text, dates, regular expressions, common data structures, and the Document Object Model (DOM), it includes application programming interfaces (APIs).

**4.6 HARDWARE REQUIREMENTS**

**WINDOWS 7**

A windows 7 or newer system is sufficient to build the entire project.

**RAM AND ROM**

4GB or more of RAM and 256GB or more SSD is sufficient.

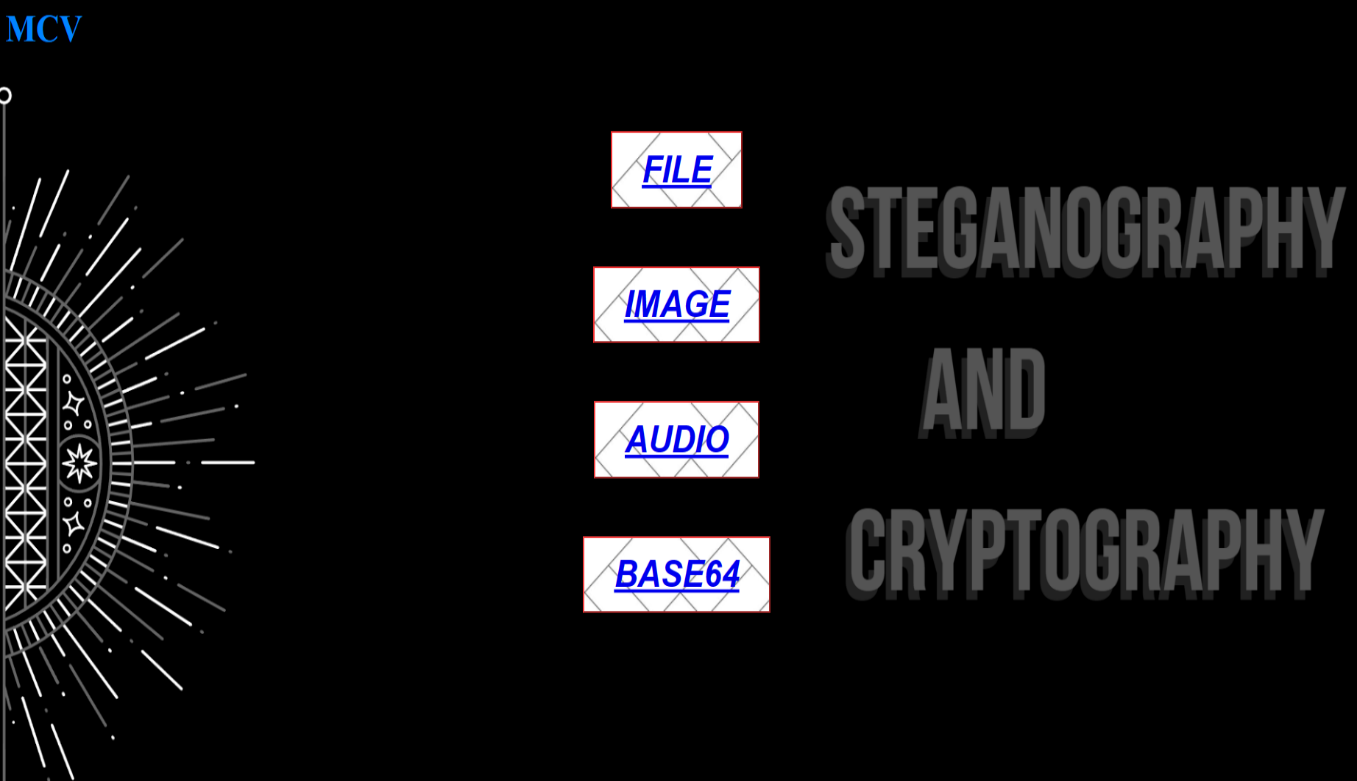
**KEYBOARD AND MOUSE**

A sensitive mouse and keyboard is also required.

**CHAPTER 5**

**METHODOLOGY**

**5.1 SELECTING TYPE OF ENCRYPTION**



**Figure 5.1** Main page

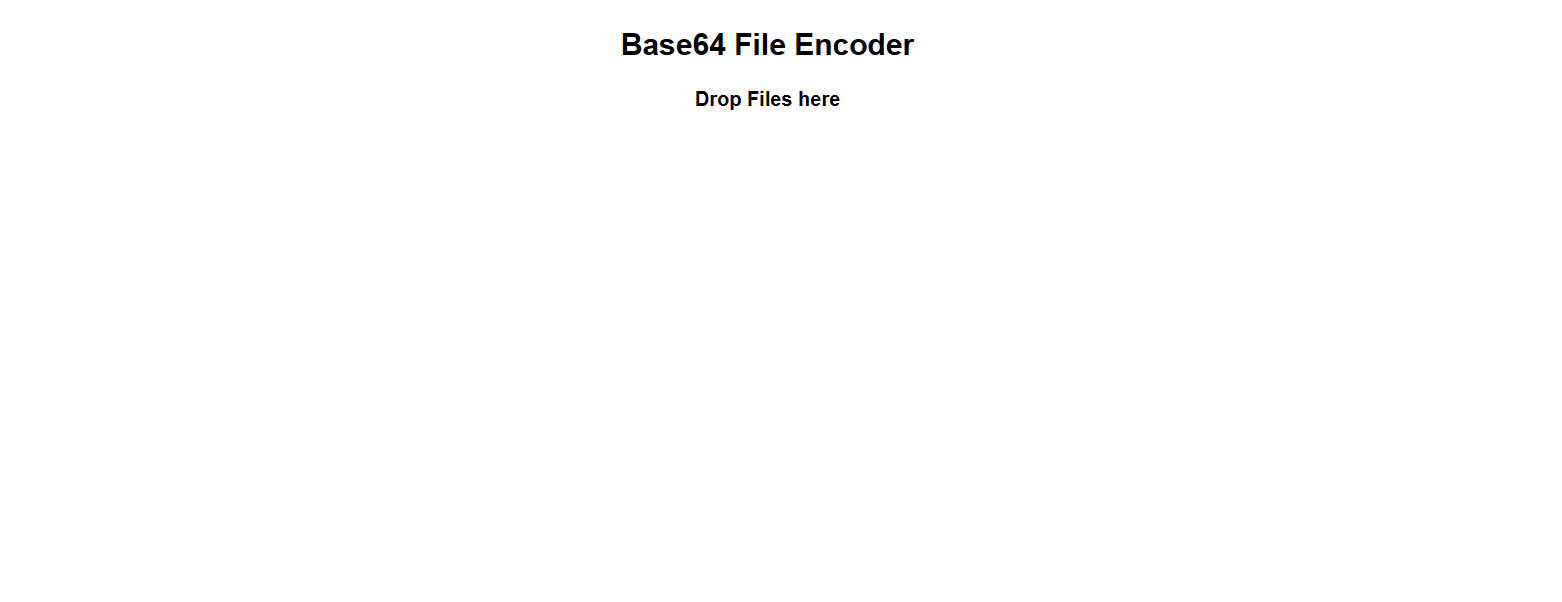
First the user must select the type of encryption they wanted. The available methods are file encryption, audio encryption, image encryption and base 64. Based on their type of data user needs to select their preferred method and encrypt it.

**5.2 FILE ENCRYPTION AND DECRYPTION**



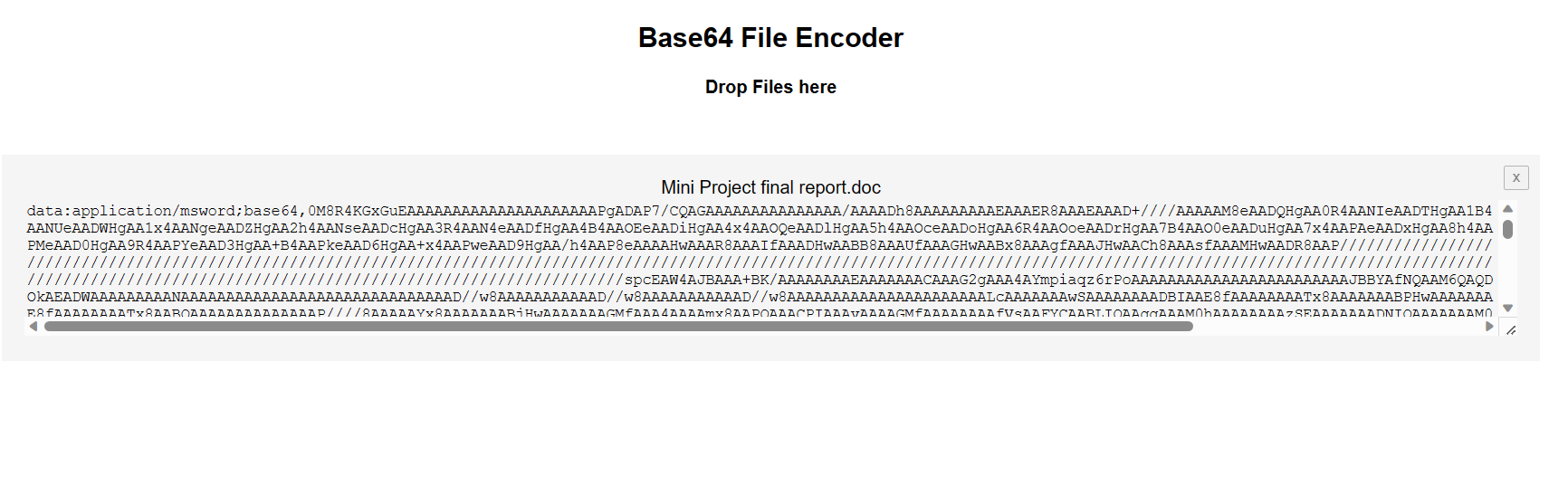
**Figure 5.2.1** File main page

Under file encryption the files can be uploaded and can be encrypted by cryptographic method. It gives a special characters which then can be decrypted to obtain the file.

