StealthPassage: Encrypted Text Concealed with Hashing

G Rajamuneeswaran [1]
Assistant Professor
Jai Shriram Engineering College
rajamuneeswarang@jayshriram.edu.in

B Sasireka[2]
UG student
Jai Shriram Engineering College
sasirekacomeng63@gmail.com

M.Swathi[3]
UG Student
Jai Shriram Engineering College
cseswathim@gmail.com

V.Vashmitha[4]
UG Student
Jai Shriram Engineering College
vashmithatirupur@gmail.com

Abstract

An innovative method of protecting confidential data is to hide it using encryption and decryption. In order to make the secret message disappear to the unaided eye, this encryption method embeds it into the visible text. When it comes to protecting data from unwanted access, the emergence of digital communication has made novel approaches necessary. One such approach is concealed text encryption. In order to better understand of concealed text encryption, this study examines the fundamental algorithms and approaches as well as their principles and methodologies. This text encryption makes certain that the encrypted communication is not revealed to uninvited parties by utilizing cryptography, the art of hiding information within other data. The content of the encrypted file will disappear, which means no one can predict the information hiding behind the whitespace background, and it is very complex to decrypt the encrypted file. This method provides stronger security for our information than other methods of cryptography.

Keyword: Encryption, Decryption, Hashing Algorithm

Introduction

In this technology evolution, we all need to secure the confidential data. An organization or a person wants to store a secret information. They will then choose "Cryptography." Cryptography focuses on techniques include Encryption and Decryption. These techniques are employed to safeguard communications and digital assets as well as to secure talks. We can encrypt the text file into another type of encrypted text file (Cipher text), hiding text into images or videos or audios etc., Protecting in formations from the attackers is the crucial one and at the same time it is complex one. By using some technology and algorithm we can protect our information from the criminal attacks. In this paper a different methodology is used to encrypt the text file. It is very useful to the organization or a single person to secure their data and information. For example, our military conversations are very confidential, so there is a need for encryption and decryption. By using this concealed text encryption and decryption, we can have a secure conversation. Even the encrypted text will not be visible to anyone. Just as other confidential communications need this strategy for secure transactions.

If the text or image something is visible to others then it’s a possible to understand the idea of encryption. Unless if it is not clear or no visible to all then there is a less chance of predicting whether it is a encrypted file or not. No one can’t decrypt the file without the encrypted method knowledge. It is more advanced method to hide the original data. Even no one cannot see anything in the encrypted file. After the encryption we can decrypt the file to the original text file. We can set the password for the encryption and decryption for the authentication purpose. In this paper hashing technology is used for the encryption and decryption techniques. Specifically, SHA-256 is used.

Modern Vs Traditional Cryptography

Modern cryptography is a major breakthrough over traditional cryptography, which provided weaker security, less inefficient techniques, and better key management systems to meet the demands of the digital age. Traditional cryptography lay the foundation for cryptographic techniques.

Traditional cryptography

Prior to the development of computers and digital technologies, conventional cryptographic refers to cryptographic techniques created and applied. From ancient civilizations, these techniques have been used for ages. Manual or mechanical procedures are at the heart of traditional cryptography systems. The rail fence cipher, substitution ciphers (like the Caesar cipher), and polyalphabetic ciphers (similar to the Viennese cipher) are a few examples of these. The algorithm or key's secret was frequently depended upon by these methods.

Secrecy was the means by which confidentiality was achieved in traditional cryptographic systems. Usually, cracking these systems needed advanced cryptanalysis abilities or familiarity with the particular method employed. But because of their simplicity, a lot of traditional systems are open to cryptographic or brute-force assaults. Problems with key management, particularly with safely sharing and keeping keys, were a common occurrence in traditional cryptography.

Modern Cryptography

The development of computing devices and digital technologies led to the creation of modern cryptography. For key management, encryption, and decryption, it mostly depends on sophisticated mathematical techniques and processing capacity. Asymmetric cryptography, or public key cryptography, is one of the main characteristics of contemporary encryption. For encryption and decryption, it makes use of sets of public and private keys. Many of the key distribution issues in conventional cryptography are addressed by this method Advanced encryption standards like AES (Advanced Encryption Standard), public key cryptography techniques like RSA and ECC (Elliptic Curve Cryptography), and hashing techniques like SHA (Secure Hash Algorithm) are used in modern cryptography.With the use of digital certificates, key exchange protocols, and cryptographic key derivation algorithms, modern cryptography provides more reliable key management procedures.

