

KRYPTOCRACK - A STEGANOGRAPHIC TOOL

Submitted in partial fulfillment of the requirements for the award of
Bachelor of Technology degree in
Information Technology

By
SUSIL KUMAR R.M (Reg.No - 39120128)
SUJAY R (Reg.No - 39120122)



DEPARTMENT OF INFORMATION TECHNOLOGY
SCHOOL OF COMPUTING

SATHYABAMA

INSTITUTE OF SCIENCE AND TECHNOLOGY
(DEEMED TO BE UNIVERSITY)

Accredited with Grade "A" by NAAC | 12B Status by UGC | Approved by AICTE
JEPPIAAR NAGAR, RAJIV GANDHI SALAI,
CHENNAI - 600119

MAY- 2023

KRYPTOCRACK – A STEGANOGRAPHIC TOOL

Submitted in partial fulfillment of the requirements for the award of
Bachelor of Technology degree in
Information Technology

By
SUSIL KUMAR R.M (Reg.No - 39120126)
SUJAY R (Reg.No – 39120122)



DEPARTMENT OF INFORMATION TECHNOLOGY
SCHOOL OF COMPUTING

SATHYABAMA

INSTITUTE OF SCIENCE AND TECHNOLOGY
(DEEMED TO BE UNIVERSITY)

Accredited with Grade "A" by NAAC | 12B Status by UGC | Approved by AICTE
JEPPIAAR NAGAR, RAJIV GANDHI SALAI,
CHENNAI - 600119

MAY- 2023



SATHYABAMA

INSTITUTE OF SCIENCE AND TECHNOLOGY
(DEEMED TO BE UNIVERSITY)

Accredited with Grade "A" by NAAC | ISO Status by ISO | Approved by AICTE

www.sathyabama.ac.in

DEPARTMENT OF INFORMATION TECHNOLOGY

BONAFIDE CERTIFICATE

This is to certify that this Project Report is the bonafide work of **SUSIL KUMAR R.M** (Reg.No - 39120126) and **SUJAY R** (Reg.No - 39120122) who carried out the Project Phase-2 entitled "**KRYPTOCRACK - A STEGANOGRAPHIC TOOL**" under my supervision from January 2023 to May 2023

[Signature]
Internal Guide

Dr. G. MATHIVANAN, M.E., Ph.D.,

[Signature]
Head of the Department

Dr. R. SUBHASHINI M.E., Ph.D.

Submitted for Viva voce Examination held on 11.05.2023

[Signature]
Internal Examiner

[Signature]
External Examiner

DECLARATION

I, **SUSIL KUMAR R.M** (Reg.No- 39120126), hereby declare that the Project Phase-2 Report entitled "**KRYPTOCRACK – A STEGANOGRAPHIC TOOL**" done by me under the guidance of **Dr. G. MATHIVANAN, M.E., Ph.D.**, is submitted in partial fulfillment of the requirements for the award Bachelor of Technology degree in Information Technology.

DATE: 11.05.2023

PLACE: Chennai



SIGNATURE OF THE CANDIDATE

ACKNOWLEDGEMENT

I am pleased to acknowledge my sincere thanks to **Board of Management of SATHYABAMA** for their kind encouragement in doing this project and for completing it successfully. I am grateful to them.

I convey my thanks to **Dr. T. Sasikala M.E., Ph. D.** Dean, School of Computing, **Dr. R. SUBHASHINI M.E., Ph.D.** Head of the Department, Department of Information Technology for providing me necessary support and details at the right time during the progressive reviews.

I would like to express my sincere and deep sense of gratitude to my Project Guide **Dr. G. MATHIVANAN M.E., Ph.D.**, for her valuable guidance, suggestions and constant encouragement paved way for the successful completion of my phase-2 project work.

I wish to express my thanks to all Teaching and Non-teaching staff members of the **Department of Information Technology** who were helpful in many ways for the completion of the project.

ABSTRACT

"Kryptocrack is a cryptographic/Steganographic tool that deals with Hash, crypto analysis, and steganography."

Cryptography & Steganography place a vital role when it comes to data sharing in a secure manner throughout the internet. The reason is information security is not a feature it is a necessary thing. But the enumeration part of penetration testing is a little time-consuming mind because of using multiple tools, several scripts, comprehensive strategy, and custom techniques and it is also used in military secret operations, cryptography & Steganography place a vital role when it securely comes to data sharing throughout the internet. The reason is information security is not a feature it is a necessary thing. Need most of the malware will come from images, videos or files. The malware files are collected and tested using the Metadata collector. This type of tool is used for a secure conversation. For example, if I am a Krypto analyst, I am getting any messages in hash values, and I have to check whether the message is suspicious or not. It is based on a blue teaming job which means, a blue team is a group of individuals who perform an analysis of information systems to ensure security, identify security flaws, verify the effectiveness of each security measure, and make certain all security measures will continue to be effective after implementation. Uses of my tool it identifies the given Hash values - Encrypt, Decrypt the hidden messages in files, videos, and images. My tool doesn't have a particular purpose it can perform both Blue Team and Red Team (provides security) operations. Overall, in cyber security Kryptocrack plays a major role.

TABLE OF CONTENTS

CHAPTER	TITLE	PAGE NO
	ABSTRACT	v
	LIST OF FIGURES	viii
	LIST OF ABBREVIATIONS	ix
1	INTRODUCTION	1
	1.1 Cyber Security	1
	1.2 Steganography	2
	1.3 Types of Steganography	2
2	LITERATURE SURVEY	6
	2.1 Inferences From Literature Survey	8
3	REQUIREMENTS ANALYSIS	10
	3.1 Software Requirements	10
4	DESCRIPTION OF PROPOSED SYSTEM	13
	4.1 Methodology	13
	4.2 Architecture Design of Proposed System	17
	4.3 Project Management Plan	19
	4.4 Description of Software for Implementation	20
5	IMPLEMENTATION DETAILS	21
	5.1 Commands Involved in the Tool	21
6	RESULTS AND DISCUSSION	25
7	CONCLUSION	26
	7.1 Conclusion	26
	7.2 Future Work	26
	REFERENCES	28
	APPENDIX	29
A	SOURCE CODE	29