To encode the message file is to be dropped in the encode section: 

**Figure 3** File Encoder

After dropping the file, special characters are obtained like this:

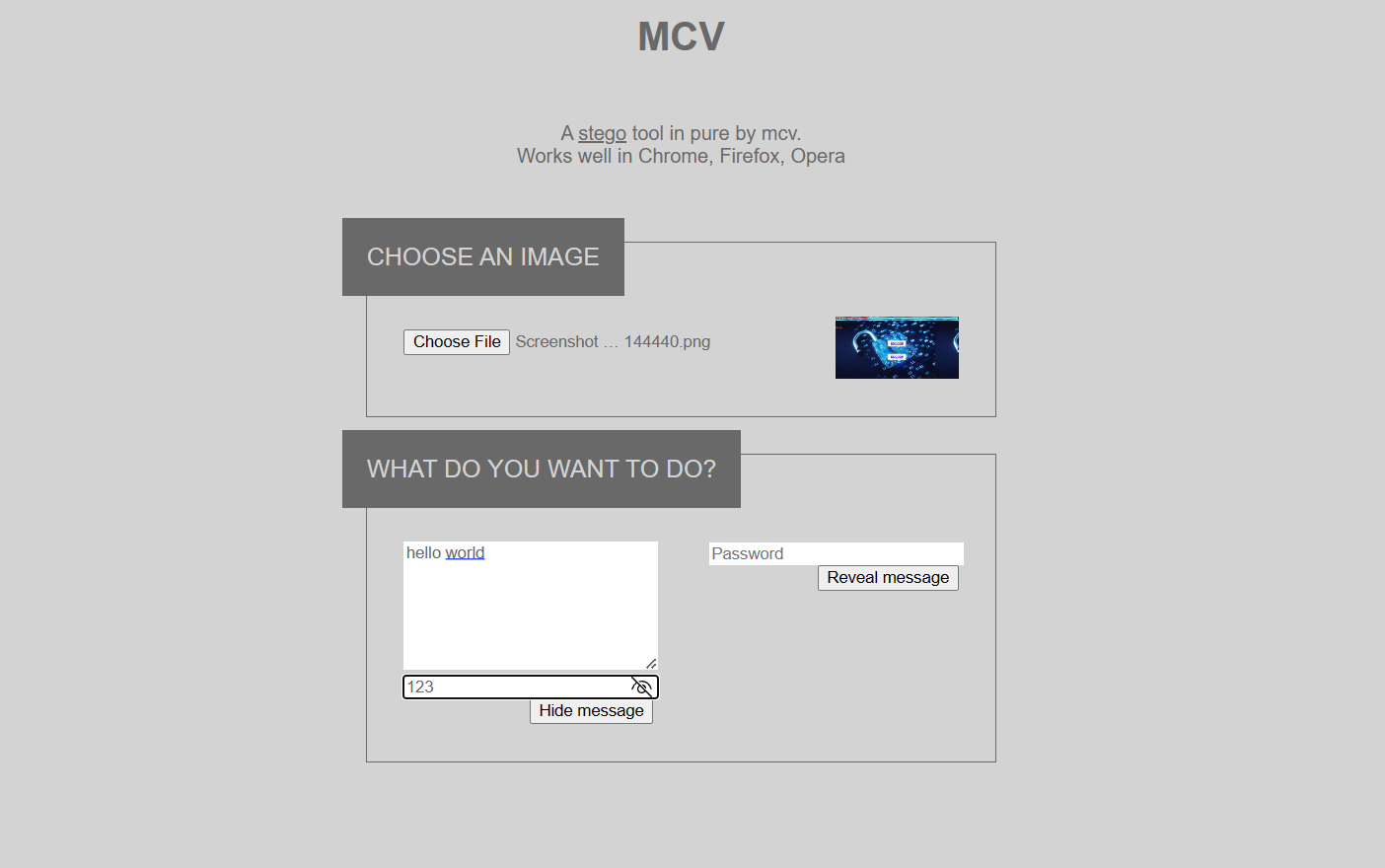
**Figure 5.2.2** File Encoder

This can be copied directly from source, and pasted in the decode section to obtain the secret file.  
**5.3 IMAGE ENCRYPTION AND DECRYPTION**

Under image steganography a secret message is encrypted inside of the image as a cover of it. The secret message can be password protected.

