International Journal of Interdisciplinary Innovative Research &Development (IJIIRD)

ISSN: 2456-236X

Vol. 04 Issue 02 |2020

# Data Protection Using Fibonacci Series Encryption And Text-In-Image Steganography

Uzochukwu Onyinye Osakwe

*Master student, Department of MCA, Jain Deemed-to-be University, Bengaluru, Karnataka, India*

## ABSTRACT

***In this present era, security has become one of the major concerns in the IT industry. To improve the security of information encryption and decryption mechanism was formulated. Encryption is the process of encoding a message or information in a way that an unauthorized person won't gain access to the information. A technique known as Steganography was created for hiding secret data within an ordinary file, pictures etc in order to avoid detection of the information. The use of steganography, in this project, is combined with encryption to create an extra layer of security to data and information.***

***This project ensures that a file stays hidden from unauthorized person. Text in image steganography helps in the hiding of a text file in an image. For enhanced security, the text in the file is secured using the Fibonacci series. These mechanisms are implemented using python.***

***Keyword: - Encryption, Decryption, Steganography, Cipher, unauthorized, Security.***

## 1. INTRODUCTION

On a daily basis, security breaches occur and one way to prevent it is by implementing security management. Management of security has been a top concern in the corporate world. Now it has been able to influence personnel. Millions of people get their information stolen every day and very little approaches are taken in to minimize this. This project has been created to a high level of security through the hiding of data with the help of encryption/decryption and steganography.

The word 'cryptography' was coined by combining two Greek words, 'Krypto' meaning hidden and 'graphene' meaning writing.

An unauthorized person cannot extract any information, even if the jumbled messages fell in their hand, Cryptography involves encoding data to ensure that it is protected from an unauthorized person. Cryptography converts data into a format that is unreadable for an unauthorized user, allowing it to be transmitted without unauthorized entities decoding it back into a readable format. Information security uses cryptography on several levels. The information cannot be read without a key to decrypt it. The information maintains its integrity during transit and while being stored, Cryptography, the process of hiding the messages to introduce secrecy in information security.

Steganography is data hidden within data. Steganography is an encryption technique that can be used along with cryptography as an extra-secure method in which to protect data. Steganography techniques can be applied to images, a video file or an audio file. Steganography is used by those seeking to pass secret message or code and ensure no one has access to them. Steganography can be used to conceal almost any type of digital content, including text, image, video or audio content; the data to be hidden can be hidden inside almost any other type of digital content.

### 1.1 History of Cryptography and Steganography

The word "cryptography" is derived from the Greek *kryptos*, meaning hidden. The origin of cryptography is usually dated from about 2000 B.C., with the Egyptian practise of hieroglyphics. The first known use of a modern cypher was by Julius Caesar (100 B.C. to 44 B.C.), who did not trust his messengers when communicating with his governors and officers. In recent times, cryptography has turned into a battleground of some of the world's best mathematicians and computer scientists. As governments do not wish certain entities in and out of their countries to have access to ways to receive and send hidden information that may be a threat to national interests, cryptography has been subject to various restrictions in many countries, ranging from limitations of the usage and export of software to the public dissemination of mathematical concepts that could be used to develop cryptosystems.

Steganography's origins date back to ancient times. The first recorded uses of steganography can be traced back to 440 BC when Herodotus mentions an example of steganography in the histories of Herodotus, ancient example is that of histories, who shaved the head of his most trusted slave and tattooed a message on it. After his hair had grown the message was hidden. The purpose was to instigate a revolt against the Persians. Wax tablets were in common use then as reusable writing surfaces, sometimes used for shorthand. An ancient example is that of histories, who shaved the head of his most trusted slave and tattooed a message on it. After his hair had grown the message was hidden. The purpose was to instigate a revolt against the Persians. Special "inks" were important stenographic tools even during the Second World War. Using invisible ink to hide secret messages in otherwise inoffensive messages. The ancient Chinese wrote messages on fine silk, which was then crunched into a tiny ball and covered in wax. The messenger then swallowed the ball of wax hiding documents recorded on microdot -- which can be as small as 1 millimetre in diameter.