B	SNAP SHOTS	39
C	RESEARCH PAPER	44

LIST OF FIGURES

FIGURE NO	FIGURE NAME	PAGE NO
1.3.1	Types of Steganography	2
1.3.2	Processed Image Steganography	4
3.1.1	VMware Environment	10
3.1.2	Kali Linux in VMware	11
3.1.3	VS code Environment	11
3.1.4	Logo of Bash	12
4.1.1	Hashing	13
4.1.2	Convert text to Hash md5	13
4.1.3	Convert text to Hash SHA1	14
4.1.4	Convert text to Hash SHA256	14
4.1.5	Convert text to Hash SHA512	14
4.1.6	Whitespace Steganography embed	17
4.1.7	Whitespace Steganography extract	17
4.2.1	Architecture Diagram	18
4.2.2	Workflow Diagram	19
5.1.1	Confirms the folder and path	21
5.1.2	Listing tools using various technologies	22
5.1.3	Text File to hash	22
5.1.4	List hashing tools	23
5.1.5	Final Output	24

10

5
5
4
4
3
3

CHAPTER 1

INTRODUCTION

1.1 CYBER SECURITY

Cyber Security is the practice of protecting critical systems and sensitive information from digital attacks. Also known as Information Technology Security and Ethical Hacking. It is the protection of computer systems and networks from information disclosure, theft of or damage to their hardware, software, or electronic data, as well as from the disruption or misdirection of the services they provide. It is otherwise known as Computer Security or Information Technology security. There are four stages in cyber security. They are,

- 1) Information Gathering
- 2) Enumeration/Scanning
- 3) Vulnerability Assessment
- 4) Reporting

The field of cyber security encompasses a wide range of technologies, practices, and policies aimed at safeguarding computer systems and networks against cyber-attacks, which may come in various forms such as viruses, malware, phishing, ransomware, and social engineering attacks.

Some common cyber security technologies and practices include firewalls, intrusion detection and prevention systems, antivirus software, encryption, access controls, incident response planning, and security awareness training for employees. As is appropriate, network security has grown to be among the top priorities in the modern world, including both individual users and programmers. The predominant aim of this system is to discover the operating system, host detection, scan open ports and detect vulnerabilities. Then it gives protection to secure the web-based system as well as illustrates every aspect of the program's features. Next, the OSINT framework will outcome gather information about an individual or organization. After using Cryptography is an essential appliance for securing information in the computer and it will examine the hash type and encrypts the hash passwords.

1.2 STEGANOGRAPHY?

Steganography is the practice of hiding secret information or messages within non-secret data or information in such a way that only the intended recipient can detect or extract it. The goal of steganography is to conceal the existence of the secret message, rather than to keep its contents secret through encryption.

Steganography can be achieved by various techniques such as hiding information within images, videos, audio files, text files, or other types of digital data. For example, a steganographic technique might involve modifying the least significant bits of a digital image or audio file to encode the secret message, while the modified data appears almost identical to the original file.

Steganography has been used for both malicious and benign purposes. In the past, it has been used by spies, terrorists, and criminals to transmit secret messages or to hide their communication from detection. However, it can also be used for legitimate purposes, such as digital watermarking, copyright protection, or to exchange private information over the internet.

1.3 TYPES OF STEGANOGRAPHY

Depending on the nature of the cover object (actual object in which secret data is embedded) Steganography can be divided into four types:

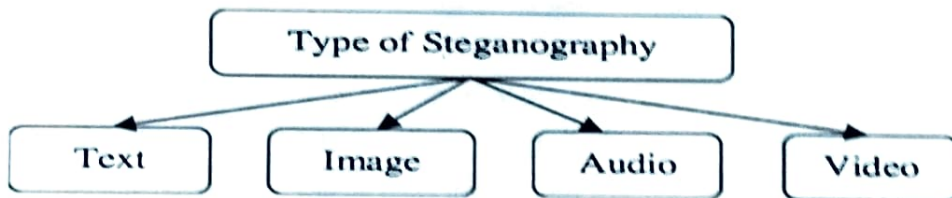


Fig.1.3.1 Types of Steganography

a) Text Steganography

Since everyone can read, encoding text in neutral sentences is doubt fully effective. But taking the first letter of each word of the previous sentence, you will see that it is possible and not very difficult. Hiding a Tutorial Review on Steganography 107 information in plain text can be done in many different ways.

Many techniques involve the modification of the layout of a text, rules like using every nth character, or the altering of the amount of white space after lines or between words. The last technique was successfully used in graphics and even after a text has been printed and copied on paper ten times, the secret message could still be retrieved. Another possible way of storing a secret inside a text is using a publicly available cover source, a book, or a newspaper, and using a code that consists for example of a combination of a page number, a line number and a character number. This way, no information stored inside the cover source will lead to the hidden message. Discovering it relies solely on gaining knowledge of the secret key.

b) Image Steganography

As stated earlier, images are the most popular cover objects used for steganography. In the domain of digital images many different image file formats exist, most of them for specific applications. For these different image file formats different steganographic algorithms exist.

To a computer, an image is a collection of numbers that constitute different light intensities in different areas. This numeric representation forms a grid and the individual points are referred to as pixels. Most images on the Internet consist of an angular map of the image's pixels (represented as bits) where each pixel is located and its color. These pixels are displayed horizontally row by row. The number of bits in a color scheme, called bit depth, refers to the number of bits used for each pixel. The smallest bit depth in current color schemes is 8, meaning that there are 8 bits used to describe the color of each pixel. Monochrome and greyscale images use 8 bits for each pixel and are able to display 256 different colors or shades of grey. Digital color images are typically stored in 24-bit files and use the RGB color model, also known as true color. All color variations for the pixels of a 24-bit image are derived from three primary colors: red, green, and blue, and each primary color is represented by 8 bits. Thus, in one given pixel, there can be 256 different quantities of red, green, and blue, adding up to more than 16 million combinations, resulting in more than 16 million colors. Not surprisingly, larger the number of colors that can be displayed, larger is the file size.

Least significant bit (LSB) insertion is a common and simple approach to embedding information in an image file. In this method, the LSB of a byte is replaced with an M's bit. This technique works well for image, audio, and video Steganography.



The cover image



The stego-image (after A is inserted)

Fig.1.3.2 Processed Image Steganography

c) Audio Steganography

Audio Steganography In a computer-based audio steganography system, secret messages are embedded in digital sound. The secret message is embedded by slightly altering the binary sequence of a sound file. Existing audio steganography software can embed messages in WAV, AU, and even MP3 sound files. Embedding secret messages in digitals.