Methodology

A. Hashing Algorithm

1. Hashing

In cryptography, a mathematical function is called a cryptographic hash function. Hash functions are commonly designed to accept variable-length inputs and produce fixed-length outputs. Hash functions that may pass messages while maintaining security are combined in a cryptographic hash function. Algebraically, hash functions "map" or "transform" a given data set into a fixed-length bit string that is called the "hash value." A variety of complexity and difficulty levels are included in hash functions, which are employed in cryptography. Password security, communication security, and cryptocurrency all use hash functions. Cryptographic hash functions add safety measures to common hash functions, making it more challenging to decode message contents or recipient and sender identity.

FORMULA:

$$h(k)=k \bmod m$$

- k is a single integer key.
- h(k) is a small integer bucket value.
- m is the size of hash table.

2. Hash table and hash function

A hash table is a data structure that maps keys to array indexes using a hash function, making key-value pair storing and retrieval efficient. The hash function uses a key as input to generate a hash code, which is subsequently used to find the index in the array where the relevant item will be kept.

A hash function's fundamental concept is to translate a given key into a numerical value that indicates the key's location in the array. To reduce collisions caused by multiple keys mapping to the same index, this numerical value should ideally be distinct for every key. Collisions are unavoidable, nevertheless, because of the array's limited size in relation to the possibly infinite number of keys.

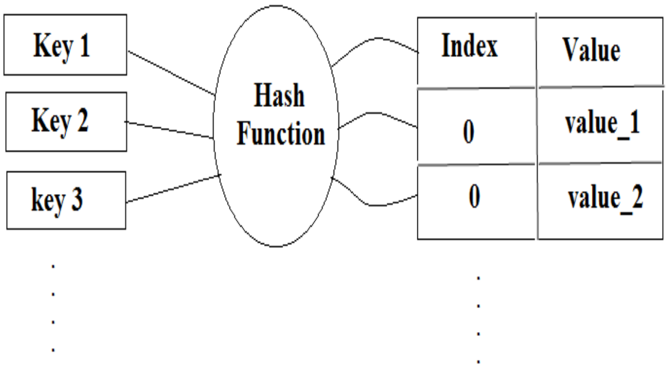

Figure 1:Hash table and hash function

B. SHA-2

A collection of cryptographic hash functions developed by the US National Institute of Standards and Technology (NIST) is referred to as "Secure Hash Algorithm," or SHA for short. SHA-0, SHA-1, SHA-2, and SHA-3 are the versions of the SHA family. Each one produces a fixed-size hash value (digest) based on the input data. These hash algorithms are mostly used to generate a hash, or unique identifier, for a piece of data, such as a message, file, or password. Data integrity checks, password storage, and digital signatures all commonly use this identity.

C. Encryption

A cryptographic hash function called Secure Hash Algorithm 256-bit, or SHA-256, produces hashes with a length of 256 bits, or 32 bytes. It is important to understand the difference between an encryption scheme and SHA-256 as a hashing technique. A fixed-size output, or digest, is produced from arbitrary-sized input data using hashing algorithms like SHA-256. Hashing differs from encryption in that it is not meant to be a one-way process.

- **Message Padding:** In accordance with the SHA-256 method, the input message must be padded to guarantee that its length is equivalent to 448 mod 512. By padding, you may make certain the input message is more than the block size.
- **Appending Length:** The padded message has an attached binary representation of the original message's length. By doing this, you can make sure that the hash function considers the message's whole length.
- **Initialization:** The hashing algorithm of SHA-256 loads a specified set of initial hash values, referred to as the "state," into it prior to processing the message.
- **Processing Blocks:** There are 512-bit blocks created from the padded message. The compression function performs a number of actions on each block in order to update the hash value.
- **Compression Function:** The message block and the current hash value are processed by the compression function within each block to generate a new hash value. Multiple rounds of operations, such as bitwise operations, modular addition, and logical functions, are involved in this process.
- **Final Hash Value:** The hash value that is obtained after processing every block is the input message's cryptographic hash**.**

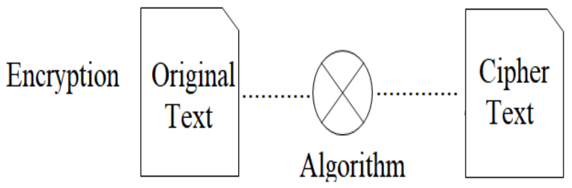

Figure 2 : Encryption Technique

D. Decryption

Since SHA-256 is a one-way cryptographic hash function, decryption and reverse engineering are not possible with it. It is not possible to recover the original input from the hash value once it has been hashed using SHA-256. The most popular method involves utilizing a dictionary or brute-force attack, in which many inputs are hashed using SHA-256 and their hash values are compared to the target hash value. Until a matched hash is identified, this procedure keeps going.

