Implementation of 3-D Pythocrypt along with Image Steganography.

Sumanth N [1 *]; Shrinidhi Holla[1]; Prajwal VS[1]

nsumanthbhat@gmail.com

Abstract

The research work describes an attempt to integrate the 3-D Pythocrypt cryptographic technique with Image Steganography and provide better security for message transmission. 3-D Pythocrypt is a new technique where we use the properties of 3-D geometric shapes to encrypt and decrypt plain text. Image-Steganography is a cryptographic technique used to hide the information within the pixel of the Image. The main ideology is that the message which needs to be transmitted is converted to unreadable form using the 3-D Pythocrypt algorithm and ciphertext which is obtained is hidden in the pixels of the Image, the Image containing the Image is transmitted to the receiver thereby maintaining the confidentiality and secrecy.

Keywords: 3-D Pythocrypt, Image-Steganography, Encryption, Decryption, Stego-file, Algorithm, Ciphertext

Introduction

The present web world is overwhelmed with a gigantic measure of information that is coming about information spillage and robbery of data. Bunches of difficulties emerge while moving or getting different sorts of encrypted information, messages, or data particularly utilizing public organizations. Digital wrongdoing is one of the greatest blemishes in this completely associated internetworking world. We present the strategy 3-D Pythocrypt along with Image-Steganography. 3-D Pythocrypt is a new technique, where the properties like area, volume, perimeter, etc. of specific 3-D geometric shapes are used to encrypt and decrypt the message which needs to be transmitted to attain confidentiality, Steganography is the art of hiding the fact that communication is taking place, by hiding information in other information. Many different career file formats can be used, but digital images are the most popular because of their frequency on the Internet. For hiding secret information in images, there exists a large variety of steganography techniques some are more complex than others and all of them have respective strong and weak points.

3-D Pythocrypt:

There is a huge number of cryptographic systems which can be used to encrypt the message and transmit the ciphertext that is generated so that the confidential information is made readable only by the intended user. Traditionally cryptographic systems are classified into two categories, Symmetric, and Asymmetric cryptographic systems. In Symmetric cryptographic systems, the same key is used for both encryption and decryption process, some of the popular symmetric techniques like the Caesar cipher model, play fair cipher model, and hill cipher model are the common examples of it. The asymmetric cryptographic system uses different keys for encryption and decryption processes called public keys and private keys, the most popular and widely used asymmetric algorithm is RSA.

3-D Pythocrypt is a new and young technique that is used to encrypt and decrypt a given message using a known 3-D geometric shape[1]. This methodology uses the geometric attributes of shapes such as Area, Volume, Perimeter, etc., to generate an algorithm using which the plain text can be encoded into nondecipherable text. This new approach is unique compared to all other existing algorithms as it does not need a key for encryption but generates one for decryption [1].

Image-Steganography:

The word steganography is of Greek origin and means "covered or hidden writing". Steganography is the art and science of communicating in a way that hides the existence of communication. By contrast, cryptography obscures the meaning of a message, but it does not conceal the fact that there is a message. The main advantage of steganography is that messages do not attract attention to themselves to messengers or recipients. Whereas the goal of cryptography is to make data unreadable by a third party, the goal of steganography is to hide the data from a third party. Often, steganography and cryptography are used together to ensure the security of the converted message.

There are many different techniques used to hide the information inside the images. In our project, we use Least Signification Bit substitution. The LSB Substitution is a method that is used to hide the information in the pixels of the image.

Least-Significant-bit substitution (LSB):

LSB substitution is the process of adjusting the least significant bit pixels of the carrier image. The LSB insertion varies according to the number of bits in an image. Ex: For an 8-bit image, the LSB bit i.e., the 8th bit of each byte of the image is changed to the bit of secret message. Similarly, for a 24-bit image, the colors of each component like RGB (red, green, blue) are changed. If the LSB of the pixel value of cover image C(i, j) is equal to the message bit SM of the secret message to be embedded, C(i, j) remains unchanged; if not set the LSB of C(i, j) to SM[2].