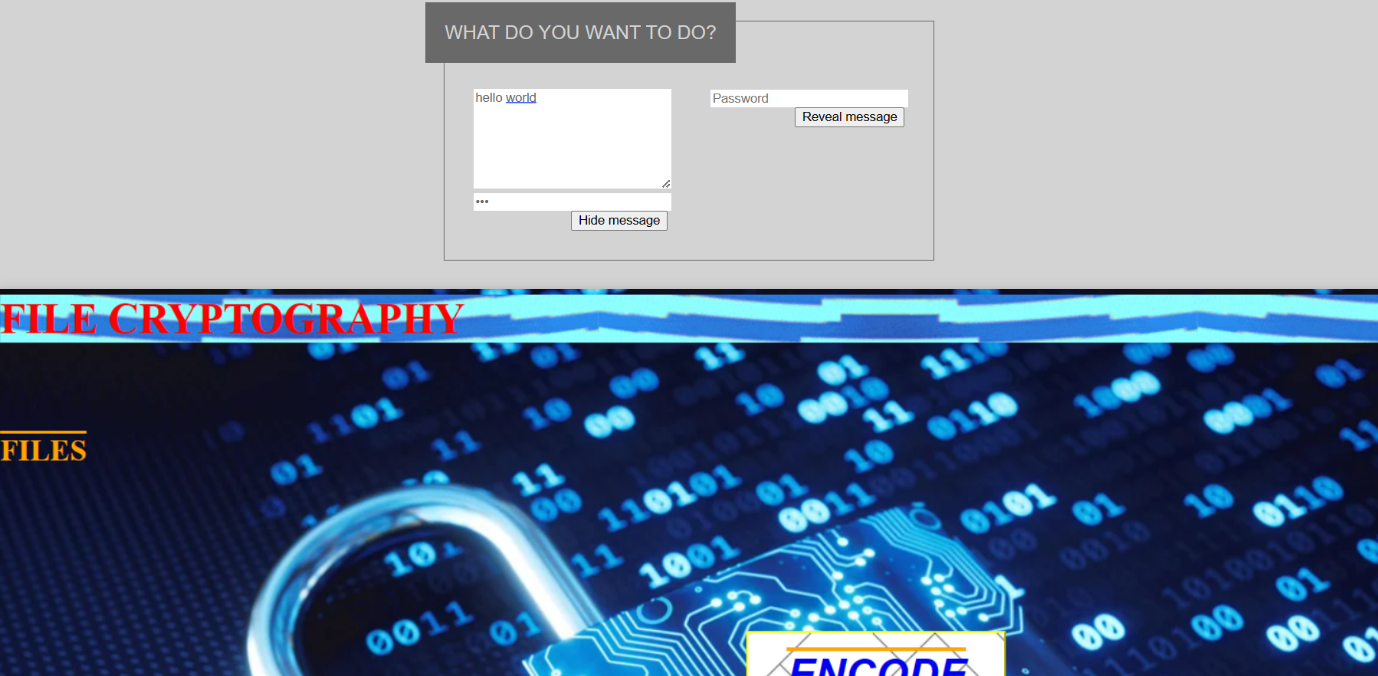
**Figure 5.3.1** Image Encoder

An image file is chosen to hide a secret massage with

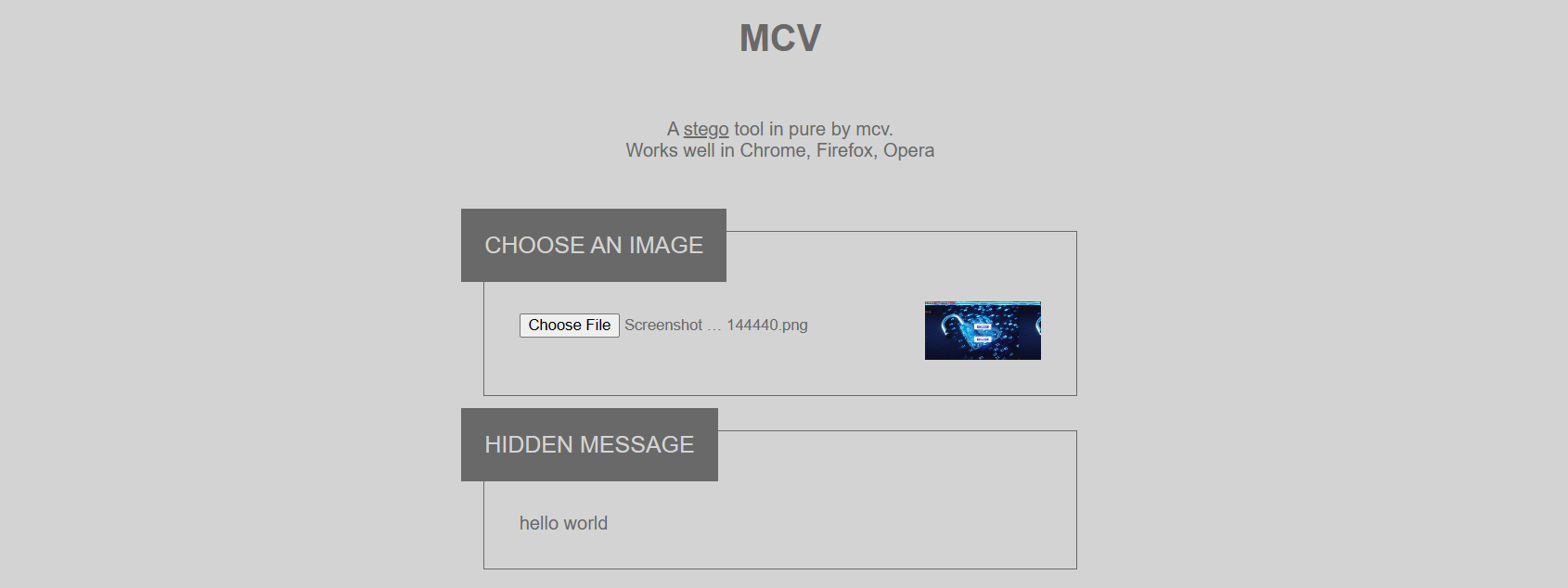


**Figure 5.3.2** Image Decoder

After selecting an preferred an image secret message in typed in the rectangular bar. Password is optional.



**Figure 5.3.3** Image Encrypt

The encrypted message appears down below which can be saved and send to the receiver.

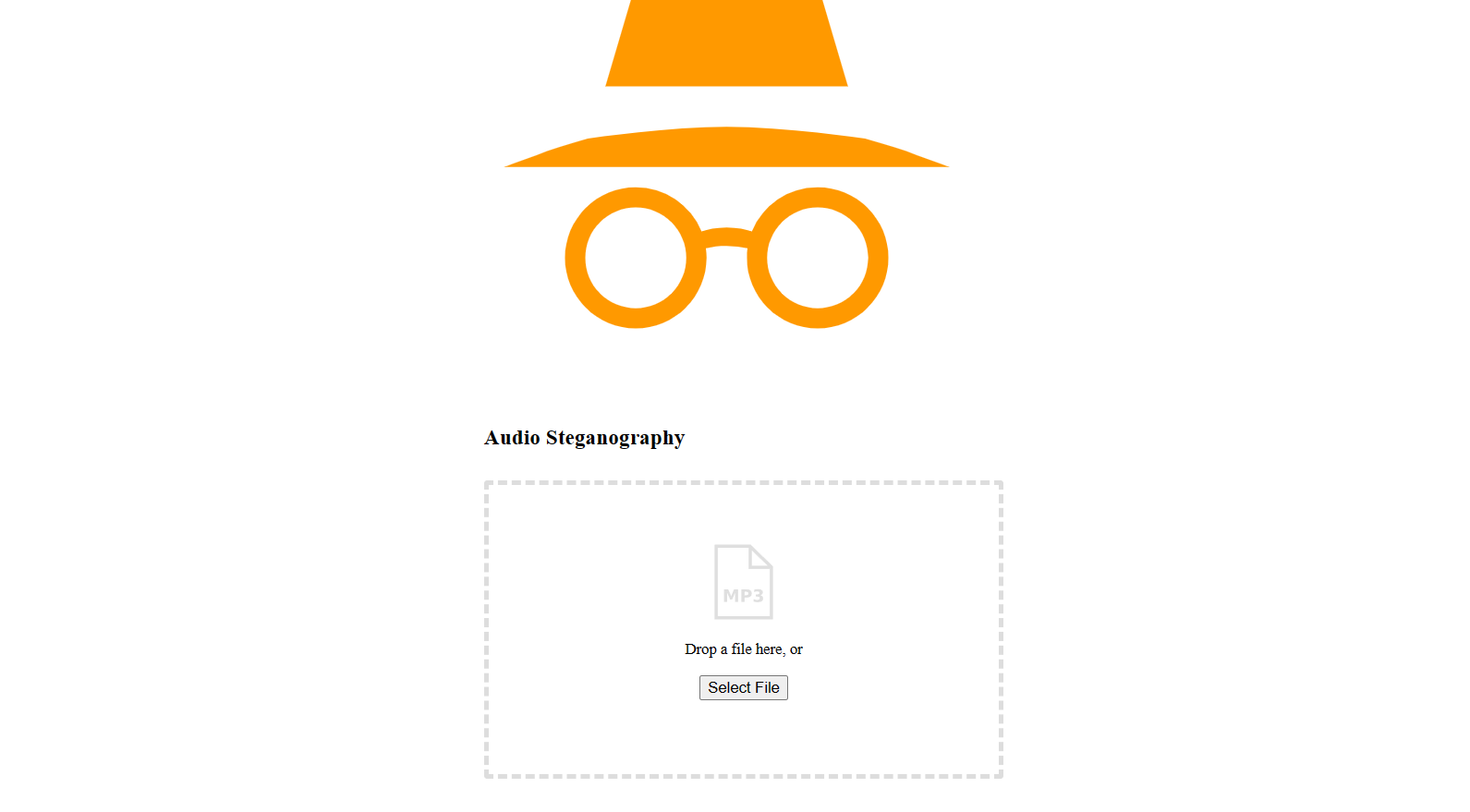
**Figure 5.3.4** Image decode

* After receiving the image receiver is to be uploaded the image.
* And password is typed to reveal the secret message
* After password is typed correctly the encrypted shows below as showing in the above picture.

And to clear the page, the page is reloaded to get rid off the information showing in the website.

**5.4 AUDIO ENCRYPTION AND DECRYPTION**

Under audio steganography secret message is covered inside of the audio file.



