Received: 30 December, 2022, Accepted: 07 February, 2023, Online: 22 February, 2023

DOI: https://doi.org/10.55708/js0202002

# Applied Salt Technique to Secure Steganographic Algorithm

**Bo Bo Oo***

Edinburgh Napier University, School of Computing, Edinburgh, EH10 5DT, UK

*Corresponding author: Bo Bo Oo, +44 77 7863 0269, bobooo.1249@gmail.com

**ABSTRACT:** Digital multimedia assets, including photographs, movies, and audio files, have become a staple of contemporary life. Steganography is a method for undetectable information concealment in these files. One can communicate messages to another by modifying multimedia signals so that a human would be unable to tell the difference between the original signal and the altered one. The widespread use of digital data in practical applications has prompted the development of new and efficient methods for ensuring its security. Steganographic techniques can be used to, at least in part, achieve efficient secrecy. There have been suggested new and adaptable audio steganographic techniques. By using cryptography, readable language is converted to unintelligible data. In order to send and receive text, multimedia, or other important digital files safely, this paper discusses secure communication media. To have secure communication tools, the tools must lessen potential risks and weaknesses. Therefore, the primary factor to take into account for creating a solid communication system is transferred media. The objective of steganographic systems is to find a secure and reliable method to hide a significant amount of secret data. This research focuses on digital image audio steganography, which has become a popular method for data concealment.

**KEYWORDS:** Steganography & Cryptography, Secure communication media, Salt Encryption, AES, Steganography with SHA-256

## 1. Introduction

In order to share information across many geographies through digital communication, a number of new technologies are constantly developing. Information can sometimes include user privacy, confidential data, and other sensitive material that needs to be segregated. Secure communication media should be used to communicate this information. Even if a crucial piece of information is given to a person who is acting strangely, unforeseen events that could result in dangerous situations could still happen. Therefore, this information is shielded from corruption or breach by a malevolent hacker using the data concealing approach. The majority of data concealment techniques use steganography, cryptography, and digital watermarking.

The message should first be encrypted using a secure cryptographic procedure before being encoded using the steganography algorithm. In that case, not even steganographic algorithms can simply decode the message. The message will be converted into ciphertext, rendering it unintelligible to attackers. The algorithms used in cryptography methods are numerous. In essence, key management infrastructure is used. To improve the encryption algorithm, symmetric and asymmetric cryptographic key management approaches are used. To confirm that the sender and receiver are the authorised users, the symmetric key is originally provided with both parties. Steganography doesn't really make message authentication better. To protect messages for visual detection from sender and receiver, numerous encryption techniques are used.

The mechanism through which steganography and cryptography will interact to create secure media is being developed in this secure communication medium. Additionally, steganalysis will be used to find stego-objects in developed material using a variety of analysis tools and evaluation results from various hashing techniques. Python programming will be used to carry out the implementation. This study will outline an improvement strategy for using secure media to transmit private information.

## 2. Related work

### 2.1. Steganography

Frequency domain and spatial domain are the two main domains that can be utilised to identify data embedding in image processing that uses pixels, according to an analysis of steganography techniques. The measurement of image quality and quantity distinguishes the two domains most proposed in [1]. Quantity is determined by using image sensitivity. Based on the results of the peak signal to noise ratio (PSNR) or the structural similarity index metric, the quality measure is examined (SSIM). Based on the results of bits per pixel, the quantity measurement is examined. In addition to these two, imperceptibility and robustness are important considerations. Robustness is the ability to clearly degraded modified image from partial attacks to lose data integrity. The human eye can detect significant changes that point to the existence of embedded data. The study of this perceptible is referred to as imperceptibility. Using bit numbers, the spatial domain integrated the simple text into the cover image.

In LSB methods, bit numbers of the message are substituted for the image's least significant bits. There will be 3 bytes for red, green, blue, and alpha when decomposing the pixel (RGBA). There are 8 bits in each byte, and one byte is used to represent each colour. The least significant bit (LSB) for each byte is the one on the right, while the most significant bit (MSB) is the one on the left (MSB). An image with an RGB value of 800x600 pixels can hold up to 180,000 bytes for embedding explained in [1].