Embedding secret messages in digital sound is usually a more difficult process than embedding messages in other media, such as digital images. In order to conceal secret messages successfully, a variety of methods for embedding information in digital audio have been introduced. These methods range from rather simple algorithms that insert information in the similar to watermarks on actual paper and are sometimes used as digital watermarks. Masking images entails changing the luminance of the masked area. The smaller the luminance change, the less of a chance that it can be detected. Observe that the luminance in Figure 2 is at 15% in the mask region if it was decreased then it would be nearly invisible [1,4, 5]. Masking is more robust than LSB insertion with

respect to compression, cropping and some image processing. Masking techniques embed information insignificant are as so that the hidden message is more integral to the cover image than just hiding it in the "noise" level. This makes it more suitable than LSB with, for instance, loss of JPEG images. A Tutorial Review on Steganography 109 form of signal noise to more powerful methods that exploit sophisticated signal processing techniques to hide information. The list of methods that are commonly used for audio steganography is listed and discussed below.

- LSB coding
- Parity coding
- Phase coding
- Spread spectrum
- Echo hiding

d) Video Steganography

Video steganography is a technique of hiding secret information or messages within digital video files. The technique is similar to image steganography, but instead of modifying individual pixels, it involves embedding the secret message within video frames or data packets. There are several methods of video steganography, including the frame manipulation method, the data hiding method, and the compressed domain method.

The frame manipulation method involves embedding the secret message by manipulating the video frames' luminance or color components. This method can be easily detected by analyzing the video's statistical properties. The data hiding method involves hiding the secret message within the data packets of the video stream.

This method is more complex than the frame manipulation method but provides better security. The compressed domain method involves embedding the secret message within the compressed video data. This method is more secure than the frame manipulation method and provides better compression ratios. Video steganography is often used for covert communication, digital watermarking, or to protect the privacy of confidential information. However, it can also be used for malicious purposes, such as hiding illegal or harmful content within a video.

CHAPTER 2

LITERATURE SURVEY

1) An Image-based Steganography model for promoting Global Cyber Security by Souvik Bhattacharyya and Gautam Sanyal at the proceedings of "International Conference on Systems, Cybernetics and Informatics".

2) An assumption can be made based on this model is that if both the sender and receiver share some common secret information the corresponding steganography protocol is known as then the secret key steganography where as pure Steganography means that there is none prior information shared by sender and receiver.

3) An extensive review of stenographic techniques in different domains has been provided. Special emphasis has been given on the insightful analysis is on the under developed aspects or fail cases of the state-of-the-art works. We have also provided a comparative analysis of the recent state-of-the-art works.

4) Performance measurement criteria of a steganographic technique like capacity, quality, and security have been discussed in detail. Security of the techniques have been analyzed by various state-of-the art attacks like RS analysis, PDH attack, relative entropy, steganalysis tools like Steg Expose, and benchmark tool like Stir Mark Benchmark 4.0, etc.

5) In 2021, Osama Fouad Abdel Wahab&, Ashraf A. M. Khalaf proposed Hiding Data Using an Efficient Combination of RSA Cryptography, and Compression Steganography Techniques. Data compression is an important part of information security because compressed data is more secure and easy to handle. Effective data compression technology creates efficient, secure, and easy-to-connect data. The main objective of this study was to reduce the physical space on the various storage media and reduce the time of sending data over the Internet with a complete guarantee of encrypting this data and hiding it from intruders.

6) In 2019, Da-Chun Wu and Hsiu-Yang Su proposed steganography via E-Books with the EPUB Format by Rearrangements the Contents of the CSS Files. With the advance of information technology and mobile devices, e-book reading has become a popular way for people to gain knowledge. However, with the widespread use of digital texts, issues about the copyright protection of e-books have arisen. The electronic publication (EPUB) format is currently one of the most widely used e-book formats. Recently, e-books, which are convenient to use anywhere at any time without paper assumptions, have had a significant influence on people's reading habits.

7) In 2019, Tabares-Soto Reinel & Ramos-Pollán Raúl proposed a Deep Learning Applied to the Steganalysis of Digital Images: A Systematic Review. Steganography consists of hiding messages inside some object known as a carrier to establish a covert communication channel so that the act of communication itself goes unnoticed by observers who have access to that channel. Steganography consists of hiding messages inside digital multimedia files (images, sound, and video) imperceptibly for any receiver. The first documents describing the use of these techniques date back to the times of Herodotus in ancient Greece.

8) In 2020, Ali Maetouq and Salwani Mohd Daud proposed a Hash Function Based on New Mersenne Number Transform. In the field of information security, hash functions are considered important as they are used to ensure message integrity and authentication. I. Cryptographic hash functions, one of the most important cryptographic primitives can be used to ensure the security of many cryptographic applications and protocols, including message authentication code, integrity, digital signature, and random number generation.

9) In 2020, Ammar Mohammed Ali and Alaa Kadhim Farhan proposed a Novel development With an Effective Expansion to Enhance the MD5 Hash Function for confirmation of a Secure E-Document. MD5 is a one-way cryptographic function used in various fields for maintaining data integrity. The application of a Hash function can provide much protection and privacy and subsequently reduce data

usage. This algorithm has characteristics that enable it to succeed in the field of digital authentication and data integrity. The large interest in information security has centered on the balanced protection of the confidentiality, integrity, and availability of data, with the amount of data required to be analyzed and provided for protection continuously varying with every case.

10) In 2019, Arnold Gabriel Benedict proposed a developed File Security System Using Multiple Image Steganography. Steganography is the process of hiding a secret message within an ordinary message & extracting it at its destination. Image steganography is one of the most common and secure forms of steganography available today. Steganography is the process of hiding a secret message within an ordinary message & draw out it to its destination. Image steganography is one of the most common and secure forms of steganography available today.

2.1 INFERENCES FROM LITERATURE SURVEY

From a literature survey on steganography, several inferences can be drawn. They are follows below,

- 1) **Steganography techniques are constantly evolving:** As new technologies and encryption techniques emerge; steganography techniques also evolve to keep up with these changes. Steganography researchers are always seeking new ways to hide data in digital media, and this field is continually advancing.
- 2) **Steganography is a valuable tool for secure communication:** Steganography provides a means for secure communication without arousing suspicion. It is used in a variety of fields, including military, law enforcement, and finance, to protect sensitive data and prevent unauthorized access.
- 3) **Steganography can be used for both benign and malicious purposes:** While steganography can be used for legitimate purposes such as secure communication, it can also be used for malicious purposes such as hiding malware or illegal content.

- 4) **The detection of steganography is an ongoing challenge:** Detecting steganography can be difficult because it is designed to blend in with the digital media it is hiding in. As steganography techniques become more sophisticated, detecting them becomes increasingly challenging.
- 5) **Steganography is not fool proof:** While steganography provides a means of secure communication, it is not fool proof. There is always a risk that the hidden data may be discovered or that the encryption may be broken.

Overall, steganography is a complex and evolving field that offers both benefits and challenges. While it provides a valuable tool for secure communication, there is always a risk that it may be used for malicious purposes, and detecting steganography remains an ongoing challenge.