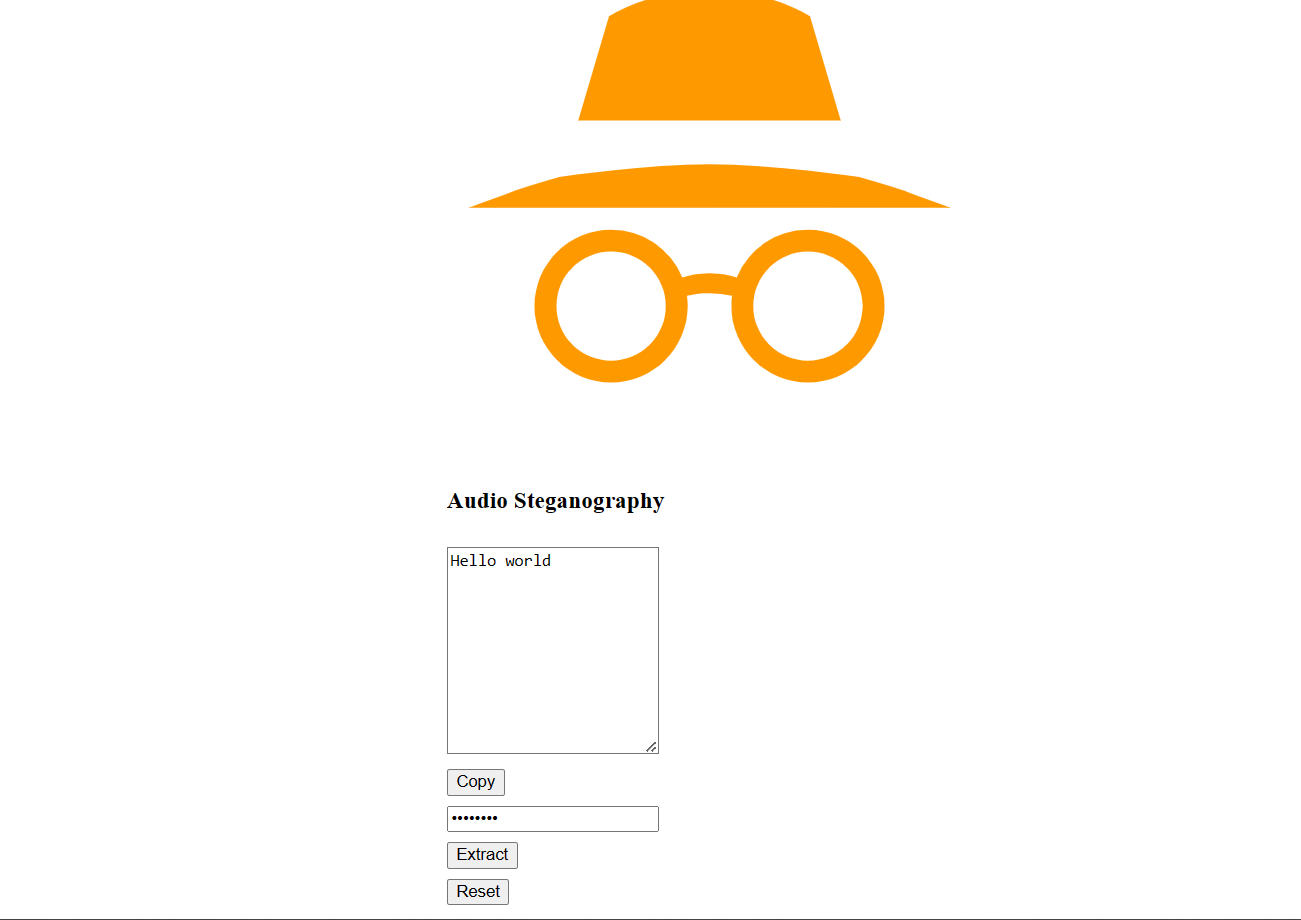
**Figure 5.4.1** Audio Page

Hide secret text messages inside MP3 files. Just choose an MP3 of your choice, type in your message, and a new MP3 file will be created.



**Figure 5.4.2** Audio Encoder

To uncover the message, load the newly created file again. Optionally, you can choose to encrypt the message with a password for additional layer of security.

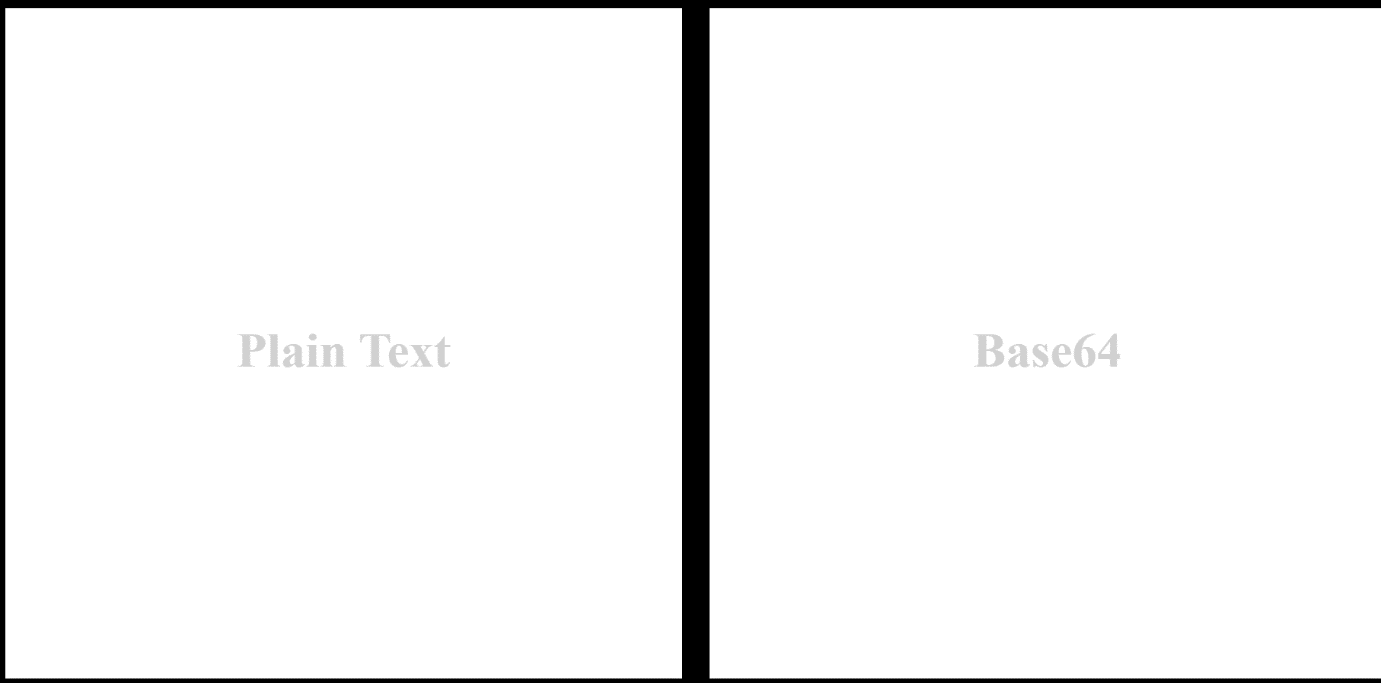


**Figure 5.4.3** Audio Decoder

This way an user can encrypt an secret message in audio steganography.

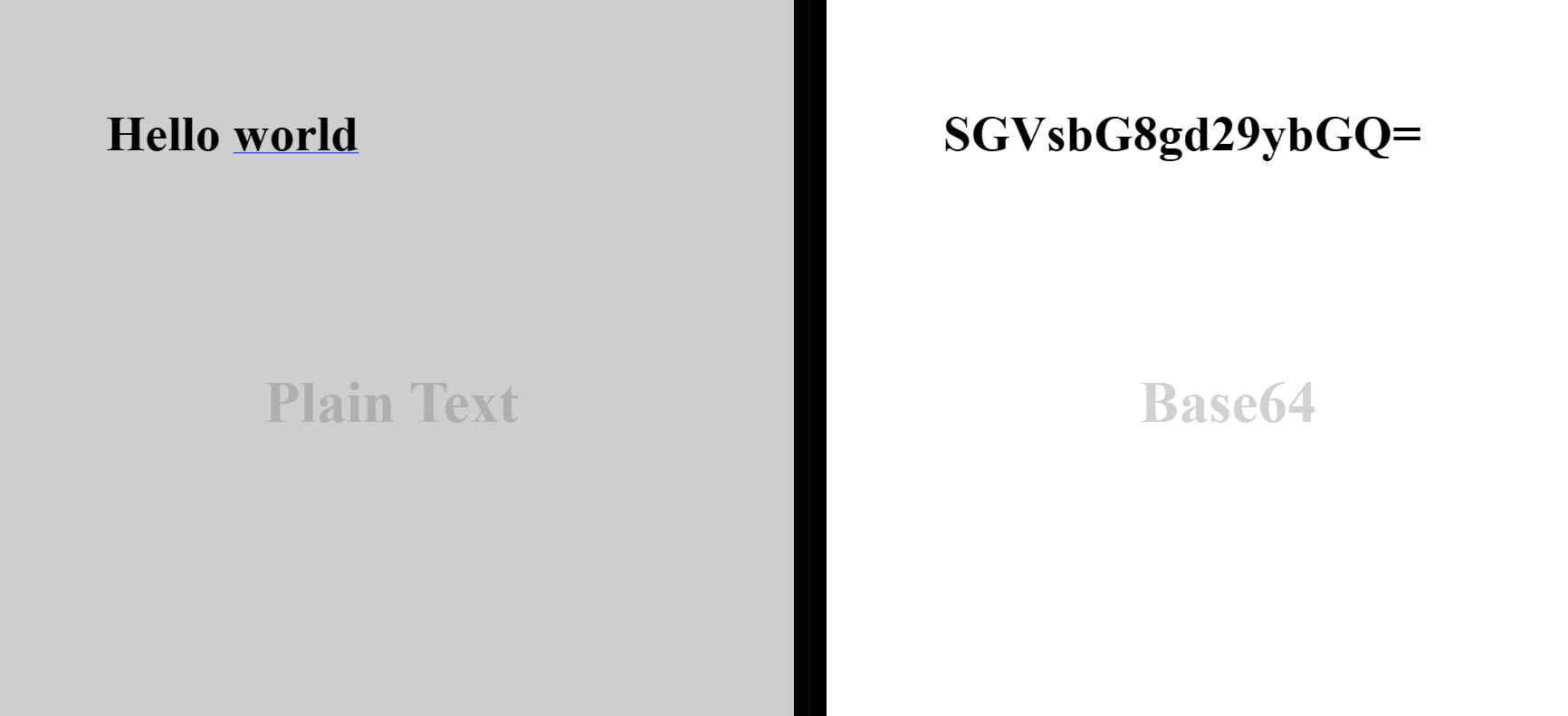
**5.5 BASE 64**

Base64is**a group of binary-to-text encoding schemes that represent binary data in sequences of 24 bits that can be represented by four 6-bit Base64 digits.**

****

**Figure 5.5.1** Base64 Page

It is a cryptographic method in which the text can be converted into special characters. The user can copy content and paste here to get an encrypted characters.



**Figure 5.5.2** Base64 file

The uniqueness is it also changes it encrypted form based on the indexing type. In the above picture the “Hello world” is in above and we can notice its cryptographic notation. Now lets see by changing its position.



