Data concealing using Hyperchaotic Text Encryption and Image Steganography

Hargobind Singh
Electronics and Telecommunications
Sardar Patel Institute of Technology
Mumbai, India
hargobind.singh@spit.ac.in

Keshav Thosar
Electronics and Telecommunications
Sardar Patel Institute of Technology
Mumbai, India
keshav.thosar@spit.ac.in

***Abstract*—This paper elaborates on the details of our product that uses a combination of image steganography and cryptography to encrypt text messages (using a pre-shared key) and conceal them in an image file, for discreet movement of Information and/or to prevent and track forgery/leaking of intellectual property. The main aim of the product is to introduce a unique combination of image steganography and cryptography that complements each other and creates an extremely discreet message encoder. All the benefits of both steganography and cryptography are used to combat each other's disadvantages and make a highly effective product. The user's message is first in encoded using appropriate cryptographic methods by our product using the key that the user provides us, this key is then again used to encode the cryptographically encoded message into an image using steganography thereby providing a double protective encoding layering to the message. This image can then be transferred to the receiver, the receiver can extract the appropriate message from the image using our product provided the receiver has the appropriate decoding key. This combination of cryptography and steganography makes our product unique and extremely safe.**

Keywords—steganography, text encryption, cybersecurity, hyperchaotic systems

I. Introduction

The importance of cybersecurity and encryption has exponentially increased over the years. Technology has deep-rooted itself in our society. This often leaves us vulnerable to cyber-attacks causing financial damage, breach of trust and even identity. With the increasing computation power and amount of pre-existing breached data, it has become very easy for the hackers to gain unauthorized access upon locking on to a target. Regardless of you as an individual, a small business, or a major corporation, you rely on computer systems daily. When you combine this with the advent of cloud services, bad cloud service security, cell phones, and the Internet of Things (IoT), you have a slew of new security risks that were non-existent only a few decades ago. All of these challenges together provided the required incentive for our project, and inspired us to come up with something unique that makes the best use of the combination of cryptography and steganography to make a product that helps users encrypt text messages (using a pre-shared key) and conceal them in an image file, for discreet movement of Information and/or to prevent and track forgery/leaking of intellectual property. The product has been provided with an engaging and simplistic user-interface that makes its use extremely self-explanatory. The user's message is first in encoded using appropriate cryptographic methods by our product using the key that the user provides us, this key is then again used to encode the cryptographically encoded message into an image using steganography thereby providing a double protective encoding layering to the message. This image can then be transferred to the receiver, the receiver can extract the appropriate message from the image using our product provided the receiver has the appropriate decoding key. The product is explained and demonstrated in the paper further.

II. Literature Review

A. *Cryptography*

Cryptography is the study of secure communications techniques that allow only the sender and intended recipient of a message to view its contents [1].

B. *Various types of text encryption*

The Caesar Cipher is one the simplest encryption algorithm. "It is a type of substitution cipher in which each letter in the plaintext is replaced by a letter some fixed number of positions down the alphabet. The method is named after Julius Caesar, who used it in his private correspondence" [2]. XOR cipher is an additive cipher based on the binary XOR operation. This cipher has become a part various complex encryption algorithm [3]. [4] describes an encryption approach where Plaintext is XOR'ed with cover text based on an 8-bit random key.

C. *Steganography*

Steganography is a technique used for the hidden exchange of information. It is the art and science of hiding the information "in plain sight". In this way, if successfully achieved, the message does not attract attention from eavesdroppers and attackers. Using steganography, information can be hidden in different carriers such as images audio or video files or even text files. But for the course of our project, we'll only explore image steganography. Image steganography techniques exploits the imperfections of human perception. Some popular techniques are as mentioned. **Least Significant Bit** (LSB) Steganography is a technique that embeds the message in the last bits of pixels in the image. Since the LSB of the pixel has the least say in the intensity of colors in the picture, the resultant image is very similar to the original image. **Spread spectrum steganography** either deals with the cover image as noise or tries to add pseudo-noise to the cover image. Statistical methods have also been used in the past for steganography.

III. Methodology

We discovered that xor operation is robust for encryption as it reduces key deduction to brute-force. To enhance the security, we propose a two-step solution where the key is first manipulated using a hyperchaotic attractor and used to encrypt the plain text, followed by concealing the cipher text using

978-1-6654-1758-7/21/$31.00 ©2021 IEEE

image steganography techniques. The block diagram can be seen in Fig. 1.