### 1.2 Review of Literature

Although security has been considered in the design of the basic Internet protocols, many applications have been and are being designed with minimal attention paid to issues of confidentiality, authentication, and privacy. As our daily activities become more and more reliant upon data networks, the importance of understanding such security issues will only increase [1]. This is where cryptography comes into the picture.

Encryption is a method of transforming data with the intension of keeping it a secret. It uses an algorithm called a cypher to encrypt data and it can be decrypted only using a special key. The encrypted information is known as ciphertext and the process of obtaining the original information (plaintext) from the ciphertext is known as decryption. Encryption is especially required when communicating over an untrusted medium such as the internet, where information needs to be protected from other third parties. Modern encryption methods focus on developing encryption algorithms (cyphers) that are hard to break by an adversary due to the computational hardness (therefore could not be broken by a practical means) [2]. Steganography is the technique in which a message is hidden in a carrier object. In image steganography, particularly, the hidden message should not be visible using simple eye inspection. The usual parties in a steganography technique are the sender, who hides a message inside a medium and the steganography file receiver, who will unveil the transmitted hidden message. The message is embedded in an image called a cover image; after the message is hidden, we have a steganography file. Usually, a secret key known as a steganography-key is transmitted between the sender and the receiver, so that the latter can decode the message [3]. Steganography involves hiding of text, image or any sensitive information inside another image, video or audio in such a way that an attacker will not be able to detect its presence. Steganography is, many times, confused with cryptography as both the techniques are used to secure information. The process of steganography is expressed by the following formula: Steganography_File = Cover_Image u Secret_Key u Message_To_Hide
The difference between steganography and cryptography is as follows [6][7]:

1 Steganography hides the existence of communication whereas cryptography makes the actual message illegible.
2 Steganography does not alter the overall structure of the data while cryptography alters the overall structure of the data.
3 The final result obtained in steganography is known as stego media while the same
4 In cryptography is called ciphertext.

### 1.3 CRYPTOGRAPHY AND STEGANOGRAPHY TECHNIQUES

There are three types of cryptographic techniques used in general:

- Symmetric-key Cryptography: In this technique, both the sender and receiver share a single key. The sender uses this key to encrypt the plaintext and send the ciphertext to the receiver. On the other side, the receiver applies the same key to decrypt the message and recover the plain text.
- Hash Functions: No key is used in this algorithm. A fixed-length hash value is computed as per the plain text that makes it impossible for the contents of the plain text to be recovered. Hash functions are also used by many operating systems to encrypt passwords.
- Public-key Cryptography: This is the most revolutionary concept in the last 300- 400 years. In Public-Key Cryptography two related keys (public and private key) are used. The public key may be freely distributed, while its paired private key, remains a secret. The public key is used for encryption and for decryption private key is used.

Text steganography can be achieved by altering the text formatting, or by altering certain characteristics of textual elements (e.g., characters). The goal in the design of coding methods is to develop alterations that are reliably decodable (even in the presence of noise) yet largely indiscernible to the reader. Various text steganography techniques include:

- Line-Shift Coding: Here, text lines are vertically shifted to encode the document uniquely.
- Word-Shift Coding: The codewords are coded into a document by shifting the horizontal locations of words within text lines while maintaining a natural spacing appearance.
- Feature Coding: In feature coding, certain text features are altered, or not altered, depending on the codeword.

Hiding information inside images is a popular technique, where a secret message can be hidden and then transferred to the intended receiver. To hide a message inside an image without changing its visible properties, the cover source can be altered in “noisy” areas With many colour variations, so less attention will be drawn to the modifications. The most common methods to make these alterations involve the usage of the least-significant bit or LSB, masking, filtering and transformations on the cover image, as mentioned below:

- LSB: A simple approach for embedding information in the cover image is using the Least Significant Bits (LSB). It is a technique in which we hide messages inside an image by replacing the Least Significant Bit of image with the bits of the message to be hidden.
- Masking and Filtering: It involves the modification of the image that can involve indiscernible changes in the image, even if the changes are not visible to the naked eye.
- Transformation: This is an overwhelmingly complex technique for image steganography. This uses discrete cosine transformation, that is majorly used in JPEG image compressions.