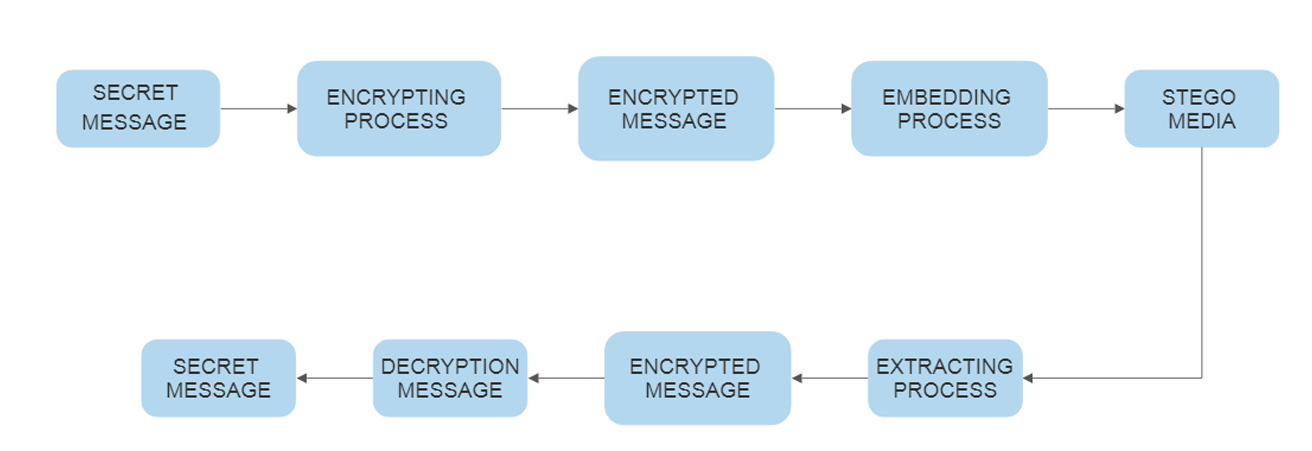
**Figure 5.5.3** Bage64 File

**CHAPTER-6**

**SYSTEM DESIGN**

**6.1 ARCHITECTURE DESIGN**

**6.1.1 FILE**

****

**Figure 6.1** Block diagram of file

**SECRET MESSAGE:**

It is a message which user decide to convert it into cryptographic method. And can be converted back by using the decryption process.

**ENCRYPTING PROCESS:**

The secret message is encrypted here. The encryption is done by converting the message into cryptographic method.

**ENCRYPTED MESSAGE:**

After the encryption process the message is encrypted and send to the receiver.

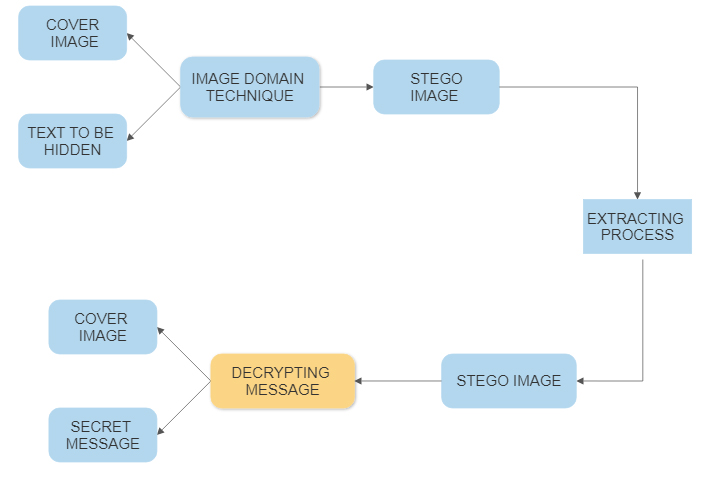
**EXTRACTING PROCESS:**

The encrypted message goes through the extracting process.

**DECRYPTION MESSAGE:**

After the user on other receives the encrypted file, it is time to decrypt it and find out the secret message.

**6.1.2 IMAGE**

****

**Figure 6.1.2** Block diagram of Audio

**COVER IMAGE:**

User has to be select an image to hide an secret message in it. The picture can be in JPG format.

**TEXT TOBE HIDDEN:**

The secret message is given to hide in the picture.

**IMAGE TECHNIQUE:**

It is a technique where a special algorithm is given to hide the message in the image.

**STEGO IMAGE:**

It is a image where the encryption is done.

**EXTRACTING PROCESS:**

It is a process where extraction takes place of the stego image.

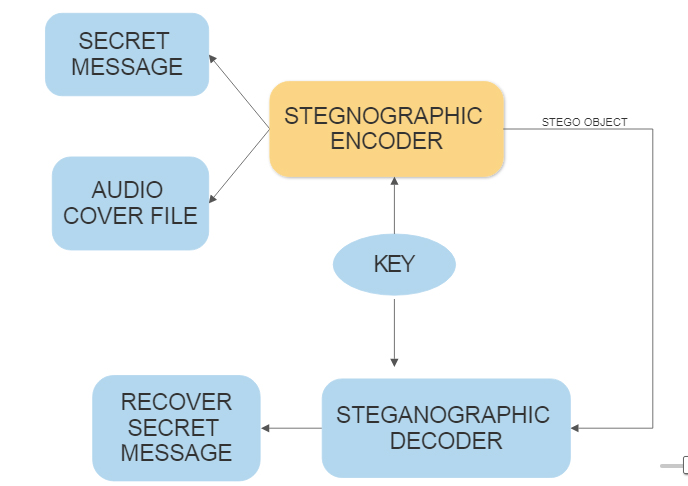
**DECRYPTION PROCESS:**

After the message is encrypted, it is decrypted on the other side to obtain the secret message.

**SECRET MESSAGE:**

After the decryption process the secret message hidden in it is revealed here.

**6.1.3 AUDIO**

****

**Figure 6.1.3** Block diagram of Audio

**SECRET MESSAGE:**

It is a message which user decide to hide it into Audio file. And can be converted back by using the decryption process.

**AUDIO COVER FILE:**

User has to be select an Audio file to hide secret message in it. The Audio can be in mp3 format.

**STEGANOGRAPHIC ENCODER:**

The secret message is encrypted here. The encryption is done by hiding a message in an audio file.

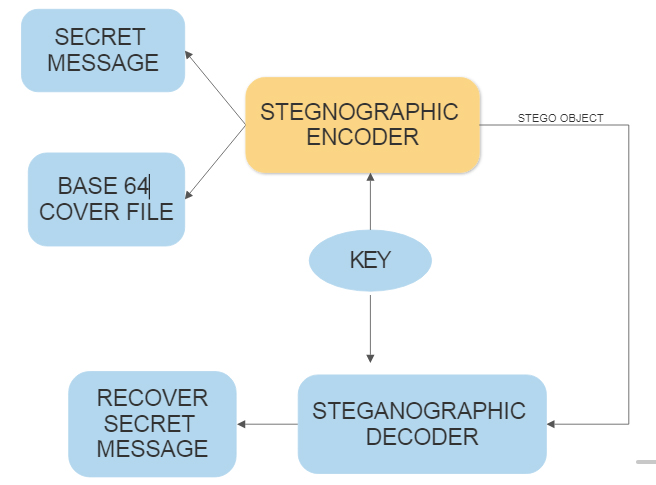
**KEY:**

It is a password given at the time of encryption. During decryption password has to be entered.

**STEGANOGRAPHIC DECODER:**

The secret message is decrypted here.

**6.1.4 BASE 64**

****

**Figure 6.1.4** Block diagram of Base64

**SECRET MESSAGE:**

It is a message which user decide to hide it into Audio file. And can be converted back by using the decryption process.

**AUDIO COVER FILE:**

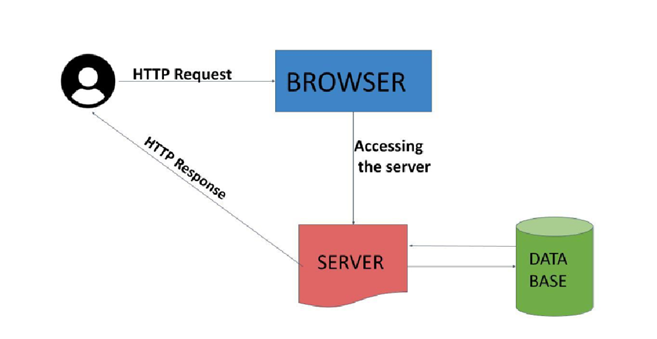
User has to be select an Audio file to hide secret message in it. The Audio can be in mp3 format.

**STEGANOGRAPHIC ENCODER:**

The secret message is encrypted here. The encryption is done by hiding a message in an audio file.

**KEY:** It is a password given at the time of encryption. During decryption password has to be entered.

**6.2 HOW THE OVERALL WEBSITE WORKS IN THE SYSTEM:**

****

**Figure 6.2** System Design

First, a user sends a request to a web browser via a URL (Universal Resource Locator). A web browser is application software for browsing and viewing information on the internet. A user can request any of the web pages by simply entering his URL in the address bar. Web browsers can display text, audio, video, animation and more. It is the responsibility for the web browser to interpret the text and message and commands contained in web pages. It used to be text-based web browser, but now graphics-based or voice-based web browser is also available.