Proposed system

The system combines the two different techniques i.e., 3-D Pythocrypt and Image-Steganography to form a complex system that provides confidentiality to our message and also provides security by hiding the information inside the image. Instead of using traditional Image-Steganography which hides the text inside the image, here, the image contains the ciphertext which is the output of the 3-D Pythocrypt algorithm. The whole system can be constructed as a tool that encapsulates these two techniques and provides a high level of abstraction to the end-users.

Algorithm

The 3-D Pythocrypt algorithm is based on the volumetric formula of the octahedron geometric shape. The octahedron shape has six faces, 12 edges, and six vertices.

Insert Figure 1

The octahedron can be divided into two pyramids.

Insert Figure 2

The volume of a single pyramid is given by,

Volume of a pyramid = (base area * height) / 3

In the case of a regular octahedron shape, the base area is given by the following equation,

The base area of a regular octahedron = a^2

So, the volume of the octahedron is given by,

The volume of octahedron = 2 * Volume of Pyramid

If we assume the volume of the pyramid as ‘v’, the height of the pyramid as ‘h’, base area as ‘a^{2}’ then, we write the above equation as,

Volume of octahedron = 2 * v

Where,

$$v = (a^2 * h) / 3$$

Hence, the volume of the octahedron is derived as,

Vol. of Octahedron = $(2 * a^2 * h)/3$

Encryption Phase:

The message which consists of English alphabets and/or symbols is converted to its ASCII equivalent values which are in decimal format. These numbers are halved and considered as inputs to calculate the volume of octahedron which is our ciphertext.

$$C = (2 * a^2 * h)/3$$

Where C is the ciphertext. This ciphertext along with the value of ‘a’ which acts as a key is fed as input to the Image-Steganography algorithm. Usually, text values are the inputs for the Image-Steganography algorithm. Here, we use the ciphertext generated which is in decimal format as the input for the Image-Steganography algorithm. We LSB technique as described earlier in Image-Steganography where the least bit of every pixel of the image is replaced by ciphertext bits thereby maintaining the quality of the image and achieving the desired secrecy.

Decryption Phase:

In the decryption phase, the ciphertext and the key are extracted from the image(s) separately and are fed as input to the 3-D Pythocrypt algorithm. One of the variables ‘a’ or ‘h’ can be used as a key however here, the value of variable ‘a’ is used as the key. Note that the key is only required in the decryption phase. Hence, we have ‘a’ and ciphertext, we need to find ‘h’. This can be calculated using the formula,

$$h = (3 * C) / (2 * a^2)$$

where C is the ciphertext and ‘a’ is the key.

Implementation

The design of the system contains two parts, the 3-D Pythocrypt and Image-Steganography. The message which needs to be encrypted is fed as an input to the 3-D Pythocrypt algorithm. The Pythocrypt algorithm converts this message to the ciphertext which is difficult to understand and also the key is generated. This will be in decimal format. The generated ciphertext and the key are now fed as input to the Image-Steganography algorithm, which hides the ciphertext and key within the image using a delimiter. However, if the length of the ciphertext is large then the key is hidden in a different image, and a special symbol or a character can be placed at the first bit to identify the image which contains the key.

Insert Figure 3

The decryption process is the reverse of encryption. At the receiver side, the image which is also called Stego-file is fed as an input to the Image-Steganography algorithm. This algorithm extracts the ciphertext and the key from the image(s) and is stored in a variable. The original message is reconstructed by deciphering the ciphertext with the help of the key.

Insert Figure 4

Insert Figure 5

Experimentation

The 3-D Pythocrypt algorithm is suitable for English alphabets, symbols, decimal values as a string, or any character which has equivalent ASCII values. The ciphertext generated is shown in file 3(additional file 1). This algorithm also works for numerical inputs, with a slight modification in the algorithm i.e., instead of converting the input to its ASCII values we can directly use the input values which are halved as the values for the variables. Also, the ciphertext and key are recovered from the Image and eventually extract the original message from the 3-D Pythocrypt algorithm.

Result

The output of the encryption phase is the image containing the ciphertext. Observe the fig. 7, which compares the original image along with the Stego-file which is the image containing the ciphertext. It is insurmountable to identify the text hidden inside the image.