Finally, secret messages can also be hidden in audio files using the following methods:

- LSB: The audio signals are converted to digital binary sequences. The Least Significant Bit of the binary sequence is converted to the binary value of the message.
- Phase Coding: It is based on the analysis of the phase discontinuities. The secret message is divided according to bits and is encoded as the phase shifts in the phase spectrum in the audio file.
- Spread Spectrum: There are 2 approaches in this method: Direct Sequence Spread Spectrum (DSSS) and Frequency Hopping Spread Spectrum (FHSS)
- Echo Hiding: In this technique, the secret message is embedded into the cover audio as an echo. They are adjusted in a way such that the echoes are inaudible to humans.

## 2. DESIGN METHODOLOGY OF PROPOSED WORK

This project can be said to be a tool that uses encryption and steganography mechanism used to provide an extra layer of security to data/information stored by the user in the system. This project uses the Fibonacci series technique for encryption and decryption. In this technique, one can secure any type of files. In this project, we propose an image steganography method which hides data in it. Image Steganography uses an image as the cover to hide the secret message.

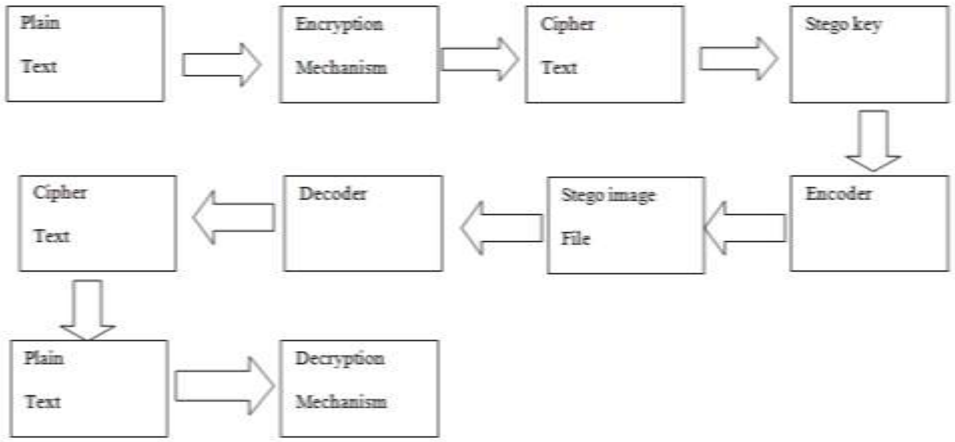

Fig -1: proposed working

This project provides two levels of security as it not only encrypts the message but also performs image steganography by sending the encrypted message along with the image. This project is designed to flow in basically 2 phases. These phases include Cryptography and Steganography which has sub-phases. The project has 2 phases; the first phase consists of an encrypter that encrypts the saved text file. This encrypter uses a principle of Fibonacci series, the file is shifted according to its position on the file in reference to the Fibonacci series principle. In the next sub-phase, we make use of a series of codes to implement a steganography technique. At this phase, the program conceals the encrypted text file inside an image.

### 2.1 ENCRYPTOGRAPHY PHASE

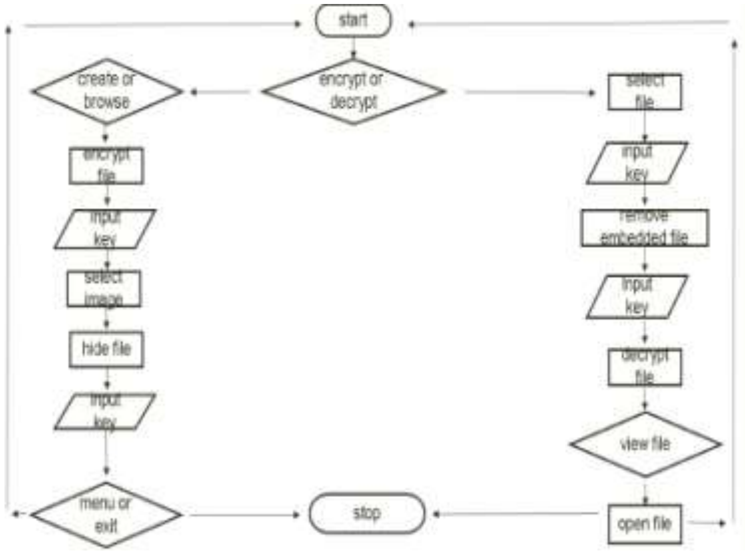

Fig -2: Data Flow Diagram (DFD)