- **Getting the Ciphertext:** Securing communication channels or storing the encrypted data allow for the acquisition of the ciphertext.
- **Choosing or Getting the Decryption Key:** In symmetric-key cryptography, the recipient chooses the decryption key, whereas in asymmetric-key cryptography, the key is supplied with the ciphertext. This depends on the encryption algorithm involved.
- **Using the Decryption Key to Apply the Algorithm:** The recipient decrypts the ciphertext by applying the algorithm over it. Reversing the effects of the encryption algorithm employed during encryption is the specific purpose of this algorithm.
- **Generate Potential Inputs:** Begin by coming up with potential inputs, such phrases or passwords, then use the SHA-256 method to hash each input.
- **Comparing hashes:** it is the third step in decoding; compare the hash values of the inputs that were created with the desired hash value.
- **Repeat:** Until you discover a match or run out of search space, keep creating and hashing inputs.
- **Optimization:** Employ strategies for speeding up the process and raising the likelihood of finding a match, such as employing rainbow tables or dictionaries of frequently used passwords.

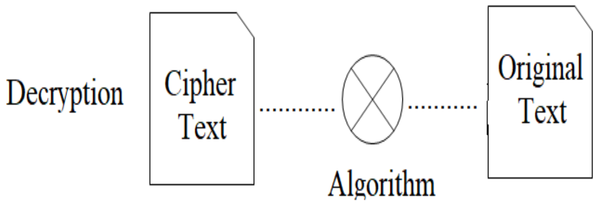

Figure 3: Decryption Technique

Table

Explanation of keys used in encryption and decryption process.

Keys	Description
Space key	These Keys are use to encrypt the entire file. For each word it will be replaced in the encryption process and reverse process for decryption
Tab key	
Enter key	

E. Authentication

One essential security measure is login password authentication, which is used to confirm a user's identity when they try to access a system, service, or application. A password is a combination of characters used as a secret credential for system, service, or application access. System lockout mechanisms are frequently used to stop brute-force attacks. The user's account may be momentarily disabled or locked to prevent unwanted access after a predetermined number of unsuccessful login attempts. Systems may implement password rules to guarantee that passwords satisfy specific complexity standards, like a minimum length, the use of special characters, numerals, and a mix of capital and lowercase letters.

In this paper, we create a system for an organization or a single person's private safe. The password is only known to the one person who is going to monitor the system. They can maintain the same password for both encryption and decryption, or they can use different passwords for both encryption and decryption operations to secure the information.

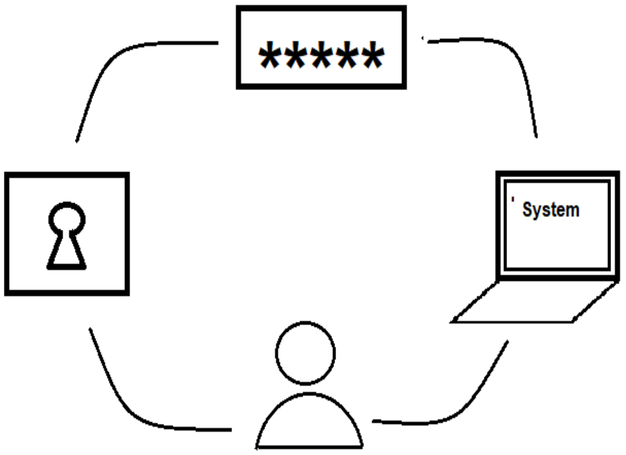

Figure 4: Authentication for security

F. Additional Features

While the fundamental idea behind invisible text cryptography is consistent across several implementations, certain approaches may provide more features or methods than others. The following are some other characteristics that certain methods of invisible text cryptography may include:

1. **Robustness:** Using strategies that make the hidden message resistant to different kinds of manipulations or attacks is one goal. To do this, the message may need to be embedded such that it is unaffected by stretching, cropping or other changes made to the carrier media.
2. **Security:** Some strategies may place a higher priority on security by using steganography coupled with robust encryption algorithms. This makes sure that even in the unlikely event that the concealed message is found, it will stay hidden and unavailable without the right decryption key.
3. **Multi-layered Encryption:** In more sophisticated implementations, the secret message could be encrypted several times using various keys or methods, enhancing communication security.
4. **Authentication and Integrity Checking:** Verifying the validity and integrity of the secret message is one way to be sure that it hasn't been altered while dissemination or storage. This is known as authenticity and integrity checking.