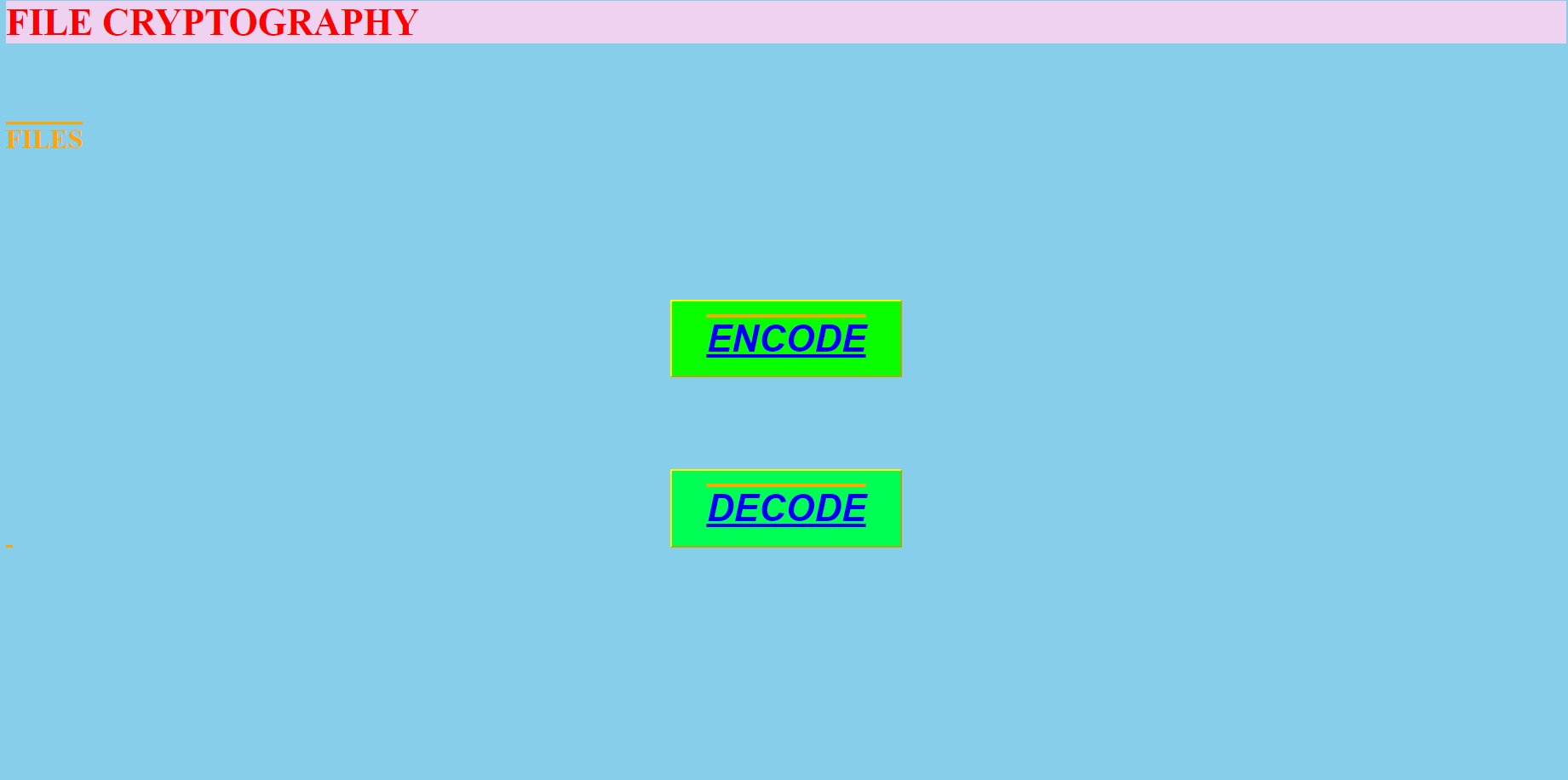
Web browsers forward HTTP (Hyper Text Transfer Protocol) request to servers. The server receives HTTP requests from the web browser and responds to the request by sending appropriate results to the web browser. A web browser receives the response from the server and displays the response to the user.

**CHAPTER-7**

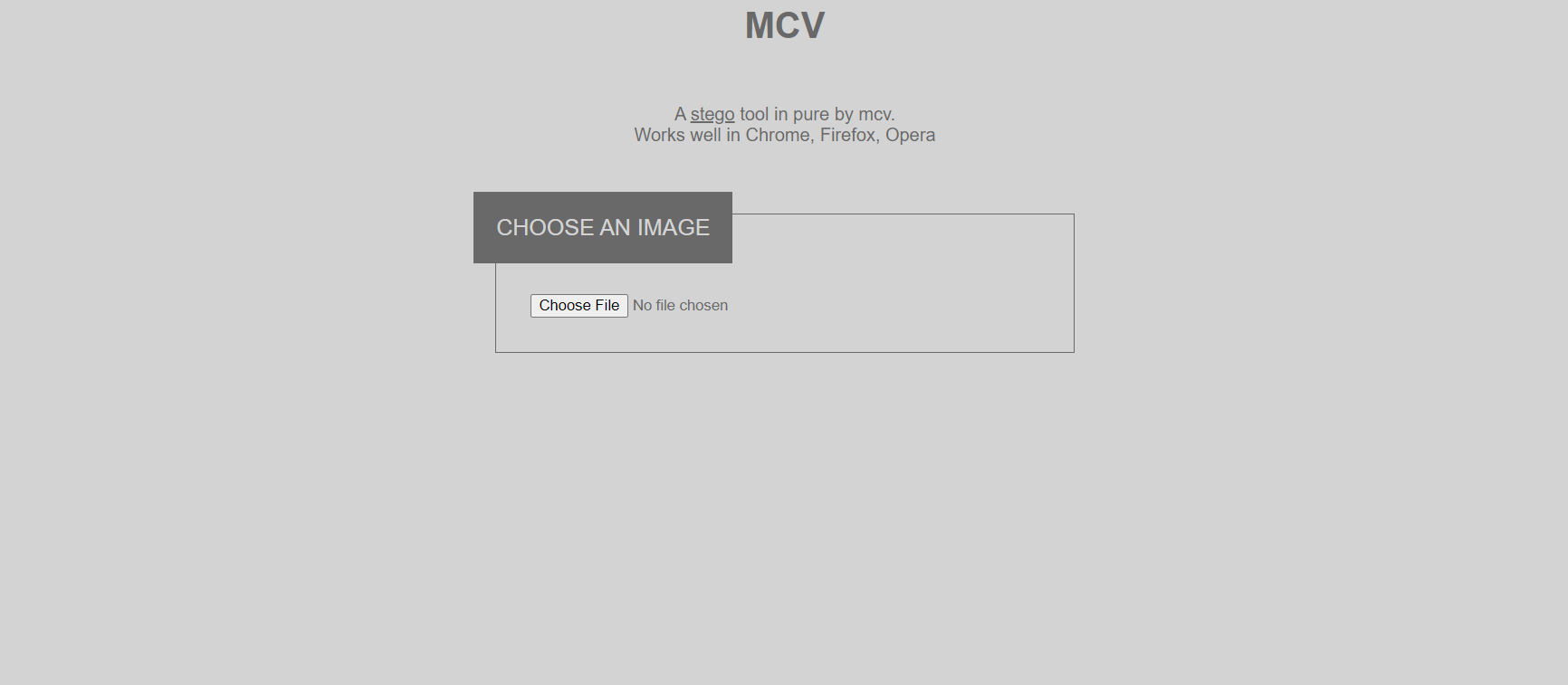
**RESULT AND DISSCUSSION**

****

**FIGURE 7.1** HOME PAGE

This is the home page of our site. Here there are different encryption methods available. At right top corner MCV denotes our project team members. Inside file menu there is encryption and decryption icons. In image the image can be dragged or uploaded directly into it. Base64 directly converts the given data into its format.