#### 2.1.1. Image Steganography

The use of a picture as a cover to conceal a message is known as image steganography. The image can be used with a variety of image formats, including Portable Network Graphics (PNG), Bitmap (BMP), and Joint Photographic Experts Group (JPEG) (PNG). The JPEG image format compression is a popular format for lowering the size of the image described in [2]. Using an image as compression enables you to maintain aesthetic characteristics that are still evident. Since the human naked eye cannot breakdown the veiled information contained within the cover image, this information is difficult for humans to see.

#### 2.1.2. Audio Steganography

A steganographic method called Audio Steganography involves encoding data using an audio-based file structure. Waveform Audio (WAV), Audio (AU), and MPEG Audio Layer III are all acceptable audio file formats (MP3). It is extremely difficult to embed the message in audio, however many different methods have been tried. An enhanced least significant bit modification technique for audio steganography shows large amounts of data can be compressed using audio, and it is difficult to hack in [3]. However, maintaining an audio signal becomes more challenging as more data are encoded. It primarily serves to safeguard digital copyright.

### 2.2. Cryptography

Encryption and decryption are the two main operations involved in cryptography. private information is transformed into bizarre, cryptic text with a variety of odd marks in order to prevent unauthorised access. It's called encryption. The output of encryption is referred to as ciphertext, which is difficult to decipher visually. Decryption is the process of converting this ciphertext back to plaintext (the original text). It is not possible to restore the ciphertext to plaintext using some cryptographic methods. The cryptography technique is carried out in these two operations using the key exchange infrastructure. The plaintext is converted to a cypher using a pseudorandom key or user-defined key, which is then utilised again during the decryption process. These three techniques are hash functions, symmetric cryptography (public-key cryptography), and asymmetric cryptography (secret-key cryptography). These three techniques are frequently used to send messages more securely in [4].

#### 2.2.1. Asymmetric cryptography

Asymmetric cryptography, also known as public-key cryptography, uses two different kinds of keys: public and private. Public key infrastructure, digital signature, channel security, and tamper detection are the main applications for public key. A digital signature is used to confirm the message's validity and provide proof that it originated with the sender. Additionally, it has the capacity to confirm the non-repudiation and data integrity. The signature enables the sender to notify the recipient if the encrypted communication is changed or expanded upon described in [5]. Plaintext, ciphertext, an encryption method, a decryption algorithm, a private key, and a public key are the different parts of a public key infrastructure.

#### 2.2.2. Symmetric cryptography

Symmetric cryptography, also referred to as secret-key cryptography, encrypts and decrypts data transformations using a single common key that is passed into a mathematical formula. Secret-key cryptography is used specifically to improve the privacy and confidentiality of data.

AES is a symmetric encryption method since it employs the same key for both both encryption and decryption. Additionally, it employs numerous rounds of the SPN (substitution permutation network) method to encrypt data. The impenetrability of AES is a result of

these encryption rounds, which are impossible to break through due to their sheer number in [6]. The United States National Institute of Standards and Technology (NIST) developed the Advanced Encryption Standard (AES) as a specification for the encryption of electronic data in 2001. Despite being more difficult to build, AES is still commonly used because it is substantially stronger than DES and triple DES. Three key lengths—128 bits, 192 bits, and 256 bits—are used in the AES encryption and decryption process. For, a fixed block length of 128 bits is used. For 128-bits, 192-bits, and 256-bits, AES uses 10, 12, and 14 rounds, respectively.

#### 2.2.3. *Hash Function*

One of the cryptographic methods that enables the complete transformation of the plaintext to the given varied fixed number is the hash functions. Digesting is the term for this transformation process. The hash functions do not need keys. Fundamentally, hash functions are used in digital signatures, password security enhancement, random number creation, and message authentication. The one way is another name for it explained in [4]. For instance, the message "Hello" is encrypted using the MD5 cryptographic hash function technique. "Hello" will result in a digest message of 128 bits rather than 16 bytes. The result will be 128 bits when another plaintext "World" message is similarly encrypted in that manner (16bytes).