CHAPTER 3

REQUIREMENTS ANALYSIS

3.1 SOFTWARE REQUIREMENTS

a) VMware (Virtualization Box)

VMware is a software that enables users to virtualization. It is virtual machines of the ware from VMware. It enables multiple copies of the same operating system, or there can be several different operating systems that can run simultaneously on the same. VMware's virtualization technology one would be able to run another machine within another physical machine and perform all tasks. Hypervisor abstracts the software from PC's hardware and thus creates and manages the virtual machines.



Fig.3.1.1 VMware Environment

b) Kali Linux (Main Operating System)

Kali Linux is Debian-based Linux distribution. Kali Linux is a specially designed OS for network analysts, Penetration testers. It is completely free and open source. So, you can use it for free and even contribute for its development. That is easily accessible and offered for free to information security experts and enthusiasts. Supported platform of the Metasploit able a vulnerable machine for developing and executing security exploits.

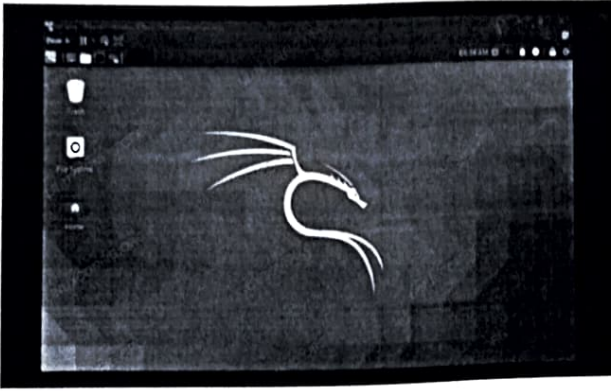


Fig.3.1.2 Kali Linux in VMware

c) Visual Studio Code (Text Editor)

Visual Studio Code also commonly referred to as VS Code, is a source-code editor made by Microsoft with the Electron Framework, for Windows, Linux, and macOS. Features include support for debugging, syntax highlighting, intelligent code completion, snippets, code refactoring, and embedded Git. Users can change the theme, keyboard shortcuts, and preferences, and install extensions that add additional functionality. In the Stack Overflow 2021 Developer Survey, Visual Studio Code was ranked the most popular developer environment tool among 82,000 respondents, with 70% reporting that they use it.



Fig.3.1.3 VS code Environment

d) Python3

Python is a high-level, general-purpose programming language. Its design philosophy emphasizes code readability with the use of significant indentation. Python is dynamically-typed and garbage-collected. It supports multiple programming paradigms, including structured (particularly procedural), object-oriented, and functional programming. It is often described as a "batteries included" language due to its comprehensive standard library.

Python is commonly used for developing websites and software, task automation, data analysis, and data visualization. Since it's relatively easy to learn, Python has been adopted by many non-programmers such as accountants and scientists, for a variety of everyday tasks, like organizing finances. Some common use cases for Python include web development, scientific computing, data analysis, artificial intelligence, and automation. Python is also frequently used as a scripting language for automating tasks on Unix-based systems. Python has a simple and easy-to-learn syntax, making it a great language for beginners. It is also popular among experienced developers due to its efficiency and versatility.

e) Bash

BASH (Bourne Again Shell) is a shell program. SHELL is the command interpreter for the Operating System. It is a command line language for UNIX-based Operating Systems. It allows you to control the computer like a developer. It is a command language that allows us to work with the file on the computer in a way that's more efficient and powerful than a Graphical User Interface (GUI). It provides functional improvements over Bourne Shell for both programming and interactive use. The file must be saved with the extension of .sh.



Fig.3.1.4 Logo of Bash

CHAPTER 4

DESCRIPTION OF PROPOSED SYSTEM

4.1 METHODOLOGY

1) Convert text to Hash md5, sha1, sha256, sha512

Hashing is a process of taking an input (in this case, text) and generating a fixed-length output string that represents the input. This output string is called a hash. Hashing is a one-way process, which means that it is easy to generate a hash from input, but it is practically impossible to generate the original input from the hash. There are several hash algorithms available, including MD5, SHA1, SHA256, and SHA512. These algorithms differ in their security, speed, and output size.

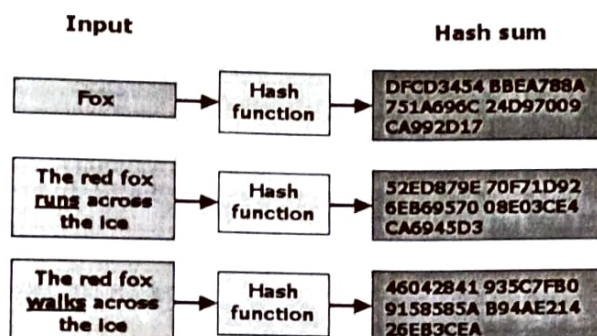


Fig.4.1.1 Hashing

2) Convert text to Hash md5

MD5 is a widely used algorithm that generates a 128-bit hash. It is fast and has been used for various purposes such as file integrity checks, password storage, and digital signatures. However, it is no longer considered secure for cryptographic purposes due to its vulnerability to collisions.

```
> Enter The Option from [1-12] OR [exit] to Exit $ 1
> Enter Text : susil
> Enter Hash Format (MD5, SHA1, SHA256, SHA512): md5
a0c9596abd3c888b665551d29d7dac63 -
0
```

Fig4.1.2 Convert text to Hash md5

3) Convert text to Hash SHA1

SHA1 is another widely used algorithm that generates a 160-bit hash. It is slightly slower than MD5 but provides better security. However, it has also been found to be vulnerable to collisions, and it is recommended to use stronger algorithms.

```
> Enter The Option from [1-12] OR [exit] to Exit $ 1
> Enter Text : susil
> Enter Hash Format (MD5, SHA1, SHA256, SHA512): sha1
e358b1cbf55d212e9a29955eefc491cb401e0047 -
0
```

Fig.4.1.3 Convert text to Hash SHA1

4) Convert text to Hash SHA256

SHA256 is a stronger algorithm that generates a 256-bit hash. It is slower than MD5 and SHA1 but provides better security due to its larger output size. It is commonly used for digital signatures, password storage, and SSL/TLS certificates.

```
> Enter The Option from [1-12] OR [exit] to Exit $ 1
> Enter Text : sha256
> Enter Hash Format (MD5, SHA1, SHA256, SHA512): sha256
5d5b09f6dcb2d53a5fffc60c4ac0d55fabdf556069d6631545f42aa6e3500f2e -
0
```