### 2.2 ENCRYPTION PHASE

Encryption is the process of converting plain text into ciphertext, which has no meaning. In the encryption phase, the message is taken into the encrypter and then the encrypter encrypts the message. Our project uses the Fibonacci series to implement the encryption phase. This happens by splitting the messages into their separated words, the words from the message are reversed and then that word is split into letters. These letters are now incremented and decremented alternatively based on the Fibonacci series. For example, if the word from a message is ‘ABC’ and that word is reversed as ‘CBA’. That word (‘CBA’) is now spitted into a letter. Now the number of letters in the word ‘fed’ is 3 so the Fibonacci series of the length of the word is ‘1,1,2’ (This excludes the first 0).

- Now the first letter of the word ‘c’ is incremented by the first number in the Fibonacci series which is 1, making ‘c’ to become’.
- The incremented letter ‘d’ is now incremented by the next Fibonacci series number which is 1 again. Therefore, converts’ to ‘e’.
- The next Fibonacci series number is 2. The encrypted letter now ‘e’ is then incremented by 2 which converts ‘e’ to ‘g’.
- Now the next letter ‘b’ will be decremented by the first number of the Fibonacci series which changes ‘b’ to ‘a’.
- The incremented letter ‘a’ is now decremented by the next Fibonacci series number which is 1 again. Therefore, converts ‘a’ to ‘`’, which is the minimum ASCII value our letters can be set as.
- The next Fibonacci series number is 2. The encrypted letter now ‘!’ is then incremented by 2 which converts ‘`’ to ‘^’.
- Then the next letter ‘a’ will be incremented by the first number of the Fibonacci series which changes ‘a’ to ‘b’.
- The incremented letter ‘b’ is now incremented by the next Fibonacci series number which is 1 again. Therefore, converts ‘b’ to ‘c’

- The next Fibonacci series number is 2. The encrypted letter now ‘e’ is then incremented by 2 which converts ‘c’ to ‘e’.
- Now the encrypted text of ‘ABC’ is now ‘g^e’

### 2.3 DECRYPTION PHASE

In this phase, the project uses the Fibonacci series principle to convert the ciphertext into a plain text. What this does it that the ciphertext is passed into the decrypter. Then it splits that cypher message into letters just as the encryption phase does and then decrements and increments the letters alternatively. Remember the encrypted text created before was ‘g^e’. Both the encryption and decryption phase act alike in this project but what differs is if the first letter is either incremented or decremented and then the rest of the letters in that word will follow alternatively to the previous letter. In decryption, the first letter of the word is decremented.

- The encrypted word being passed in here is ‘g^e’. This is divided into letters and the length of the word (g^e) is recorded as 3 to define the number of Fibonacci series will be implemented.
- Now the first letter of the word ‘g’ is decremented by the first number in the Fibonacci series which is 1, making ‘g’ to become ‘f’.
- The incremented letter ‘f’ is now decremented by the next Fibonacci series number which is 1 again. Therefore, converts ‘f’ to ‘e’
- The next Fibonacci series number is 2. The encrypted letter now ‘e’ is then decremented by 2 which converts ‘e’ to ‘c’.
- Now the next letter ‘^’ will be incremented by the first number of the Fibonacci series which changes ‘^’ to ‘_ ’.
- The incremented letter ‘_’ is now incremented by the next Fibonacci series number which is 1 again. Therefore, converts ‘ _ ’ to ‘ ` ’, which is the minimum ASCII value our letters can be set as.
- The next Fibonacci series number is 2. The encrypted letter now ‘!’ is then incremented by 2 which converts ‘ ` ’ to ‘a’.
- Then the next letter ‘e’ will be decremented by the first number of the Fibonacci series which changes ‘e’ to’.