Table 1: MD5 Hash Table

| Plaintext | Hash value (MD5) | Output size |
|---|---|---|
| Hello | 8b1a9953c4611296a827abf8c47804d7 | 128 bits (16bytes) |
| World | f5a7924e621e84c9280a9a27e1bcb7f6 | 128 bits (16bytes) |
| Hello World | b10a8db164e0754105b7a99be72e3fe5 | 128 bits (16bytes) |

There are hundreds of different hashing algorithms available, and each one is tailored for a certain sort of data, speed, security, etc. Secure Hashing Algorithm, or SHA. There are two variants of the algorithm: SHA-1 and SHA-2. They differ in the bit-length of the signature as well as in creation (how the resultant hash is made from the original data). The National Institute of Standard of Technology released SHA (NIST). The hash value produced by FIPS 180-4 SHA can be MD. It generates a higher hash value than MD, is faster, and is more secure than MD. The output of SHA is a hash value of 160 bits (20 bytes) with 20 rounds.

As a hashing algorithm response to developing BCrypt assaults, SCrypt was developed. SCrypt is used in many software programmes to implement the protection against password cracking. For the purpose of generating the peak time for password processing, SCrypt uses a specific amount of their hardware resources in their farm. However, employing a specific amount of memory allows you to restrict an attacker's capacity to find passwords using high-tech gear. SCrypt is used to strengthen the encryption algorithm based on the findings.

### 2.3. *StegAnalysis*

The method known as steganalysis aims to counter steganography by locating the concealed data and extracting or erasing it. For law enforcement organisations, it becomes essential to decipher the communication or at the very least render it useless to the recipient, as is the case with nearly all such approaches. Through steganalysis, the primary attribute of a stego-object is analysed based on its robustness, capability, and imperceptibility. The steganalysis is carried out in the steganography studio to look at the detection of images that show the presence or absence of steganographic information using various algorithms and various image format types in [7]. In order to identify the cover image, steganalysis is performed using server tools like Openpuff and Steganography Studio. Visual analysis (examining with human visual abilities to perceive the existence of information) and statistical analysis (examining of modification in statistical properties to the images). To improve security assessments, steganalysis can be researched on cutting-edge technologies like artificial intelligence, neural networks, fuzzy logic, and genetic logic by extracting data more thoroughly through statistical qualities as a progressive digital forensic.

## 3. Proposed System

In steganography, there are three main cover file formats that are utilised. They are steganography for audio, steganography for video, and steganography for images. Data steganography in audio and video is a very dedicated approach because even little changes can cause significant noise affects. This had a negative impact on the original quality and greatly affected the capacity of the human visual system (HAS) and human auditory systems (HVS). HAS is more sensitive than HVS when compared to each other. In order to see the variations in noise in an image file, you must look at it in great detail for a few seconds. The development of communication medium is more adaptable and trustworthy when using image and audio steganography. The effectiveness of audio steganographic techniques is influenced by a number of factors. Each feature's significance and effect vary depending on the application and the transmission environment. The durability to noise, compression, and signal manipulation, as well as security and the ability to hide concealed data, are among the most crucial characteristics shown in [8]. The robustness criteria is the

most difficult to meet in a steganographic system when paired with data hiding-capacity because it is closely related to the application.

The most practical approach based on the spatial domain is called least significant bit (LSB). The image is broken up into a large number of pixels as part of the spatial domain process. A pixel has 24 bits in total. Red, blue, and green are represented by each 8-bit colour. The least significant bit of these three values is used in the LSB algorithm's processing. The first step of the method is to read the image and transform it into image pixels. The message is then transformed into a bit as well. The LSB of the picture is used to replace the message bits to create the stego-image. The image is not lost when the LSB is changed, and great perceptual transparency is supported. As a result, these changes are not easily visible to humans. In order to hide data, several image steganography programs alter bits using the least significant bit (LSB) technique. In low resolution pictures with 8-bit colour, changing the LSB could cause a noticeable shift in the colour palette, making it simple to spot hidden material. Another sign that there is hidden information present in an image is padding or cropping. The Hide-and-Seek tool can only be used to create fixed-size graphics.

## 4. Methodology

By using data hiding techniques on the communication carrier, the process can be divided into two primary parts: encryption and decryption. There will be two actors while employing a communication carrier: a sender and a receiver. Before sending the carrier, the sender must complete the encryption process. The system needs three user inputs for the encryption method: a cover image, a message, and a secret key. Stego-object as well as a shared secret key are needed for decryption. the symmetric communication mechanism that uses encryption. The sender must enter the secret and message into the system in order for symmetric communication to flow.