Fig.4.1.4 Convert text to Hash SHA256

5) Convert text to Hash SHA512

SHA512 is an even stronger algorithm that generates a 512-bit hash. It is slower than SHA256 but provides better security due to its larger output size. It is recommended for applications that require the highest level of security, such as government and military applications.

```
> Enter The Option from [1-12] OR [exit] to Exit $ 1
> Enter Text : susil
> Enter Hash Format (MD5, SHA1, SHA256, SHA512): sha512
d4fcf2976e7054e027a257fb193a765c7f55ebf9704d800c47cfdcf820ce430e9612f185c4bd9bad370a7ffbf9020c97138e0262754df9fb0f966239adbdb8d6 -
0
```

Fig.4.1.5 Convert text to Hash SHA512

6) Cryptography Process

- Hash Identifier

Hash-identifier is also helpful for identifying which hashing algorithm is being used to provide a checksum value for a download. And it can be used

to determine what program a hashed file or value may belong to, such as an SQL database or another vendor-specific format. A hashing function turns the readable passwords into jumbled-up messes of letters and numbers that should not be able to be reverse-engineered. Software that can distinguish between the various hashing algorithms used to secure data, particularly passwords. Data exchange between integrated data management systems is done using the encryption method of hashing. The hashing identifier in Eloqua can be used to practice and recognize two different types of hashes in order to exchange phone numbers and email addresses in an unidentified fashion. The capability provides hashed versions of the recent contact field information and allows you to map these details to other systems without providing any Personal Identifiable Information (PII). The performance uses SHA256 hashes to peculiar identify contacts.

- **John The Ripper**

The tool for breaking passwords John the Ripper can recognize the majority of password hash types and offers a user-friendly command-line interface. Some of the key features of the tool include offering multiple modes to speed up password cracking, automatically detecting the hashing algorithm used by the encrypted passwords, and the ease of running and configuring the tool making it a password cracking tool of choice for novices and professionals alike. John the Ripper is a password cracker that works offline. In other words, it searches collected data for passwords without getting in touch with the target. Due to the fact that the method is often performed locally, on the attacker's workstation, this prevents the production of suspicious traffic. Although its primary application is to decrypt password hashes, John may also be used to decrypt encrypted private keys, secured archive files, and many other kinds of data.

- **Hashcat (Hash Cracking)**

Hashcat is a well-known and efficacious passcode cracker that is used by penetration testers, system administrators, perpetrators, and intelligence agencies. The Hashcat seems to be a multi-threading functionality that allows you to set the numerous threads and prioritize execution. Password

cracking differs from assuming a site username and password, which typically allows only one limited set of assumptions before holding the account. Rather, anyone who has managed to gain access to a computer system containing encryption keys ("hashes") will often attempt to break those hash values in order to retrieve the passwords. Hashcat is a particularly fast, efficient, and versatile hacking tool that assists brute-force attacks by conducting them with hash values of passwords that the tool is guessing or applying. When used for benign purposes, such as in penetration testing one's own infrastructure, it can reveal compromised or easy-to-guess credentials. Penetration testers on engagement will frequently find themselves cracking stolen password hashes to move laterally inside a network, or to escalate privileges to an admin user. Since penetration testers work to find security holes on purpose, under contract, so that their customer can improve their security, this is also a perfectly legitimate use case.

7) Steganography Process

Steganography is the practice of concealing secret information within other non-secret data such as text, image, video, or audio files in such a way that it does not appear to be modified or tampered with. The goal of steganography is to hide the existence of the secret message from an observer. Steganography techniques can be divided into two main categories: spatial domain and transform domain. In the spatial domain, the secret message is hidden in the least significant bits of the cover data, such as the least significant bits of an image's pixel values.

The science of protecting communications from outside observers is known as cryptography. Take the original communication, or plaintext, and change it into unintelligible ciphertext. The user can view the communication since the key enables them to decode it. It is also examined how strong encryption's randomness is, which makes it more difficult for someone to predict the algorithm's input or key. We can increase our privacy by using cryptography to create connections that are more secure and reliable. Due to improvements in cryptography, only authorized users should be able to access encrypted files, folders, or network connections. Raw data can be safeguarded via encryption in

addition to combining data into a secure configuration. Crypto encodes messages and data to prevent anyone other than the destination node from seeing, interpreting, or processing it. In the modern era, encoding is used to safeguard metadata. A goal of this computational science field is to organize details in a manner that only permits users can perceive.

Whitespace steganography is a type of steganography where the secret information is hidden within the whitespace characters (space, tab, newline) of a text document. This type of steganography is also known as space steganography or text steganography. Whitespace steganography works by embedding the secret message within the whitespace characters of a text document, such that the document appears unchanged to the human eye. This is achieved by replacing the whitespace characters with hidden characters that represent the secret message. The hidden characters can be either visible or invisible, depending on the technique used. One common technique for whitespace steganography is called zero-width non-joiner (ZWNJ) steganography.

```
> Enter The Option from [1-12] OR [exit] to Exit $ 9
> Enter Filename : susil.txt
> Enter the Message : iwillkillyou
> Enter Hidden Filename : hide.txt
> Enter the Message to Hide (No space): letmein
> Enter Password : susil
```

Fig.4.1.6 Whitespace Steganography embed

```
> Enter The Option from [1-12] OR [exit] to Exit $ 10
> Enter Hidden Filename : hide.txt
> Enter Password : susil
letmein0
```

Fig.4.1.7 Whitespace Steganography extract

4.2 ARCHITECTURE DESIGN OF PROPOSED SYSTEM

System architecture refers to the overall design and organization of a system, including its components, their interactions, and the principles and guidelines that govern their construction and evolution. The purpose of system architecture is to ensure that the system meets its functional and non-functional

requirements, while also being scalable, maintainable, and extensible. It provides a blueprint for the system, defining its components and how they fit together to achieve the desired functionality.

