A Combined Application of Steganography in Variegated Multimedia

|  |  |
| --- | --- |
| Anuj Soni | Nandani Sharma |
| Poornima Institute of Engineering  & Technology, Jaipur, India | Poornima Institute of Engineering  & Technology, Jaipur, India |
| 2017pietcsanuj014@poornima.org | [nandani@poornima.org](mailto:nandani@poornima.org) |

# *Abstract* — Steganography is one of the security techniques working on the concept of obscurity, the process of hiding the confidential message between sender and intended recipient. Steganography has been popularly known for hiding confidential data in image type predominantly. However, it can be equally fruitive in all other types of files, including digital images, audio and video. This paper offers a review on steganography of different types of media. Various implementations have different requirements of the steganography concept. This paper tends to perform steganography techniques over all types of multimedia.

***Keywords -- Multimedia, Data Security, Cryptography, Steganography, Cloud***

# Introduction

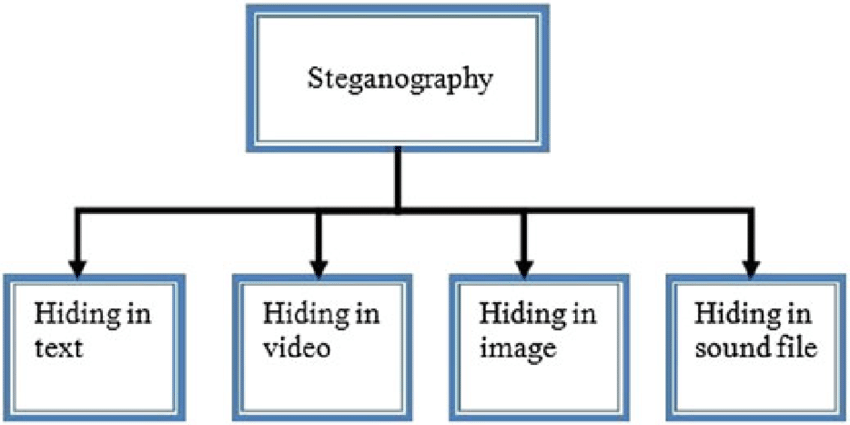
Data security is one of the most sensitive aspects of IOT, Cloud Computing, almost everywhere. In crucial view of the need of efficient techniques in information hiding from any chance of violation of confidentiality, integrity, and availability, different people have come up with different ideas and concepts of data obscurity. Although, steganography is not a new concept but new advancements and improvements have been constantly made for better implementation of steganography. This supports the innovation of different approaches to enhance data security in every field possible.

**Steganography** is the process of hiding secret data within an ordinary, non-secret, file, most commonly images, which act as carrier in order to avoid any breach; the required data can be then decrypted by the intended receiver using a key. Steganography can be combined with encryption standards as an extra step for hiding data; so both Cryptography and Multimedia Processing work hand-in-hand. Steganography techniques can be easily defined as **‘hiding data within data’**, which means to write secretive data in a way that only the sender and receiver (authorized nodes) understand the message and have access to the obscured information to alter it in any way.

Figure 1 explains the architecture of Steganography.

It is needed that we explore better encryption techniques for all types of multimedia because information uploaded onto any warehouse need to be safe and secure from any third-party access and any destructive malware. Numerous publications have been put forward regarding the effectiveness of stenography in majorly data oriented fields like Cloud Computing and IOT.

Cloud Computing has evolved data security issues that are sensitive to the users. It provides an abandoned source of computer resources and facilitates communication as well. Consequently, a high level of data security is required in order to protect the user information. Different articles, reviews and recent researches have supported the applicability of steganography approach for data security over cloud. Furthermore, cryptography is identified among other types of steganography with successful cases of data protection recorded. Therefore, Steganography is an effective technique in cloud computing towards enhancing cloud data security.



**Literature Survey**

1. Jacob Adeboye Ajala, Sanika Singh, Saurabh Mukherjee, & Sudeshna Chakraborty have implemented the “Applications of Steganography Techniques in Cloud Computing” and published their work under IEEE in 2019. The approach they used was chunking of image files for recipient and decryption of images at the receiver side by file recombination techniques. The experiments had successful results; however, accuracies are to be worked upon.

2. Surbhi Singla & Anju Bala have showcased their work by the title “Cryptography & Steganography Algorithms for Cloud Computing” published under IEEE in 2018. The paper implemented a combination of Cryptography and Steganography algorithms to achieve data security over Cloud Platforms. The experiment concluded with a future scope of better algorithms for User node authentication for “Man-in-the-Middle” detection.

3. B. Fathima Mary & D. I. George Amalarethinam published their experiment in the paper by the name “Data Security Enhancement in Public Cloud Storage using Data Obfuscation & Steganography” under IEEE in 2017. The paper contained the MRADO technique to improve the classical obfuscation techniques by integrating substitution and transposition with ASCII values. The experiment was conducted on text type data only, so that leaves a scope for other multimedia.