Utilizing the LSB approach, steganography and cryptography are combined in this system. The entered file is chosen as an audio file in this system. After that, the communication is encrypted using just one secret key. The Image Steganography and cryptography are also combined as different mechanism for encryption and decryption. Both systems are suggested and employ the LSB algorithm to conceal the message in communication media. Utilizing various essential communication networks has its benefits. Depending on the user's decision during encryption, the stego-object can be either an image or an audio file.

The AES algorithm first converts the secret key into a hash digest value. The salt will be generated prior to hashing the AES in order to combine the secret key. This procedure is only used in one-way operation. The hash value cannot be converted back to its original form and cannot be used to determine the secret key's value.

The hash value and encrypted message are base64

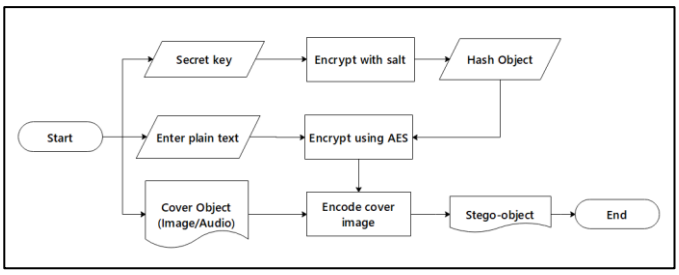


Figure 1 Encryption Algorithm

encoded into unintelligible ciphertext. The cover object is additionally mixed with the ciphertext using the LSB steganography algorithm. The ciphertext of the encrypted communication is converted to binary format. First, an RGBA format conversion is performed on the cover image. These binary-formatted data are also converted to hexadecimal form. By using a delimiter, the modified binary value of the message is inserted into the hexadecimal format value of the cover image. The system will return the cover image as the stego-image to deliver the message over communication media to the recipient once all of the transform values have been fully included into the cover image.

On the other side, High data embedding capacities are

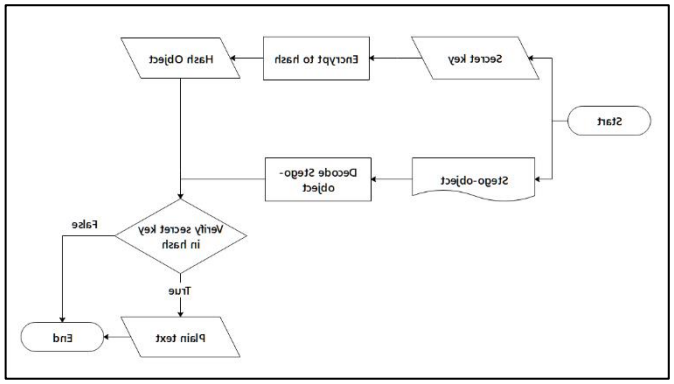

Figure 2: Decryption Algorithm

possible with the LSB method, which is also reasonably simple to use alone or in combination with other hiding methods. This method's limited resistance to noise addition, which makes it susceptible to even straightforward attacks, lowers its security performance. The data will probably be lost if the stego-audio is filtered, amplified, has noise added to it, or is compressed using lossy techniques. Without impacting the perceived transparency of the stego audio signal, it has extended the depth of the embedding layer from the fourth to the sixth and eighth LSB layers to improve the robustness of the LSB approach against distortion and noise addition. The other bits can be switched to create a new sample that is more similar to the original in order to reduce embedding error.

The communication carrier (stego-object) is extracted on the recipient side using a shared key. The stego-object is initially broken down into an acceptable format by identifying a delimiter to recreate the binary data. By converting to binary, these hexadecimal values are retrieved back into plaintext. The system begins ciphertext decryption once the ciphertext has been successfully obtained. There is a password verification function that must be passed through in order to acquire the original message prior to the decryption of the ciphertext. The system extracts the salt from the ciphertext before encrypting the newly entered password from the receiver and converting it to a hash value. The system then compares the newly created hash value to the other hash value that was derived from the stego-object. The generated hash must be verified in order to ensure that the password is valid. The system unpads the result and sends the message to the recipient after the ciphertext has been decrypted.

The suggested steganography system's encryption and decryption procedures are shown in the diagram below. The encryption procedure for both audio and image steganography requires the cover file, password, and secret message in order to produce a new stego-image. The application simply needs a password and stego-object to decrypt data.