Result

We can encrypt our private information with this method in just a minute. Nobody is able to figure out how we encoded and decoded the encrypted data.Whitespace Steganography involves hiding information within the spaces, tabs, and line breaks of a text document. By strategically placing these characters, a hidden message can be encoded. Other than an image, cipher text, audio, or video, we can get an invisible file full of white spaces. It is very difficult to understand the concept hiding behind this space. And it’s very hard to find the number of words embedded within the text file.

The final result will satisfy the user and give security to the user’s information. The number of spaces allocated to each and every character depends on the administrator, and no one can find the value, so it is more difficult to decrypt the encrypted file. Only by using the number of space values can we decrypt the file. But the number of spaces is allocated during the coding process. This is a more secure and trustworthy system for our confidential and private files. An organization will get good performance and security by using this system.

Future Enhancement

Only one system or device within the organization has the ability to both encrypt and decode data. Allow the sharing of encoded files between two or more people or organizations. Furthermore, the size of the encoded document's file depends on the key, which varies depending on each character in the private document. Thus, in the next upgrade, the key size should be utilized efficiently.

By encrypting the text in the document, the length may increase. We use any number of spaces for every word. So the length may increase more than the original document’s length. In further development, we will work to reduce the size of the file after encrypting. In this tab, as well as the number of times the enter key is used, it will append the length of the document. After decrypting the document, the original contents are replaced, and the original length is restored.

Conclusion

Finally, a technique called or This Stealth Passage, provides a variety of methods for hiding information in what appears to be innocent data. Secure communication, digital watermarking, and covert data transmission are just a few uses for this encryption and decryption technique.Even though some methods have their uses, there is a chance that they are going to be abused or utilized for illegal actions like surreptitious communication. As such, it is imperative that the application of this text cryptography be handled sensibly and ethically, following the law and accepted moral principles.

Additionally, the stability of the algorithm, the intricacy of the encoding technique, and the capacity to recognize and understand concealed messages are some of the variables that describes how successful this whitespace encryption and decryption is. The possibilities of steganography techniques and approaches for identifying them are always evolving as technology progresses.

Overall, research on Stealth Passage: Encrypted text Concealed with hashing is still very interesting and has applications in many other domains, including as digital forensics, cyber security, and information hiding. To fully realize its potential advantages and handle any security risks, this subject requires ongoing study and development.

REFERENCES

[1]. Al-Khedhairi et al., 2018. "Hybrid cryptosystem based on pseudo chaos of novel fractional order map and elliptic curves," Volume 8, pages 57733–57748, IEEE Access, 2020.

[2]. B. Ge, X. Chen, G. Chen, and Z. Shen, "Secure and fast image encryption algorithm using vector operation and Hyper-Chaos-Based key generator," IEEE Access, vol. 9, pp. 137635–137654, 2021

[3]. Z. Hua, Y. Zhou, C.-M. Pun, and C. L. P. Chen, "Image encryption using 2D logistic-sine chaotic map," in IEEE Int. Conf. Syst., Man, Cybern. (SMC), Oct. 2014, pp. 3229–3234.

[4]. Ben Ge, X. Chen, G. Chen, and Z. Shen, "A secure and quick image encryption algorithm utilizing vector operation and a hyper-chaos-based key generator," IEEE Access, vol. 9, pp. 137635–137654, 2021.

[5]. A review of text watermarking: theory, methods, and applications was published in IEEE Access in 2016 by NURUL SHAMIMI KAMARUDDIN, AMIRRUDIN KAMSIN, LIP YEE POR, and HAMEEDUR RAHMAN.

[6]. M. G. Kuhn, R. J. Anderson, and F. A. P. Petitcolas, "Information hiding-A survey," Proc IEEE, vol. 87, no. 7, 1999, pp. 1062–1078).

[7]. Kim, M.-Y. "Text watermarking by syntactic analysis," in Proc. 12th WSEAS Int. Conf. Comput., 2008, p. 904.

[8]. G. Sharma and D. Coumou, "Watermark synchronization: Perspectives and a new paradigm," in Proc. 40th Annu. Conf. Inf. Sci. Syst., 2006, pp. 1182–1187.

[9]. Razam, Qazaim, Ahmed, Alturki, and Anwar, "Systematic and Critical Review of RSA Based Public Key Cryptographic Schemes:Past and Present Status," IEEE Access, Identifier 10.1109/ACCESS.2021.3129224, 2021.

[10]. T. Eisenbarth, S. Kumar, C. Paar, A. Poschmann, and L. Uhsadel, "A survey of lightweight-cryptography implementations" IEEE Desktop.