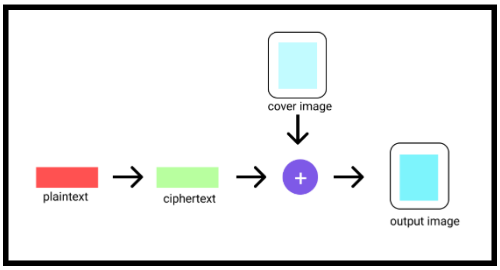


Fig. 1. General Cryptographic steps

IV. Experimental Setup

A. System Requirements

For this paper, we used Python as the programming language. The following libraries were installed:

a. numpy, for efficiently processing large integers and data blocks

b. fastapi, to create the frontend

All the dependencies were installed on Acer's Aspire 7 with 8GB RAM, 512 SSD, Nvidia GeForce GTX 1650 and Intel i5 9th gen processor.

B. Algorithm

After going through the previous works in the field, we came up with the following algorithm for text encryption.

Step 1. Get a 16-character long key (pad the string if the length is less) resulting to a 16-byte block

Step 2. Split the block into 4 C integers (size 4 bytes)

Step 3. Use the 4 integers as a seed value to a 4D hyperchaotic attractor and iterate over the attractor for desirable number (32 in our case). To prevent integer-overflow use the mod operator to reduce the integer.

Step 4. Convert the resulting integers to a 16-byte long cipher block.

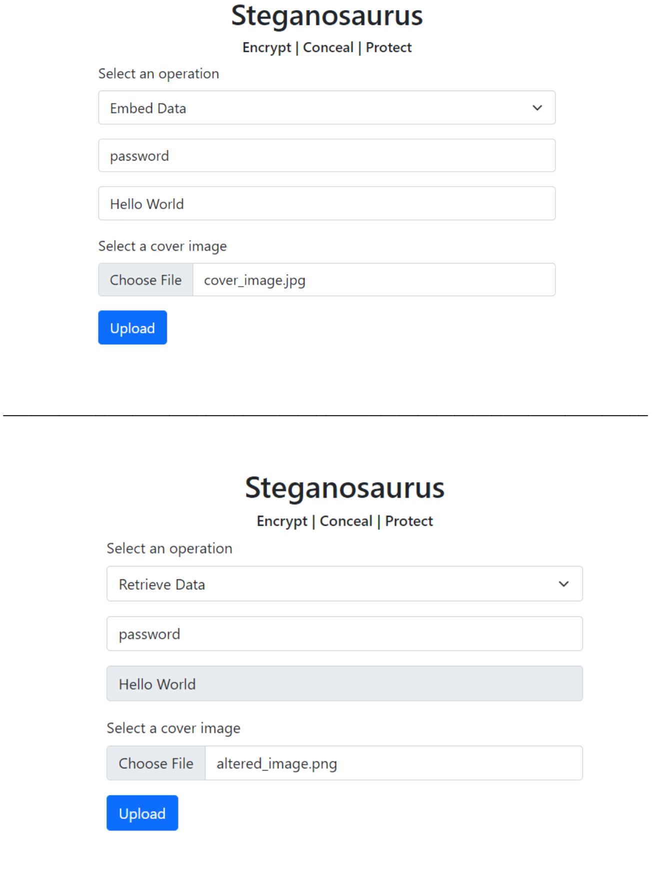
Step 5. Convert the plaintext into a byte array (pad the string if the length is not a multiple of 16)

Step 6. Take chunks of 16 bytes and xor them with the cipher block, resulting in an encrypted block.

Step 7. Convert all such blocks back to a byte array resulting in cipher text.

Step 8. Use a preferred steganography method (LSB in our case) to hide the cipher text

The decryption simply extracts the data from the image and using the key, derives the final cipher block which is xor' ed with the cipher text to get back the original text.