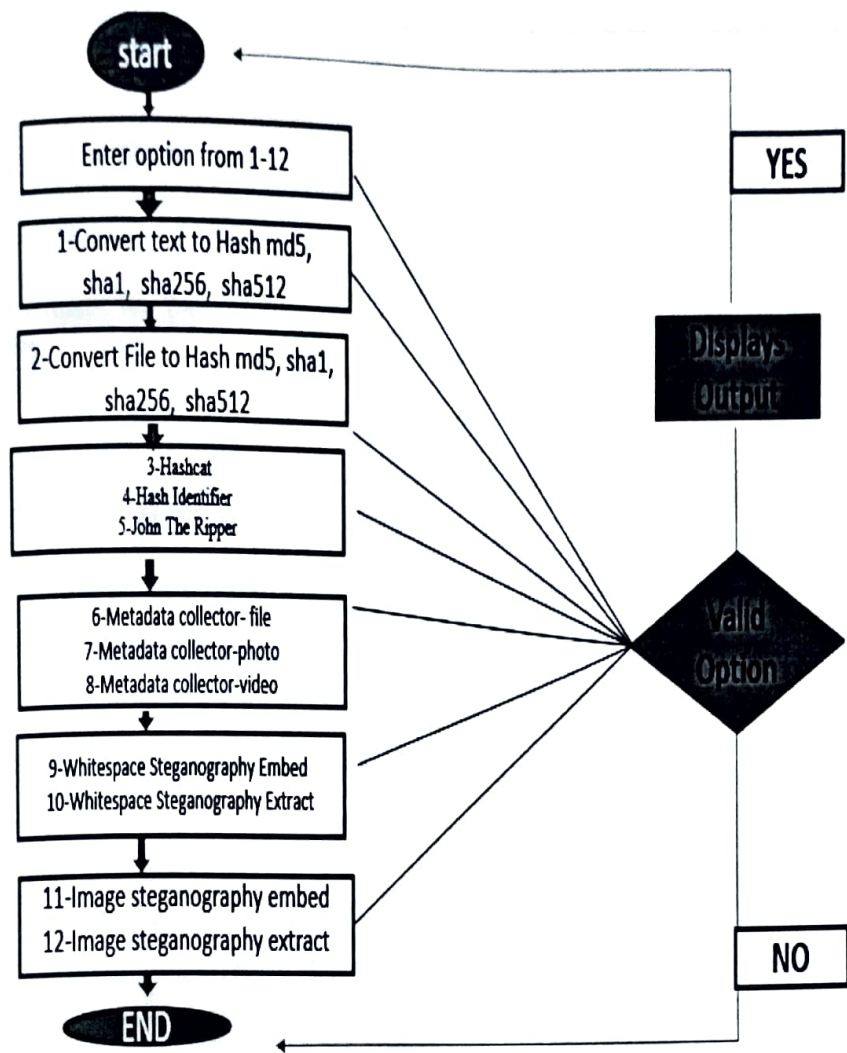


Fig.4.2.1 Architecture Diagram

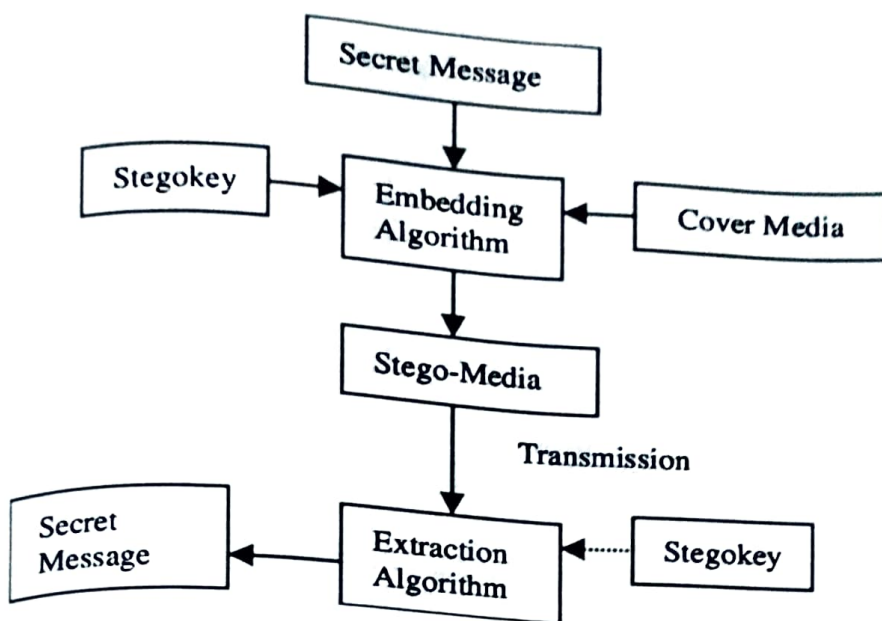


Fig.4.2.2 Workflow Diagram

4.3 PROJECT MANAGEMENT PLAN

- a) KRYPTOCRACK gives highly accurate data comes to pen testing and digital forensic
- b) It is much more stable in Linux.
- c) Even though some tools are efficiently available, I combined all tools in a single comprehensive script.
- d) The tool is made up of Python3 and bash script, it allows you to control the computer like a developer.
- e) This helps to give accuracy and precision and reduces the time
- f) It a very little time-consuming owing to the employment of numerous tools, and scripts, including thorough techniques in one script in order to ensure that it is unified.
- g) As the project is developed of various technologies built in single scripts to make time intensive so it is integrated
- h) It moves concerning quickly and conveniently employs all of the mentioned tools to their fullest extent utilizing only a single all-encompassing script.

4.3 DESCRIPTION OF SOFTWARE FOR IMPLEMENTATION

Python3 is a computer programming language that is frequently used to create applications and websites, automate procedures, and analyze data. Python3 is not specialized for any particular issue and may be employed to develop a wide range of diverse programming. Python supports modules and packages, which encourages program modularity and code reuse. Python also has a number of libraries that enable coders to write programs for data analysis. It is fully extensible as well as works well with other libraries and this language is perfectly suited to develop your tool. Its adaptability and complete novice-friendliness have elevated its position at the top of the list of languages for programming in practice nowadays.

BASH (Bourne-Again SHELL) is a popular Unix shell, a command-line interface for interacting with a computer's operating system. BASH is an enhanced version of the original Bourne shell (.sh) and is the default shell for most Linux distributions, as well as macOS. BASH allows users to enter commands and execute them on the system. It provides a powerful scripting language for automating tasks and manipulating files and directories. BASH also supports command line editing, command history, and job control, allowing users to manage multiple processes and jobs simultaneously.

Some common BASH commands include

- ls: lists files and directories in the current directory
- cd: changes the current working directory
- mkdir: creates a new directory
- rm: removes a file or directory
- cp: copies a file or directory
- mv: moves or renames a file or directory
- echo: prints a message to the console
- cat: prints the contents of a file to the console

BASH also allows users to create custom scripts, which can be used to automate complex tasks or perform repetitive actions. BASH scripts can be executed from the command line or scheduled to run at specific times using cron.

CHAPTER 5

IMPLEMENTATION DETAILS

5.1 COMMANDS INVOLVED IN THE TOOL

This tool supports both Blue Teamer/ Red Teamer to enumerate information in disparate technologies like Hashing, embed, extract the secret message, and steganography. Install the VMware player (virtual box), and Kali Linux. Then Import the Kali Linux to the VMware player, once it is imported then do the configuration to get that in the working process.