The additional file contains the 3-D Pythocrypt program and the Image-Steganography program that takes ciphertext as the input. File 1(additional file 1) is the 3-D Pythocrypt program written in Java programming language, file 2(additional file 1) is the implementation of Image-Steganography in python programming language. File 3(additional file 1) is the snapshot of the result of 3-D Pythocrypt algorithm when it is tested with a sample text and also the time taken by the algorithm to encrypt and decrypt the given plain text is calculated. File 4(additional file 1) displays the time taken to encrypt and decrypt the ciphertext to/from the image selected.

Conclusion

With the results of the experimentation, it is concluded that,

- The 3-D Pythocrypt along with Image-Steganography is a new technique that can be implemented to attain a higher security level along with secrecy.
- It provides better security than most of the existing cryptographic techniques and is infeasible for cryptographic attacks.
- Only some part of the numerical values can be obtained and also it is infeasible to find the original plain text by observing the pattern of ciphertext.
- The 3-D Pythocrypt algorithm can be made difficult by implementing many geometric shapes and selecting which shape to be used dynamically.
- The codes are designed separately and one can make use of only the 3-D Pythocrypt algorithm to transmit the ciphertext if there is no need for data secrecy. This algorithm is concise and can be integrated into data transferring platforms.

Declarations

Availability of Data and materials

All the data that are used in this work is open source and is available on the internet. The working prototype of the 3-D Pythocrypt algorithm (file 1), the Image-Steganography algorithm (file 2) , the sample output of 3-D Pythocrypt algorithm (file 3) and estimated time of Image-Steganography(file 4) are submitted in the additional file attached respectively. The required figure and data are presented in this work. No additional datasets or materials are used in the work presented.

Competing Interests

The authors declare that they have no competing interests.

Funding

NA

Author's contribution

SN developed the 3-D Pythocrypt algorithm and developed the system. SH and PVS provided insight into the survey methods and references. SN drafted the manuscript. All the authors have read and approved the final manuscript.

Acknowledgments

NA

Author Details

[1] Student, Department of Information Science and Engineering, Jyothy Institute of Technology - Bangalore affiliated to Visveswaraya Technological University, Belgaum, Karnataka, India

References

S., Harsha & Bhaskar, N. & Prakash, Mysore. (2015). A 3-d advancement of PythoCrypt for any file type. Journal of Open Innovation: Technology, Market, and Complexity. 1. 10.1186/s40852-015-0022-8.

Dewangga, I.G.A.P. & Purboyo, Tito & Nugrahaeni, R.A.. (2017). A new approach of data hiding in BMP image using LSB steganography and caesar vigenere cipher cryptography. International Journal of Applied Engineering Research. 12. 10626-10636.

Mstafa, Ramadhan & Bach, Christian. (2013). Information Hiding in Images Using Steganography Techniques. 10.13140/RG.2.1.1350.9360.

Figure Legend

Fig 1: Octahedron: A 3-D geometric shape.

Fig2: Octahedron: Expressed as 2 pyramids.

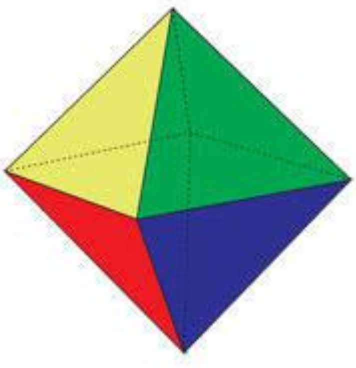
Fig 3: Flow of Encryption process.

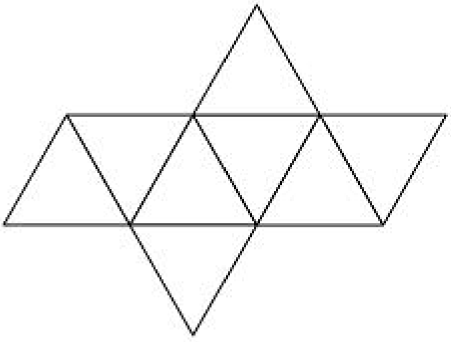
Fig 4: Flow of Decryption process.