- The incremented letter ‘d’ is now decremented by the next Fibonacci series number which is 1 again. Therefore, converts’ to ‘c’
- The next Fibonacci series number is 2. The encrypted letter now ‘e’ is then incremented by 2 which converts ‘c’ to ‘a’.
- Now ‘g^e’ is now converted to ‘cba’.
- Then the word(cba) is now reversed to ‘abc’

## 3. STEGANOGRAPHY PHASE

This phase works with basically two mechanisms: the insertion mechanism and the extraction mechanism. The insertion mechanism encodes the text to the image and the extraction mechanism decodes the text out of the image. To understand steganography, you must be able to understand the concept of images. Images are simply made out of pixels; a huge number of pixels are combined to make an image look the way they are. A pixel is the smallest unit of a digital image or graphic that can be displayed and represented on a digital display device. Pixels are combined to form a complete image, video, text.

These pixels are then combined together to produce an image. An image can contain hundreds/thousands of pixels. Each pixel is made up of certain data. Those data are called RGB (Red Green Blue). These data identify the mode of the images, RGB holds tons of values and these values determine the colour of the image pixel when joined together. If the RGB is (0,0,0) then the pixel will have to be completely black and if the RGB is (255,255,255) then the pixel is going to be white. This RGB has 0 as its minimum and 255 as its maximum, exceeding this range will lead to discolouration of the pixel. The RGB data can hold different values and those different values can promote a color (0,234,123),(34,65,124),(189,62,15),etc.

### 3.1 INSERTION MECHANISM

The insertion mechanism simply involves embedding the secret message to the carrier image. It makes use of certain customized principles to hide a message inside an image. The following explains the principles used in promoting data hiding in images.

- A copy of the selected image is used to hide the data
- The secret message is passed into the program, divided into multiple letters (including the spaces) and then converted into their binary format.
- Each letter/character is now in their binary form.
- Since the binary number contains 8 bits, we are going to take 3 pixels out of the image which is holding 3 RGB data and use those each data to hold a single bit.
- Then that RGB data is returned back to the image and implemented

### 3.1 EXTRACTION MECHANISM

The extraction mechanism refers to the extraction of the secret message from the image. This removes the secret message that is still in its encrypted format out of the image. The extraction mechanism gets the pixels from the image by row and column. Since these pixels contains RGB data and the message has been entered into this data. The message can now be extracted.

## 4. CONCLUSIONS

This project shows that an encryption and steganography algorithms can be created to serve the purpose of ensuring the protection of data/information by implementing cryptography for making sensitive data unreadable and steganography to hide the data in an image.

With the results showing that the image still remains intact and the encrypted file has been decrypted properly to its original state, it can be safely said that the algorithm has been successfully implemented.

## 5. ACKNOWLEDGEMENT

I want to especially thank **Professor. Subarna Panda** for guiding me throughout this research paper, which has expanded my knowledge of data security. Without his support I do not think this research paper will be a success, I am very thankful.

## 6. REFERENCES

[1] Lipi Kothari, Rikin Thakkar, Satvik Khara, "Data hiding on the web using a combination of Steganography and Cryptography", International Conference on Computer, Communications and Electronics (2017)

[2] Sumeet Kaur, Savina Bansal, RK Bansal, "Steganography and Classification of Image Steganography Techniques", International Conference on Computing for Sustainable Global Development (2014)

[3] Juan M. Gutiérrez-Cárdenas, "Secret Key Steganography with Message Obfuscation by Pseudo-Random Number Generators", IEEE 38th Annual International Computers, Software and Application Conference Workshops (2014)

[4] A. Cheddad, J. Condell, K. Curran, and P. McKevitt, "Digital image steganography: Survey and analysis of current methods", vol. 90, pp. 727–752 (2010)

[5] B. Dunbar, "A Detailed look at Steganographic Techniques and their use in an Open- Systems Environment" (2002)

[6] Rina Mishra, Praveen Bhanodiya, "A Review on Steganography and Cryptography", International Conference on Advances in Computer Engineering and Applications (2015)

[7] Khan Muhammad, Jamil Ahmad, Haleem Farman, Muhammad Zubair, "A Novel Image Steganographic Approach for Hiding Text in Color Images using HSI Color Model", Islamia College Peshawar (2015)

[8] www.google.com

[9] www.github.com

[10] www.init.org

[11] www.quora.com