Steganosaurus

Encrypt | Conceal | Protect

Select an operation

Embed Data

password

Hello World

Select a cover image

Choose File cover_image.jpg

Upload

Steganosaurus

Encrypt | Conceal | Protect

Select an operation

Retrieve Data

password

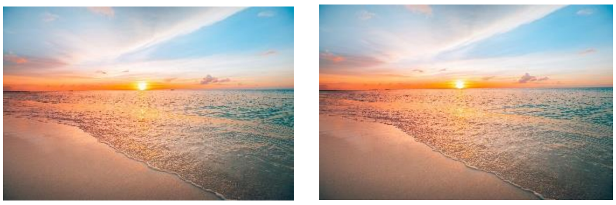
Hello World

Select a cover image

Choose File altered_image.png

Upload

Fig 2. User Interface of the Product



Cover Image

Altered Image

Fig. 3. Side to side comparison of LSB method

V. Result Analysis and Discussion

The product works as per expectations and all the assumptions about the reliability of the methods, algorithms and processes mentioned in the workflow of the product stands true. The 2 protective layers in the encryption process makes the project unique and novel. The choice of XOR cipher for encryption in conjunction with the least significant bit steganographic method turned out to be successful. All the secondary aspects of the program like inputting of data, security key, Images and their consequence retrieval is highly robust and efficient. Fig 2 shows the user interface of the product and Fig 3 shows a side-by-side comparison of the original and altered image. Upon analyzing the results, it is safe to say that the product delivers on its aim effectively. The most prominent constraint of our approach is that the message length should be strictly less than the number of pixels in the cover image.

VI. Conclusion

On careful observation of the results, process, and performance parameters we see that the product works satisfactorily, the encoding and decoding processes are highly efficient and robust. The user interface works smoothly and is extremely user friendly. The process of loading/downloading images and typing the security key to encode/decode messages is robust as well. The functionalities and purpose of the product is fulfilled satisfactorily. In the end we can say that the performance in fulfilling its aim is highly satisfactory and is highly reliable in its purpose.

Acknowledgement

We would like to extend our gratitude to Dr. Reena Sonkusre for her guidance without which this project could not have taken shape, her research in this area has been a source of motivation for us to work in this area. We would also like to thank our institute for providing us with such opportunities that help us learn and grow.

References

[1] "Cryptography Definition", www.kaspersky.com, 2021. [Online]. Available: https://www.kaspersky.com/resource-center/definitions/what-is-cryptography. [Accessed: 05- Oct- 2021]

[2] "Caesar cipher - Wikipedia", En.wikipedia.org, 2021. [Online]. Available: https://en.wikipedia.org/wiki/Caesar_cipher. [Accessed: 05- Oct- 2021]

[3] "XOR cipher - Wikipedia", En.wikipedia.org, 2021. [Online]. Available: https://en.wikipedia.org/wiki/XOR_cipher. [Accessed: 05- Oct- 2021]

[4] Sudan S. Kataria, T. Kumar, K. Singh and M. S. Nehra, "ECR (encryption with cover text and reordering) based text steganography," 2013 IEEE Second International Conference on Image Information Processing (ICIIP-2013), 2013, pp. 612-616, doi: 10.1109/ICIIP.2013.6707666.

[5] M. A. Khan, K. K. Mishra, N. Santhi and J. Jayakumari, "A new hybrid technique for data encryption," 2015 Global Conference on Communication Technologies (GCCT), 2015, pp. 925-929, doi: 10.1109/GCCT.2015.7342801.

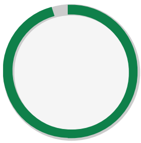
[6] Seddik, Hassen & Eddine, Maalaoui "A new hybrid encryption technique permuting text and image based on hyperchaotic system" 2016 63-68. 10.1109/ATSIP.2016.7523060.

[7] Hamid, Nagham & Yahya, Abid & Ahmad, R.Badlishah & Al-qershi, Osamah. "Image Steganography Techniques: An Overview" 2012 International Journal of Computer Science and Security. 6. 168-187.

Dupli Checker

PLAGIARISM SCAN REPORT

5%
Plagiarised



95%
Unique

Date	2021-12-03
Words	841
Characters	5558

Content Checked For Plagiarism

This paper elaborates on the details of our product that uses a combination of image steganography and cryptography to encrypt text messages (using a pre-shared key) and conceal them in an image file, for discreet movement of Information and/or to prevent and track forgery/leaking of intellectual property. The main aim of the product is to introduce a unique combination of image steganography and cryptography that complements each other and creates an extremely discreet message encoder. All the benefits of both steganography and cryptography are used to combat each other's disadvantages and make a highly effective product. The user's message is first in encoded using appropriate cryptographic methods by our product using the key that the user provides us, this key is then again used to encode the cryptographically encoded message into an image using steganography thereby providing a double protective encoding layering to the message. This image can then be transferred to the receiver, the receiver can extract the appropriate message from the image using our product provided the receiver has the appropriate decoding key. This combination of cryptography and steganography makes our product unique and extremely safe.