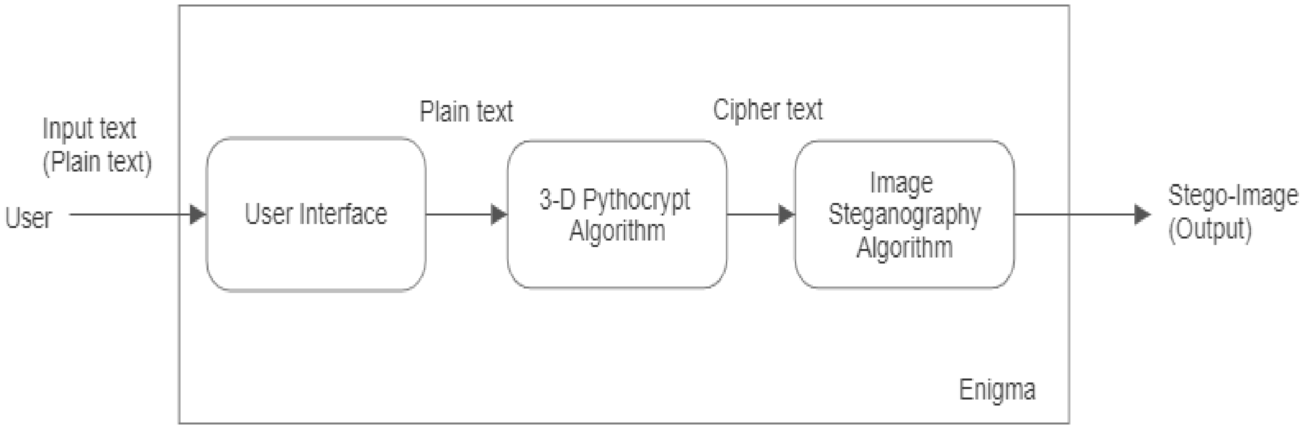
Fig 5: Workflow of the entire process.

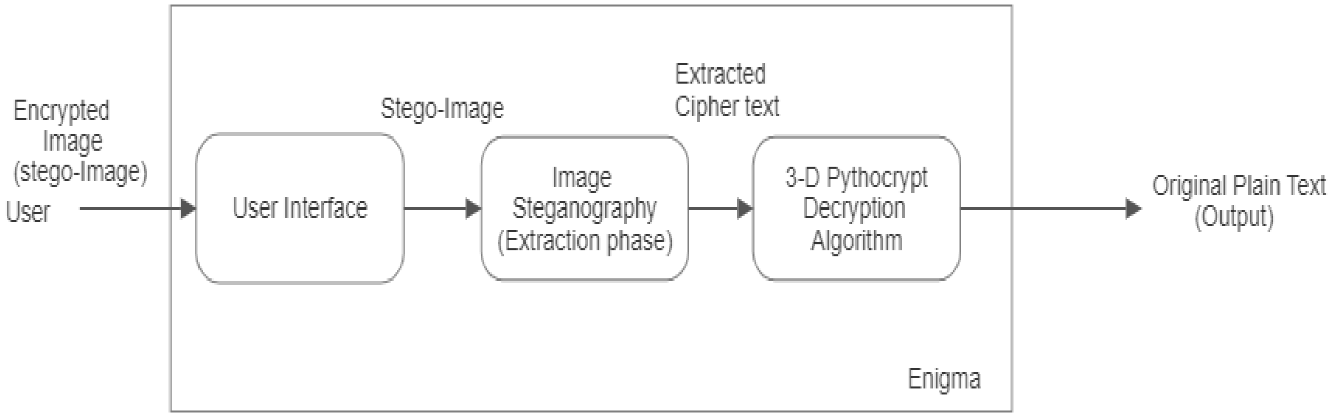
Fig 6: Image of ciphertext generated from 3-D Pythocrypt algorithm.