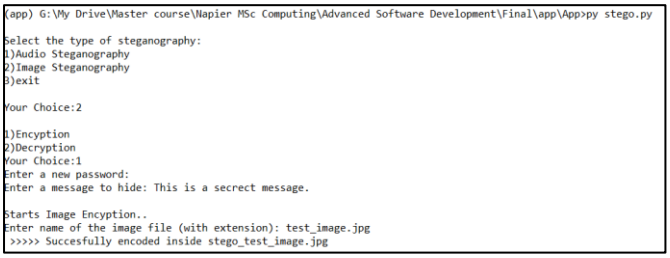


Figure 3: Encryption Process

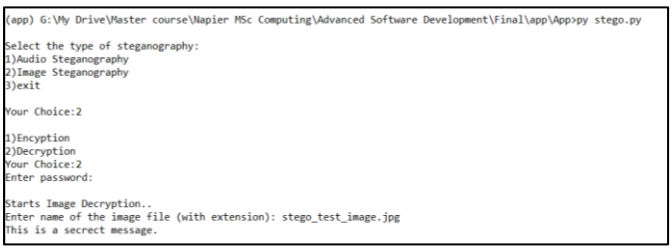


Figure 4: Decryption Process

## 5. Experimental Results

The two techniques from the data hiding techniques will be used to produce the secure stego-object. The evaluation of each method will be done separately from this implementation of data concealing strategies. For the steganography, the evaluation will be performed on the changes of stego-object and original cover object.

The system's performance is controlled by the local host machine: Storage: 1TB HDD with read/write speeds of 100 MB/s, CPU Processor: Intel(R) Core (TM) i7-7500U CPU @ 2.70GHz, 2901 Mhz, 2 Core(s), and Operating System: Windows 10 Pro 64 bit As a result, utilising this local machine, the results of both encryption and detection with cryptography are acquired.

As a result of the changes in their pixel construction and attributes, the difference between the original cover image and stego-object is compared. These outcomes were acquired using the output characteristics of https://www.textcompare.org/image/. Size in bytes, dimension, bit depth, horizontal resolution, and vertical resolution are all aspects of an image's attributes. Bit depth is the term used to describe the colour information stored in an image. The image can store more colour values due to the huge number of bit depth values. The measurement of pixel density, known as horizontal and vertical resolution, is typically expressed in dots per inch (dpi). A 1-inch square has a grid of pixels that is 72 pixels wide by 72 pixels high when a picture has a resolution of 72 dpi. Changes in size, bit depth, and horizontal and vertical resolution can be seen in these findings. Comparing the stego-picture to the cover image, the size has risen. Then the bit depth increased by roughly 8 and both stego-object resolutions were displayed at 96 dpi.

The bytes that will be embedded in the cover picture will be located initially from the above and stored until the final hiding with the pink areas, based on the results of the difference in images. The only way to see these allocations is by employing a tool for comparing and contrasting.

The steganalysis is performed to investigate the presence of the encrypted message. In this steganalysis, the stego-object are used to detect with several steganography. The detection process is performed with decoding the stego-image into text information.

Table 2: Steg-analysis Tools Table

| No. | Steg-analysis Tools | Detection Results |
|---|---|---|
| 1. | Stegdetect | Failed |
| 2. | Mcafee Steganography Defense Initiative | Failed |
| 3. | Steghide | Failed |
| 4. | Steganography Online | Failed |
| 5. | VSL | Failed |

The difference between the cover image and the stego image is being compared in this experiment's results. The test is carried out using Guiffy Image Diff (11.11). The highlighted portion of the stego-object showed a small discrepancy between the stego-image and the original image. The secret data is totally encrypted after starting at the beginning of the image and being put in that highlighted bit.

Figure 5: Original Image

Figure 6: Stego-Image

Figure 7: Image Difference between Original Image and Stego-image

Audio steganography is used on fixed LSBs to determine the point at which the difference between the host message and stego message may be heard. Every sample of the host message's fixed bits is replaced with bits from the secret message without employing the randomness suggested in Bit Selection and Sample Selection. In this following, it is simpler to conceal the existence of noise or secret data. A frequency study of the same data, however, makes it clear that there is foreign data in the media. The main goal of the suggested approach was to keep noise levels low by minimising the disparity between original audio and stego audio. There is no discernible difference between the stego signal and the original signal, even after stegano-manipulation.