First, you open the VMware and then boot the Kali Linux, once that opens type the password to get into the Kali Linux. Then open the terminal. In that terminal type, the command that command will confirm the path or folder and whether we use the right folder or not.

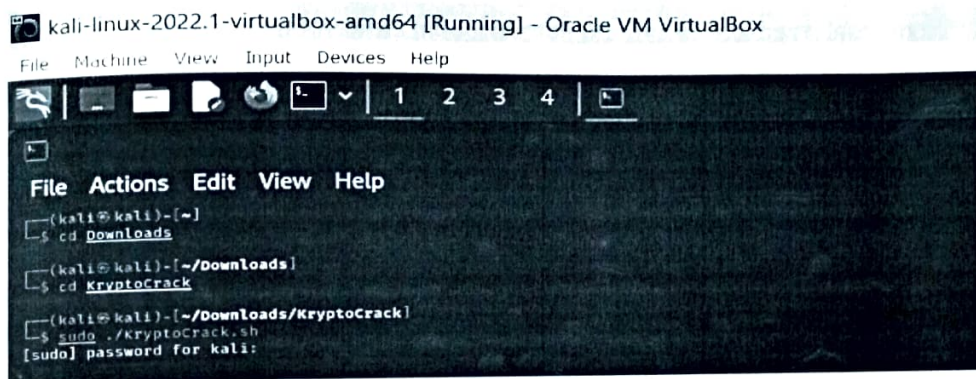


Fig.5.1.1 Confirms the folder and path

Once it has been done it will pop up a sudo password for Kali, type the correct password then only it will allow you to proceed further. Again, type the command ls it will list the tools or technologies and the technologies it will display the available service or tool as well as choose the available service.

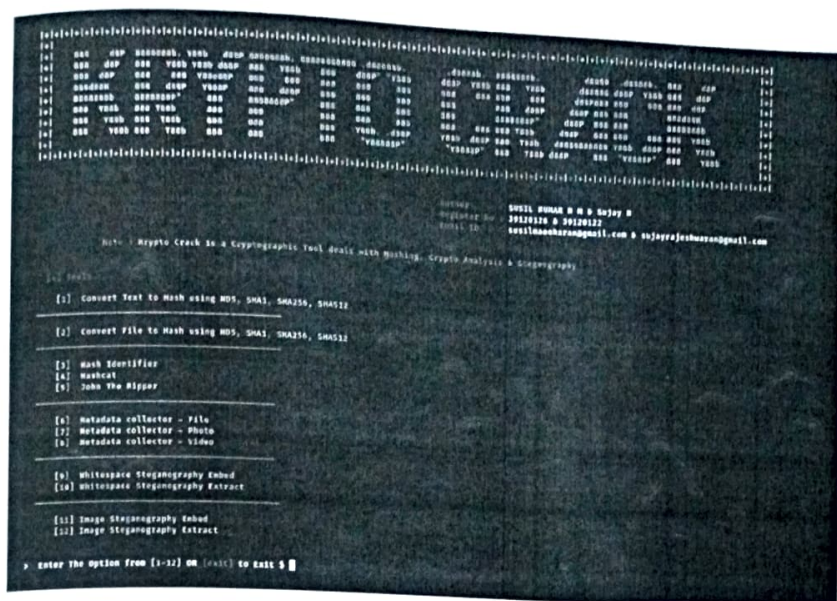


Fig.5.1.2 Listing tools using various technologies

Further, the process is a little bit quite a difference because here we using various technologies in a single script to make the process will consume less time for testing. This tool will support disparate technologies like Hashing, Metadata collector, Image and white space steganography.

Hashing is a process of taking an input (in this case, text) and generating a fixed-length output string that represents the input. This output string is called a hash. Hashing is a one-way process, which means that it is easy to generate a hash from an input, but it is practically impossible to generate the original input from the hash.

There are several hash algorithms available, including MD5, SHA1, SHA256, and SHA512. These algorithms differ in their security, speed, and output size.

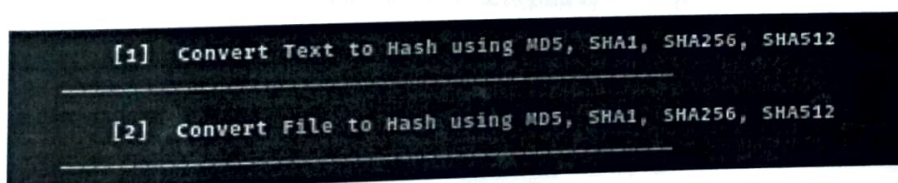


Fig.5.1.3 Text File to hash

Hashcat is a popular password-cracking tool that is used to recover lost or forgotten passwords. It is a free and open-source software that supports various hash types and password cracking methods. Hashcat is designed to run on multiple platforms, including Windows, Linux, and macOS.

Hash identifier is a tool that is used to identify the type of hash value that is generated from a given plaintext or password. Hash values are often used for password storage and authentication purposes. However, since different applications and systems use different hash functions, it is important to identify the hash type to select the correct cracking method.

John the Ripper (JTR) is a popular password-cracking tool that is used to recover lost or forgotten passwords. It is free and open-source software that supports various hash types and password-cracking methods. JTR is designed to run on multiple platforms, including Windows, Linux, and macOS. JTR supports various password-cracking techniques, including brute-force attacks, dictionary attacks, and hybrid attacks.

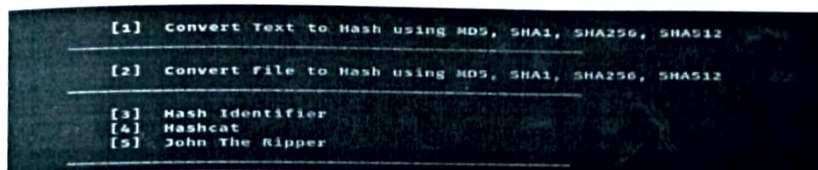


Fig.5.1.4 List hashing tools

A metadata collector is a tool or software that is used to gather metadata information from digital files. Metadata is the data that describes other data and provides information about a file's content, such as author, date created, file type, and location. Metadata collectors are commonly used by digital forensics investigators, law enforcement agencies, and intelligence agencies to gather information about digital files and their owners. This information can be used to investigate crimes, track down individuals, and gather intelligence.