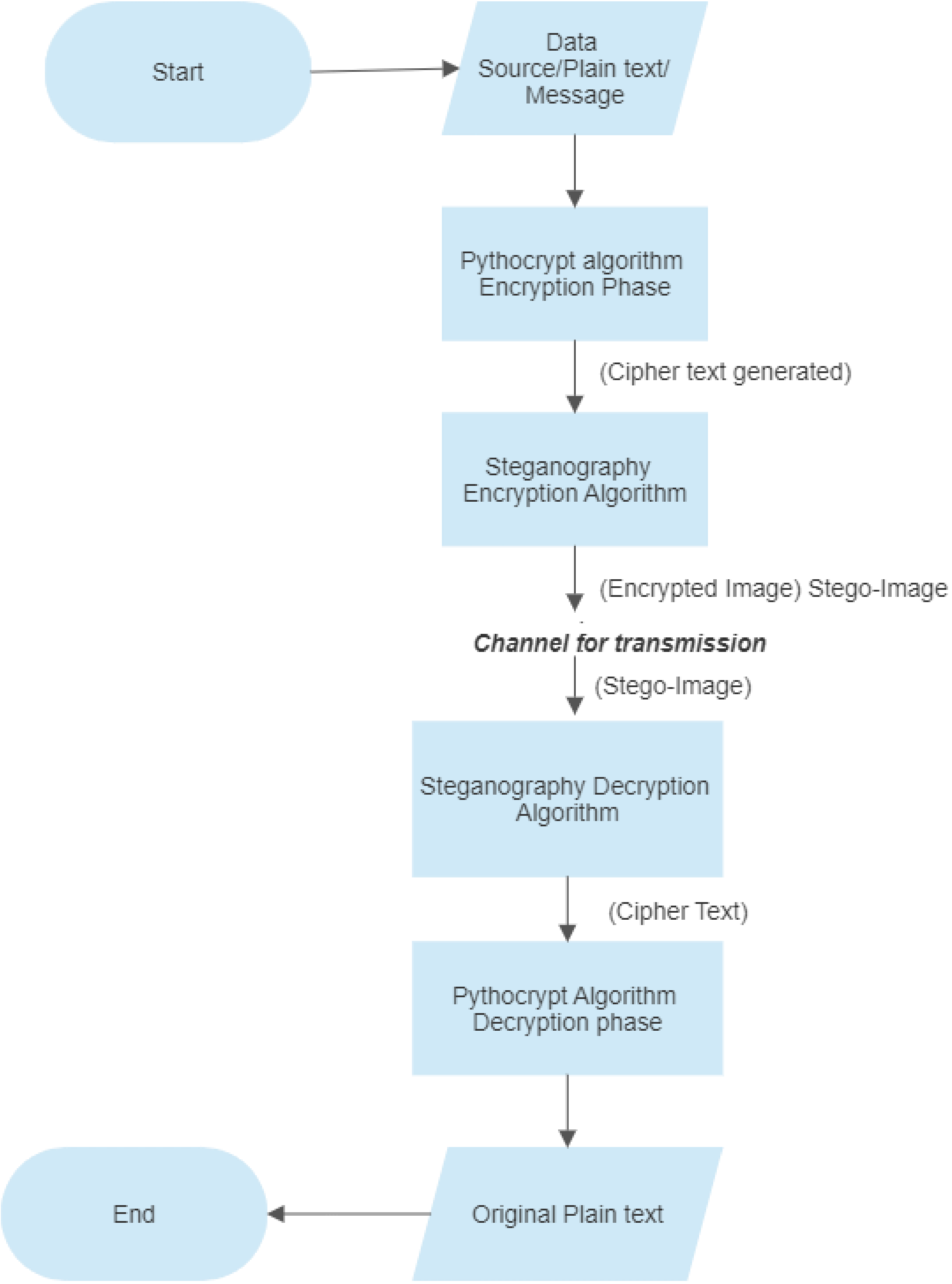
Fig 7: Comparison of the original image with Stego-file








Encrypted Image (stego-Image)
User
User Interface
Stego-Image
Image Steganography (Extraction phase)
Extracted Cipher text
3-D Pythocrypt Decryption Algorithm
Original Plain Text (Output)
Enigma


Start
Data Source/Plain text/ Message
Pythocrypt algorithm Encryption Phase
(Cipher text generated)
Steganography Encryption Algorithm
(Encrypted Image) Stego-Image
Channel for transmission
(Stego-Image)
Steganography Decryption Algorithm
(Cipher Text)
Pythocrypt Algorithm Decryption phase
Original Plain text
End

Source Image

Encoded Output Image