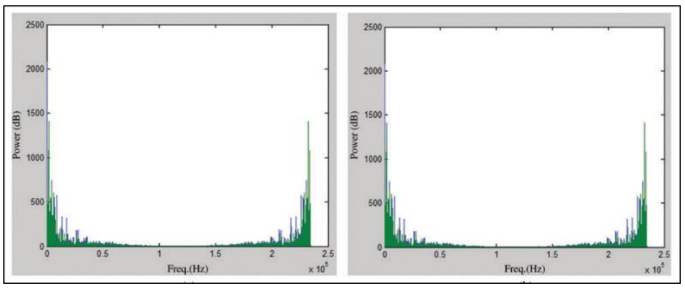


Figure 8: Comparison between Original Audio and Stego-audio

## 6. Conclusion

The system that was put into place had benefits for protecting communication medium thanks to data-hiding algorithms. With base 64 encoding and the SHA-256 hashing technique, the message and secret key can be compressed thanks to the robust security of AES encryption. Utilizing the most recent hashing algorithm development raises the security level of password authentication. Controlling the resilience and lowering the level of suspicion in a visual attack on a carrier using LSB. The techniques based on audio steganography primarily work with audio and spoken signals for a protective communication. While evaluating these techniques, the key steganographic characteristics of capacity, security, and resilience are taken into account. The difference image in the performance section shows the modifications and differences between the original and the stego-image. Because of the LSB approach and base64 encoding, the final output size does not vary even when a significant quantity of data is inserted into the cover image.

## Acknowledgment

I would like to thank my Supervisors at Edinburgh Napier University, for her kind support throughout this research process.

## Conflict of Interest

The authors declare no conflict of interest.

## References

[1] P. Rajkumar, R. Kar, A. K. Bhattacharjee, H. Dharmasa, "*A Comparative Analysis of Steganographic Data Hiding within Digital Images*," International Journal of Computer Applications, vol. 53, no. 1, pp. 1–6, 2012, doi:10.5120/8382-1981.

[2] V. Lokeswara Reddy, Dr.A. Subramanyam, Dr.P. Chenna Reddy, "*Stegnography Rajarao Kaviliga Related papers Implementation of LSB Steganography and its Evaluation for Various File Formats*," J. Advanced Networking and Applications, vol. 868, , pp. 868–872, 2011.

[3] M. Asad, J. Gilani, A. Khalid, "*An enhanced least significant bit modification technique for audio steganography*," Proceedings - International Conference on Computer Networks and Information Technology, pp. 143–147, 2011, doi:10.1109/ICCNIT.2011.6020921.

[4] G. Kessler, "*An Overview of Cryptography (Updated Version 24 January 2019)*," Publications, 2019.

[5] D.S.Abdul. Elminaam, H.M.A. Kader, M.M. Hadhoud, "*Performance Evaluation of Symmetric Encryption Algorithms on Power Consumption for Wireless Devices*," Undefined, pp. 343–351, 2009, doi:10.7763/IJCTE.2009.V1.54.

[6] Rūta Rimkienė, *What is AES Encryption and How Does It Work? | Cybernews*, https://cybernews.com/resources/what-is-aes-encryption/, 2022.

[7] Y. JinaChanu, Kh. Manglem Singh, T. Tuithung, "*Image Steganography and Steganalysis: A Survey*," International Journal of Computer Applications, vol. 52, no. 2, pp. 1–11, 2012, doi:10.5120/8171-1484.

[8] F. Djebbar, B. Ayad, K.A. Meraim, H. Hamam, "*Comparative study of digital audio steganography techniques*," Eurasip Journal on Audio, Speech, and Music Processing, vol. 2012, no. 1, pp. 1–16, 2012, doi:10.1186/1687-4722-2012-25/FIGURES/12.



**Bo** received his BSc in Hons Computing from Edinburgh Napier University and is currently pursuing his MSc in Computing from the same university. Additionally, he is attending Contemporary Technology University for an MSc in Computer Science (Data Science and Applied Artificial Intelligence).

His research interests include Data Analytics and Wrangling, Scripting for Cybersecurity and Networks, Software Security and cryptography.