Keywords—steganography, text encryption, cybersecurity, hyperchaotic systems

I. INTRODUCTION

The importance of cybersecurity and encryption has exponentially increased over the years. Technology has deep-rooted itself in our society. This often leaves us vulnerable to cyber-attacks causing financial damage, breach of trust and even identity. With the increasing computation power and amount of pre-existing breached data, it has become very easy for the hackers to gain unauthorized access upon locking on to a target. Regardless of you as an individual, a small business, or a major corporation, you rely on computer systems on a daily basis. When you combine this with the advent of cloud services, bad cloud service security, cell phones, and the Internet of Things (IoT), you have a slew of new security risks that were non-existent only a few decades ago. All of these challenges together provided the required incentive for our project, and inspired us to come up with something unique that makes the best use of the combination of cryptography and steganography to make a product that helps users encrypt text messages (using a pre-shared key) and conceal them in an image file, for discreet movement of Information and/or to prevent and track forgery/leaking of intellectual property. The product has been provided with an engaging and simplistic user-interface that makes its use extremely self-explanatory. The user's message is first in encoded using appropriate cryptographic methods by our product using the key that the user provides us, this key is then again used to encode the cryptographically encoded message into an image using steganography thereby providing a double protective encoding layering to the message. This image can then be transferred to the receiver, the receiver can extract the appropriate message from the image using our product provided the receiver has the appropriate decoding key. The product is explained and demonstrated in the paper further.

II. LITERATURE REVIEW

A. Cryptography

Cryptography is the study of secure communications techniques that allow only the sender and intended recipient of a message to view its contents [1].

B. Various types of text encryption

The Caesar Cipher is one the simplest encryption algorithm. "It is a type of substitution cipher in which each letter in the plaintext is replaced by a letter some fixed number of positions down the alphabet. The method is named after Julius Caesar, who used it in his private correspondence" [2]. XOR cipher is an additive cipher based on the binary XOR operation.

This cipher has become a part various complex encryption algorithm [3]. [4] describes an encryption approach where Plaintext is XOR'ed with cover text based on an 8-bit random key.

C.	Steganography

Steganography is a technique used for the hidden exchange of information. It is the art and science of hiding the information "in plain sight". In this way, if successfully achieved, the message does not attract attention from eavesdroppers and attackers. Using steganography, information can be hidden in different carriers such as images audio or video files or even text files. But for the course of our project, we'll only explore image steganography. Image steganography techniques exploits the imperfections of human perception. Some popular techniques are as mentioned.

Least Significant Bit (LSB) Steganography is a technique that embeds the message in the last bits of pixels in the image.

Since the LSB of the pixel has the least say in the intensity of colors in the picture, the resultant image is very similar to the original image.

Spread spectrum steganography either deals with the cover image as noise or tries to add pseudo-noise to the cover image.

Statistical methods have also been used in the past for steganography.

III.	METHODOLOGY

We discovered that xor operation is robust for encryption as it reduces key deduction to brute-force. To enhance the security, we propose a two-step solution where the key is first manipulated using a hyperchaotic attractor and used to encrypt the plain text, followed by concealing the cipher text using

Matched Source

Similarity 3%

Title:A Novel Magic LSB Substitution Method (M-LSB-SM) using ...

بواسطة K Muhammad · 2015 · تم اقتباسها في عدد: 170 — Figure 2: Degradation in the quality of Lena stego image by hiding data in different image planes. LSB-M slightly modifies the image pixels by adding ± 1 ...

https://arxiv.org/pdf/1506.02100

Similarity 3%

Title:(PDF) Methodology of Spread-Spectrum Image Steganography

... Distortion Steganography [37] deals with either cover image as a noise or tries to add pseudo random noise to the cover image. It transmits the data for the ...

https://www.researchgate.net/publication/277983772_Methodology_of_Spread-Spectrum_Image_Steganography