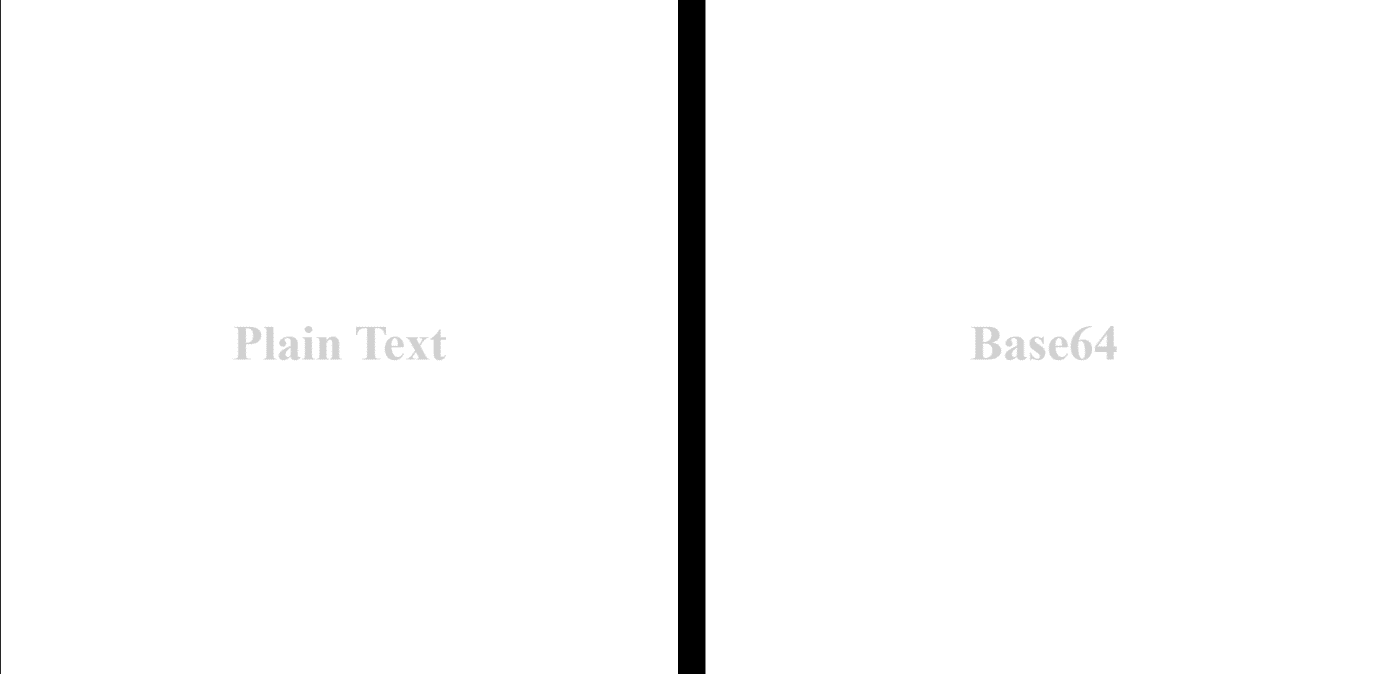
**FIGURE 7.2** FILE SITE



**FIGURE 7.3** IMAGE SITE



**FIGURE 7.4** AUDIO STEGANOGRAPHY SITE

****

**FIGURE 7.5** BASE 64 SITE

**CHAPTER 8**

**CONCLUSION**

A creative and exciting method for transmitting private information covertly is steganography. It is essential that cybersecurity professionals have a thorough understanding of this practise because it can be utilised for both good and bad purposes1. One of the most crucial cybersecurity techniques is steganography, which is used to safeguard sensitive data before it is delivered to a public or private network2. Data can be protected by masking it, however doing so may not provide full protection. Using a steganography technique, it is feasible for an adversary to discover the presence of a text message in the image file and then to be successful in extracting information from the image, which can be disastrous in real-world scenarios3. The field of cybersecurity relies heavily on steganography.

**FUTURE WORK**

The future works with steganography and cryptography includes adding the following methods :

Traditional based steganography methods: Conventionally, Least Significant Bits (LSB) substitution method is employed to perform image steganography. Images are usually of higher pixel quality, out of which not all the pixels are used. LSB methods works under the assumption that modifying a few pixel values would not show any visible changes. The secret information is converted into a binary form. The cover image is scanned to determine the least significant bits in the noisy area. The binary bits from the secret image are then substituted in the LSBs of the cover image. The substitution method must be performed cautiously as overloading the cover image may lead to visible changes leaking the presence of the secret information.

CNN-Based Steganography Methods: Image steganography using CNN models is heavily inspired from the encoder-decoder architecture. Two inputs – cover image and the secret image are fed as the input to the encoder to generate the stego image and the stego image is given as input to the decoder to output the embedded secret image. The basic principle is the same except different methods have tried different architectures. The way the input cover image and the secret image are concatenated are also different in different approaches while the variations in the convolutional layer, pooling layer are expected. The number of filters used, strides, filter size, activation function used and loss function vary from method to method. One important point to note here is the size of the cover image and the secret image has to be same, so every pixel of the secret image is distributed in the cover image.

Security and Robustness:

Security is associated with embedding and robustness is associated with the extraction of the secret image. From our observations, CNN-based methods and GAN-based methods yield higher security. It is worth noting that the extraction of the secret images is prone to loss in information in deep learning methods. However, in traditional methods, the security is less but the robustness is high. PSNR measure is used to correlate the security and the robustness. From 5 and it can be noted that [49] has the highest PSNR value explaining the higher security of the GAN based method. The highest value of PSNR being 64.7, given by the cycle GAN based image steganography method.

Some of the aspects that can be considered for future works are enumerated below,

* Usage of popular networks U-Net, cycleGAN and using DCT and DWT have been considered and more exploration on the other customized architectures can be attempted. For example, Recurrent Neural Networks (RNNs) instead of CNNs can be further explored. A customized WGAN can be replaced with other variants of GAN.
* The majority of image steganography methods use either text or gray scale image as the secret information and there is a need for more research in hiding image in image and image in video.
* Experiments related to optimizing the parameters and decreasing the storage capacities can be further conducted using various datasets.
* The era of quantum computing is not far away, more efforts on developing designs on quantum images can be explored.
* To benefit from a combination of methods, an ensemble of traditional and deep learning methods can be further studied.
* Efforts can be directed to form a benchmark dataset containing images from various source cameras, image formats. A compilation of all possible algorithms can also be done to create the steganography images.
* Many methods have considered the hiding capacity, security and robustness as the performance measure. However, there are possibilities for man-in-the-middle attacks when the transfer happens through untrusted channels. Tampering of the stego image can also happen during the transfer. These attacks and the performance of the designed algorithm against these attacks can be considered for evaluation along with other metrics.

**APPENDICES 9**

**APPENDIX A – SOURCE CODE**

**Home page:**

<html>

<head>

<title>STEGANOGRAPHY AND CRYPTOGRAPHY</title>

<STYLE>

body {

background-image:url("MCV.png");

background-size: 100% ;

}

h1 {

font-weight: bold;

font-size: 35px;

margin: 4px 2px;

cursor: pointer;

color:rgb(0, 132, 255);

}

button{

background-image: url('https://image.shutterstock.com/image-vector/mondrian-pattern-vector-design-diagonal-260nw-1724546761.jpg');

font-style: italic;

font-weight: bold;

font-size: 35px;

text-align: center;

padding: 15px 32px;

display: inline-block;

margin: 4px 2px;

}

</STYLE>

</head>

<BODY>

<h1> MCV</h1>

<!-- FILE-->

<br>

<br>

<br>

<br>

<button style="background-color: rgb(44, 167, 238);

border-color: rgb(240, 46, 46);

color:rgb(168, 188, 224);

display:block; margin: 0 auto;"

type="button">

**FILE:**

<!DOCTYPE html>

<html>

<head>

<style>

body

background-image: url('https://assets.rebelmouse.io/eyJ0eXAiOiJKV1QiLCJhbGciOiJIUzI1NiJ9.eyJpbWFnZSI6Imh0dHBzOi8vYXNzZXRzLnJibC5tcy8xOTAxMjAxMi9vcmlnaW4uanBnIiwiZXhwaXJlc19hdCI6MTY3MDg5MDc0NX0.kH7srv1\_ZZjd1bX7rHO\_3O4bv7MxUze708dL1jeEnnE/img.jpg?width=1200&height=800&quality=85&coordinates=106%2C0%2C107%2C0');

}

button {

background-image: url('https://image.shutterstock.com/image-vector/mondrian-pattern-vector-design-diagonal-260nw-1724546761.jpg');

font-style: italic;

font-weight: bold;

padding: 15px 32px;

text-align: center;

text-decoration: none;

display: inline-block;

font-size: 35px;

margin: 4px 2px;

cursor: grab;

}

h1 {

background-image: url('https://i.gifer.com/OoMG.gif');

font-weight: bold;

font-size: 35px;

margin: 4px 2px;

cursor: pointer;

}

h2{

color:orange;

font-size:25px;

text-decoration: overline;

</style>

</head>

<h1 style="background-color: rgb(239, 210, 240); border-color: blue; color:red; display:block; margin: 0 auto;" >

FILE CRYPTOGRAPHY

</h1>

<br>

<br>

<br>

<h2> FILES <h2/>

<br>

<br>

<br>

<br>

<button style="background-color: rgb(9, 255, 0);

border-color: yellow;

color:brown;

display:block; margin: 0 auto;"

type="button"

onclick="file:///C:/Users/Student/Desktop/Murari'/mini%20project/file/encoding\_text.html">

<a href="file:///C:/Users/knajm/Desktop/Mini%20project/File/encoding.html"> ENCODE </a>

</button>

<br>

<br>

<br>

<button style="background-color: rgb(0, 255, 85);

border-color: yellow;

color:brown;

display:block; margin: 0 auto;"

type="button"

onclick="file:///C:/Users/Student/Desktop/Murari'/mini%20project/file/decoding.html">