**Security Survey**

[Ref. 1] According to the study showcased by Ermetic, IDC surveyed 300 senior IT chiefs in the United States across the Banking (12%), Insurance (10%), Healthcare (11%), Government (8%), Utilities (9%), Manufacturing (10%), Retail (9%), Media (11%), Software (10%) and Pharmaceutical (10%) sectors. Organizations ranged in size from 1,500 to more than 20,000 employees. Some of the report’s key findings include:

* 79% of companies experienced at least one cloud data breach in the past 18 months, survey on June 2020, and 43% said they had 10 or even more.
* Top three cloud security threats are security misconfiguration of production environments (67%), lack of visibility into access in production environments (64%) and improper IAM and permission configurations (61%)
* Top three cloud security priorities are compliance monitoring (78%), authorization and permission management (75%), and security configuration management (73%)
* Top cloud access security priorities are maintaining confidentiality of sensitive data (67%), regulatory compliance (61%) and providing the right level of access (53%)
* Top cloud access security challenges are insufficient personal/expertise (66%), integrating disparate security solutions (52%) and lack of solutions that can meet their needs (39%)

The full report is here: [https://bit.ly/2MmZkDt](https://cts.businesswire.com/ct/CT?id=smartlink&url=https%3A%2F%2Fbit.ly%2F2MmZkDt&esheet=52229552&newsitemid=20200603005175&lan=en-US&anchor=https%3A%2F%2Fbit.ly%2F2MmZkDt&index=3&md5=57afd0569962861ecea221001a8676c2).

# Description

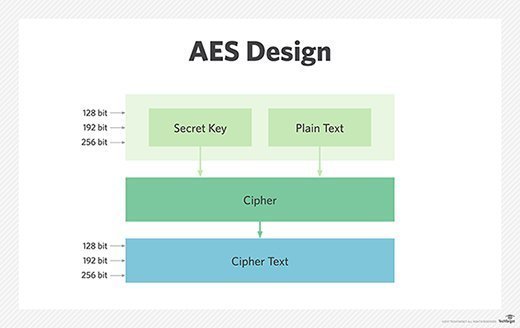
The server security systems randomly produce access keys after an ‘optional’ processing over the key itself for more complex encryption. In this process, the sender encodes the media data with the system produced key which then is concealed into an image that is later split and stored onto the cloud. The server maintains data safety during the data sharing process using Man-in-the-Middle detection as the data proprietors gives the key to the receiver through a one-to-one communication maintaining security as well. The mutual key is covered into a picture to maintain the security of the key.

The data exchange between the servers and the authenticated receivers maintains confidentiality and integrity. Although, cloud computing is useful in computer-based systems, maintaining the data integrity through the systems is the most substantial aspect of cloud computing. In order to effectively accommodate multiple users through the cloud computing program, the platform utilizes cloud resources to the users through 3 services (IaaS, PaaS, and SaaS).

# Algorithm

AES Encryption on Text:

* AES Mode
* Padding
* Key
* Block Cipher
* Hashing





**AES Algorithm**

State = M

AddRoundKey(state, &w[0])

For i = 1 at step 1 till 9

SubBytes(state)

ShiftRows(state)

MixColumns(state)

AddRoundKey(state, &w[i\*4])

End for

SubBytes(state)

ShiftRows(state)

AddRoundKey(state, &w[40])

**Audio Encryption:**

1. Obtain Audio File - WAV File Format for High Quality PCM Audio Data.
2. Initialize source audio file.
3. Get data from source audio file as a string of bytes.
4. Convert data into list of readable integer ordinal format.
5. Initialize text message to be embedded.
6. Hide text message into the list order data.

* 1 frame = 4 bytes; pack order data to hex and write byte by byte.
* Gets non-readable data from the source wave file.
* Return all the wave parameters as a tuple (immutable).

1. Get output file path.
2. Write new embedded data into a new file (filename given earlier).

Note – When encrypting into images, the following steps should be considered:

* Open an image and observe the pixel in hexadecimal.
* If the pixels blue channel falls in the 0-5 range then 1 bit of information is stored.
* End the stream with a delimiter of 15 1’s and 0’s to take up 2 bytes.
* When time is to retrieve it pull all the blue bits of 0 and 1 until the stream obtains the delimiter of fifteen 1’s and 0’s.
* User-defined data manipulating functions include rgb2hex(), hex2rgb(), str2bin(), and bin2str().
* The operations will include hiding, retrieving, encoding, and decoding, which will form the methods.

# RESULTS

We have successfully implemented the steganography over text type data, images data, and audio files. We have also performed AES encryption on the Text Data and Image Slicing using Python as the coding language. In the cloud based systems, data can easily be altered by violation of the CIA principles of information security by ‘Man-in-the-Middle’ users (intruders). In conclusion, this issue has raised the need to enhance data security especially for multimedia files with an amalgamation of security of each type of files uploaded onto the cloud platforms.

# Future Work

Since we have covered a small part on steganography, a lot of work is left out. We will be working on video steganography and asymmetric key encryption. Concluding the work, we find that although steganography is not a new concept, still it thrives for more complex encryption system and as we will see advancement in Cryptographic standards, new updates will also be seen in Steganographic system.

# References

1. Jacob Adeboye Ajala, Sanika Singh, Saurabh Mukherjee, & Sudeshna Chakraborty have implemented the “Applications of Steganography Techniques in Cloud Computing” and published their work under IEEE in 2019.
2. Surbhi Singla & Anju Bala have showcased their work by the title “Cryptography & Steganography Algorithms for Cloud Computing” published under IEEE in 2018.
3. B. Fathima Mary & D. I. George Amalarethinam published their experiment in the paper by the name “Data Security Enhancement in Public Cloud Storage using Data Obfuscation & Steganography” under IEEE in 2017.