In this, my tool tells the file size, file name, file type, file type extension, directory, JFIF Version, MIME Type, etc. in an Image. Line count, no of words, file size, file name, file type extension, modification date and time, file access date and time, etc. in a File.

```

> Enter The Option from [1-10] OR [EXIT] to Exit $ #
> Enter file (Any Format) : sample2.mp4
ExifTool Version Number : 12.54
File Name : sample2.mp4
Directory :
File Size : 1056 kB
File Modification Date/Time : 2023:01:31 14:01:59-05:00
File Access Date/Time : 2023:01:31 14:02:53-05:00
File Inode Change Date/Time : 2023:01:31 14:02:53-05:00
File Permissions : -rw-r--r--
File Type : MP4
File Type Extension : mp4
MIME Type : video/mp4
Major Brand : MP4 Base Media v1 [ISO 14496-12:2003]
Minor Version : 0.2.0
Compatible Brands : isom, iso2, avc1, mp41
Media Data Size : 0
Media Data Offset : 1051515
Movie Header Version : 0
Create Date : 0000:00:00 00:00:00
Modify Date : 2014:07:19 17:15:29
Time Scale : 1000
Duration : 5.31 s
Preferred Rate : 1
Preferred Volume : 100.00%
Preview Duration : 0 s
Poster Time : 0 s
Selection Time : 0 s
Selection Duration : 0 s
Current Time : 0 s
Next Track ID : 3
Track Header Version : 0
Track Create Date : 0000:00:00 00:00:00
Track Modify Date : 0000:00:00 00:00:00
Track ID : 1
Track Duration : 5.28 s
Track Layer : 0
Track Volume : 0.00%
Image Width : 1280
Image Height : 720
Graphics Mode : srcCopy
Op Color : 0 0 0
Compressor ID : avc1
Source Image Width : 1280
Source Image Height : 720
X Resolution : 72
Y Resolution : 72
Bit Depth : 24
Video Frame Rate : 25
Matrix Structure : 1 0 0 0 1 0 0 0 1
Media Header Version : 0
Media Create Date : 0000:00:00 00:00:00
Media Modify Date : 0000:00:00 00:00:00
Media Time Scale : 48000
Media Duration : 5.31 s
Media Language Code : und
Handler Description : SoundHandler
Balance : 0
Audio Format : mp4a
Audio Channels : 2
Audio Bits Per Sample : 16
Audio Sample Rate : 48000
Handler Type : Metadata
Handler Vendor ID : Apple
Encoder : Lavf53.24.2
Image Size : 1280x720
Megapixels : 0.922
Avg Bitrate : 1.58 Mbps
Rotation : 0
0

```

Fig.5.1.5 Final Output

CHAPTER 6

RESULTS AND DISCUSSION

Thus, my project Kryptocrack-a steganographic tool concludes that is a useful tool. That can embed and extract hidden messages from images and also covert the given text into Hash values, it also collects the data from the file, image, and video. This should produce high accuracy, as well as beneficial data is essential for testing. Also, it provides security for the web-based application as well as shows all of the application's detailed information. Following that, the Open-source structure would also obtain data on a specific person or organization. Even when using Cryptography, which is an effective mechanism for safeguarding data stored on a computer, which will start examining a hash variety and authenticate the hash credentials.

CHAPTER 7

CONCLUSION

7.1 CONCLUSION

Everything is going online on the internet as a result of the ongoing digital revolution, and as we all know, the web is not an extremely secure protocol. As a result, precautions must be taken to protect the authenticity as well as the secrecy of the info. To expand reports of information security, cyber threats, as well as information leakage, researchers should ensure the security of our vital information. A vulnerability assessment is a complete and accurate method for detecting security vulnerabilities.

7.2 FUTURE WORK

Steganography is the art and science of concealing information within digital media such as images, audio, video, and text, without arousing suspicion. As technology continues to advance, the future scope of steganography is likely to expand in several ways:

- a) **Advanced Encryption:** Steganography will continue to evolve as a means of secure communication, and advanced encryption techniques will play a critical role in this. New encryption methods, such as quantum encryption, may also become popular for use in steganography.
- b) **Artificial Intelligence:** The use of artificial intelligence (AI) in steganography will likely grow, allowing for more advanced techniques for hiding information in data. AI can be used to analyze and understand the patterns in digital media, making it possible to create more effective hiding techniques.
- c) **Deep Learning:** Deep learning algorithms can be trained to learn how to detect and extract hidden messages, making it more difficult for stenographers to hide information. Therefore, future steganography techniques must take into account the threat posed by deep learning algorithms.

- d) **Applications in Cyber security:** Steganography is also expected to find new applications in cyber security, such as hiding malware within images, videos, and other digital media, making it difficult for antivirus software to detect.
- e) **Advancements in Imaging Techniques:** Advancements in imaging techniques, such as high dynamic range (HDR) and 3D imaging, will offer new opportunities for steganography. With more complex images, there will be more room to hide information and new methods of encoding and decoding the information will be required.

Overall, steganography is likely to continue to play an essential role in secure communication and information hiding. As technology advances, so will the techniques used in steganography, making it even more challenging to detect and prevent hidden information.

REFERENCES

- [1] S. Kamil, M. Ayob, S. N. H. S. Abdullah, and Z. Ahmad, "Challenges in multi-layer data security for video steganography revisited," *Asia-Pacific J. Inf. Technol. Multimedia*, vol. 7,
- [2] T. D. Denemark, M. Boroumand, and J. Fridrich, "Steganalysis features for content-adaptive JPEG steganography," *IEEE Trans. Inf. Forensics Security*, vol. 11, no. 8, Aug. 2016,
- [3] Y. Wu, Y. Xiang, Y. Guo, J. Tang, and Z. Yin, "An improved reversible data hiding in encrypted images using parametric binary tree labeling," *IEEE Trans. Multimedia*, vol. 22,
- [4] S. A. El_Rahman, "A comparative analysis of image steganography based on DCT algorithm and steganography tool to hide nuclear reactors confidential information," *Comput. Electr. Eng.*, vol. 70, pp. 380–399
- [5] S. Solak, "High embedding capacity data hiding technique based on EMSD and LSB substitutional algorithms," *IEEE Access*, vol. 8,
- [6] S. Rahman, F. Masood, W. Ullah Khan, N. Ullah, F. Qudus Khan, G. Tsaramirsis, S. Jan, and M. Ashraf, "A novel approach of image steganography for secure communication based on LSB substitution technique," *Comput. Mater. Continua*, vol. 64,
- [7] R. Wazirali, W. Alasmay, M. M. E. A. Mahmoud, and A. Alhindi, "An optimized steganography hiding capacity and imperceptibly using genetic algorithms," *IEEE Access*, vol. 7,