<a href="file:///C:/Users/knajm/Desktop/Mini%20project/File/decoding.html">DECODE</a>

</button>

<body bgcolor="skyblue"></body>

**IMAGE:**

import math

from steno import database as db

import cv2

def encrypt\_image(img\_path: str, message: str, new\_path: str):

# load the image

img = cv2.imread(img\_path)

# break the image into its character level. Represent the characters in ASCII.

message = [format(ord(i), '08b') for i in message]

\_, width, \_ = img.shape

# algorithm to encode the image

pix\_req = len(message) \* 3

row\_req = pix\_req / width

row\_req = math.ceil(row\_req)

count, char\_count = 0, 0

for i in range(row\_req + 1):

while count < width and char\_count < len(message):

char = message[char\_count]

char\_count += 1

for index\_k, k in enumerate(char):

if (k == '1' and img[i][count][index\_k % 3] % 2 == 0) or (

k == '0' and img[i][count][index\_k % 3] % 2 == 1):

img[i][count][index\_k % 3] -= 1

if index\_k % 3 == 2:

count += 1

if index\_k == 7:

if char\_count \* 3 < pix\_req and img[i][count][2] % 2 == 1:

img[i][count][2] -= 1

if char\_count \* 3 >= pix\_req and img[i][count][2] % 2 == 0:

img[i][count][2] -= 1

count += 1

count = 0

# Write the encrypted image into a new file

cv2.imwrite(new\_path, img)

db.format\_oth('img', new\_path)

def decrypt\_image(img\_path: str):

# Algorithm to decrypt the data from the image

img = cv2.imread(img\_path)

data = []

stop = False

for index\_i, i in enumerate(img):

i.tolist()

for index\_j, j in enumerate(i):

if index\_j % 3 == 2:

# first pixel

data.append(bin(j[0])[-1])

# second pixel

data.append(bin(j[1])[-1])

# third pixel

if bin(j[2])[-1] == '1':

stop = True

break

else:

# first pixel

data.append(bin(j[0])[-1])

# second pixel

data.append(bin(j[1])[-1])

# third pixel

data.append(bin(j[2])[-1])

if stop:

break

message = []

# join all the bits to form letters (ASCII Representation)

for i in range(int((len(data) + 1) / 8)):

message.append(data[i \* 8:(i \* 8 + 8)])

# join all the letters to form the message.

message = [chr(int(''.join(i), 2)) for i in message]

return ''.join(message)

**AUDIO:**

<meta charset="UTF-8">

<meta http-equiv="x-ua-compatible" content="ie=edge">

<meta name="viewport" content="width=device-width, initial-scale=1.0">

<title>AUDIO</title>

<meta name="description" content="Hide secret text messages inside MP3 files. Just choose an MP3 of your choice, type in your message, and a new MP3 file will be created. To uncover the message, load the newly created file again. Optionally, you can choose to encrypt the message with a password for additional layer of security.">

<meta name="keywords" content="Steganography,Audio, MP3">

<link rel="icon" type="image/x-icon" href="assets/img/favicon.ico">

<link rel="stylesheet" type="text/css" href="../../node\_modules/bootstrap/dist/css/bootstrap.css">

<link rel="stylesheet" type="text/css" href="assets/css/style.css">

</head>

<body onload="enableHoverEffects()">

<div class="container">

<header>

<div class="row pb-4">

<div class="col-4 col-md-3">

<img src="assets/img/logo.svg" class="logo">

</div>

<div class="col-8 pl-0 align-self-end col-md-9 pl-md-4">

<h3 class="mt-3">Audio Steganography</h3>

</div>

</div>

</header> <div id="main">

<div class="row">

<div class="col-12 pb-4 pb-md-5 pt-md-4">

<div id="dropArea">

<img src="assets/img/mp3.svg" class="mp3">

<small>Drop a file here, or</small>

<button onclick="input.click()" type="button" class="btn btn-secondary btn-sm">Select File</button>

<input onchange="loadFile()" type="file" id="input" name="input" accept=".mp3"/>

</div>

</div>

</div>

<div class="row">

<div class="col-12">

<h5>How it works <span class="question-mark">?</span></h5>

</div>

</div>

<div class="row pb-3">

<div class="col-12 text-justify">

<p>

Hide secret text messages inside MP3 files. Just choose an MP3 of your choice, type in your message, and a new MP3 file will be created. To uncover the message, load the newly created file again. Optionally, you can choose to encrypt the message with a password for additional layer of security.

</p>

</div>

**BASE64:**

function atob() {

let textArea = document.getElementById('input1')

let input = textArea.value

document.getElementById('error-box').style.display = 'none'

if (textArea.classList.contains('error')) {

textArea.classList.remove('error')

textArea.value = ''

document.getElementById('input2').value = ''

return

}

let binaryCode = stringToEightBit(input)

let sixBitGroup = binaryToSixBit(binaryCode)

let encodedString = readSixBits(sixBitGroup)

document.getElementById('input2').value = encodedString

}

function btoa() {

let input = document.getElementById('input2').value

let binaryCode = numberToSixBitBinary(input)

let eightBitGroup = binaryToEightbit(binaryCode)

let decodedString = readEightBits(eightBitGroup)

document.getElementById('input1').value = decodedString

}

function stringToEightBit(string) {

if (!string) {

document.getElementById('input2').value = ''

return

}

const binaryCode = []

for (let i = 0; i < string.length; i++) {

let charCode = string.charCodeAt(i)

// convert character number to 8 bit

for (let j = 7; j >= 0; j--) {

let quotient = Math.floor(charCode / 2 \*\* j)

charCode = charCode % (2 \*\* j)

binaryCode.push(quotient)

}

}

return binaryCode

}

function binaryToSixBit(binaryCode) {

let sixBitGroup = []

let start = 0

let end = 6

let remainder = Math.floor(binaryCode.length % 6)

if (remainder) {

// making a flag to put "=" at the end of the encoded string :

flag = (remainder === 4) ? 1 : 2;

for (let n = 0; n < flag \* 2; n++) {

// Adding zeros to make the length divisible into six :

binaryCode.push(0)

}

}

**CHAPTER 10**

**REFERENCES**

[1] [Aditya Saxena](https://ieeexplore.ieee.org/author/37089472824) , [Ganga Maheshwari](https://ieeexplore.ieee.org/author/37089472399),” Digital Image Steganography”, 2021.

[Shital P. Rajput](https://ieeexplore.ieee.org/author/37086454241) , [Shital P. Rajput](https://ieeexplore.ieee.org/author/37086454241) , [Girish K. Patnaik](https://ieeexplore.ieee.org/author/37997397900) , ”An Efficient Audio Steganography Technique to Hide Text in Audio”, 2018.

[2] [Fahmi Anwar](https://ieeexplore.ieee.org/author/37087130193) , [Eko Hari Rachmawanto](https://ieeexplore.ieee.org/author/37086046813) , [Christy Atika Sari](https://ieeexplore.ieee.org/author/37086536435) , [De Rosal Ignatius Moses Setiadi](https://ieeexplore.ieee.org/author/37086320108),” StegoCrypt Scheme using LSB-AES Base64”, 2019.

[3] G Diwakara Reddy, Yaddanapudi VSSRR Udai Kiran, Prabhdeep Singh, Shubhranshu Vikram Singh, Sanchita Shaw, Jitendra Singh, ”A Proficient and secure way of Transmission using Cryptography and Steganography”, 2022.

[4] [Jeba Nega Cheltha C](https://ieeexplore.ieee.org/author/37089035468), [Manik Rakhra](https://ieeexplore.ieee.org/author/37086409223), [Rajan Kumar](https://ieeexplore.ieee.org/author/37089032592), [Himd weep Walia](https://ieeexplore.ieee.org/author/37085711949) , “A Review on Data hiding using Steganography and Cryptography”, 2021.

[5] Nazmun Nahar,Md. Kawsher Ahmed, Tareq Miah, Shahriar Alam, [Kh. Mustafizur Rahman](https://ieeexplore.ieee.org/author/37089330940),[Md. Anayt Rabbi](https://ieeexplore.ieee.org/author/37089333533), “Implementation of Android Based Text to Image Steganography Using 512-Bit Algorithm with LSB Technique”, 2021

[6] [N. Manohar](https://ieeexplore.ieee.org/author/37089219640), [Peetla Vijay Kumar](https://ieeexplore.ieee.org/author/37088426158),“ Data encryption and decryption using steaganography ”, 2020.

# [7] Nandhini Subramanian, Omar Elharrouss, Somaya Al-Maadeed, Ahmed Bouridane,” Image Steganography: A Review of the Recent Advances”,2021.

# [9] Varun R V; Soumiya K. S, “Exploring the Effectiveness of Steganography Techniques: A Comparative Analysis“, 2023

# [8] Weixuan Tang; Bin Li; Mauro Barni; Jin Li; Jiwu Huang,” Steganography Using Deep Reinforcement Learning”,2022.