ElGamal Encryption with Image Steganography

A PROJECT REPORT

Submitted by

BL.EN.U4CSE17010	Aravind V. Nair
BL.EN.U4CSE17048	Isha Saikumar
BL.EN.U4CSE17091	Nirmal Sharon Joji
BL.EN.U4CSE17107	Rakshana J

in partial fulfillment for the award of the degree

of

BACHELOR OF TECHNOLOGY

IN

COMPUTER SCIENCE , ENGINEERING

AMRITA SCHOOL OF ENGINEERING, BANGALORE

AMRITA VISHWA VIDYAPEETHAM

BANGALORE 560 035

November-2020

Table of Contents

1. Abstract

In today's world almost all digital services like internet communication, medical and military imaging systems, multimedia systems need a high level of security. There is a need for security level in order to safely store and transmit digital images containing critical information. This is because of the faster growth of multimedia technology, internet and cell phones. Therefore there is a need for image encryption techniques in order to hide images from such attacks

ElGamal Cryptosystem is an algorithm used by modern computers to encrypt and decrypt messages. It is an asymmetric cryptographic algorithm. Asymmetric means that there are two different keys. This is also called public-key cryptography because one of the keys can be given to anyone.

The ElGamal algorithm modified suitable for RGB image encryption. Experimental results show that the proposed approach can successfully encrypt/decrypt various images, and the algorithm has a good encryption effect. Cipher image developed by this method will be entirely different when compared to the original image. This approach provides better security and it will be suitable for the secure transmission of images over the Internet.

2. Introduction

2.1 ElGamal

ElGamal encryption is a public-key cryptosystem. It uses asymmetric key encryption for communicating between two parties and encrypting the message. This cryptosystem is based on the difficulty of finding discrete logarithm in a cyclic group that is even if we know g^a and g^k, it is extremely difficult to compute g^ak.

Suppose Alice wants to communicate to Bob.

Bob generates public and private key :

- Bob chooses a very large number q and a cyclic group Fq.
- From the cyclic group Fq, he choose any element g and an element such that gcd(a, q) = 1.
- Then he computes h = g^a.
- Bob publishes F, h = g^a, q and g as his public key and retains a private key.

2.1.1 ElGamal Encryption

Alice encrypts data using Bob's public key :

- Alice selects an element k from cyclic group F such that gcd(k, q) = 1.
- Then she computes p = gk and s = hk = gak.
- She multiples s with M.
- Then she sends (p, M*s) = (gk, M*s).

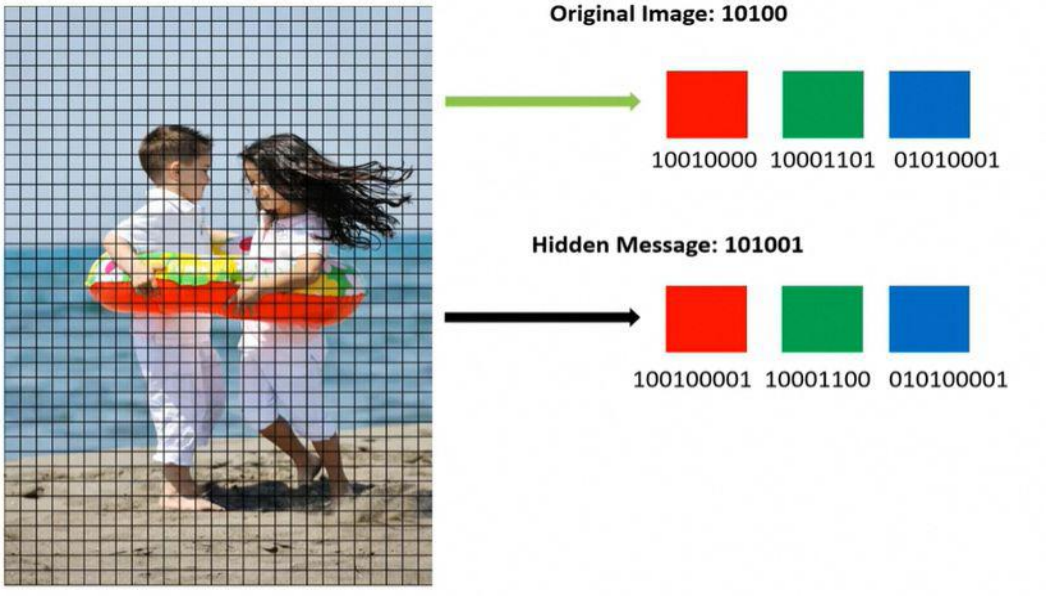
2.1.2 ElGamal Decryption

Bob decrypts the message :

- Bob calculates $s' = p_a = g_{ak}$.
- He divides M*s by s' to obtain M as $s = s'$.

2.2 Steganography

Steganography is the method of hiding secret data in any image/audio/video. In a nutshell, the main motive of steganography is to hide the intended information within any image/audio/video that doesn't appear to be secret just by looking at it. The idea behind image-based Steganography is very simple. Images are composed of digital data (pixels), which describes what's inside the picture, usually the colors of all the pixels. Since we know every image is made up of pixels and every pixel contains 3-values (red, green, blue).



2.2.1 Steganography Encryption

Every byte of data is converted to its 8-bit binary code using ASCII values. Now pixels are read from left to right in a group of 3 containing a total of 9 values. The first 8-values are used to store binary data. The value is made odd if 1 occurs and even if 0 occurs.

For example:

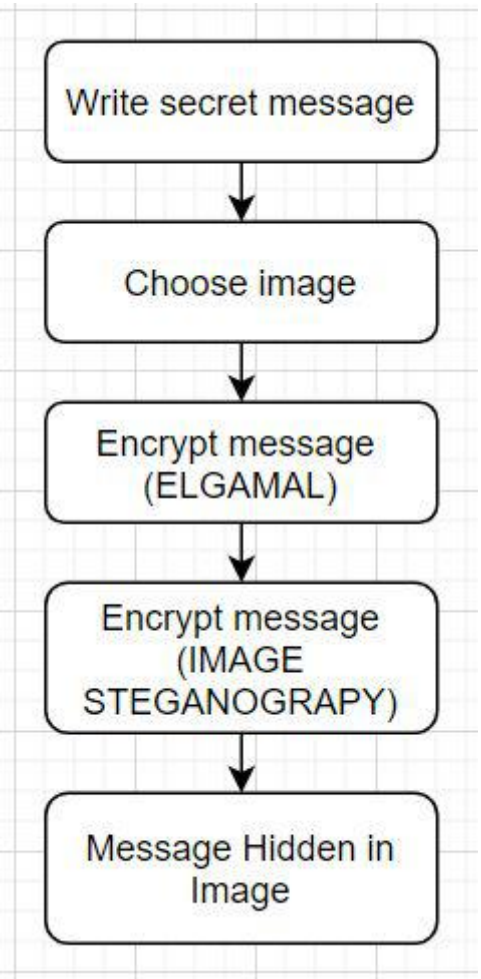
Suppose the message to be hidden is ' **Hii** '. Since the message is of 3-bytes, therefore, pixels required to encode the data is 3 x 3 = 9. Consider a 4 x 3 image with a total 12-pixels, which are sufficient to encode the given data.

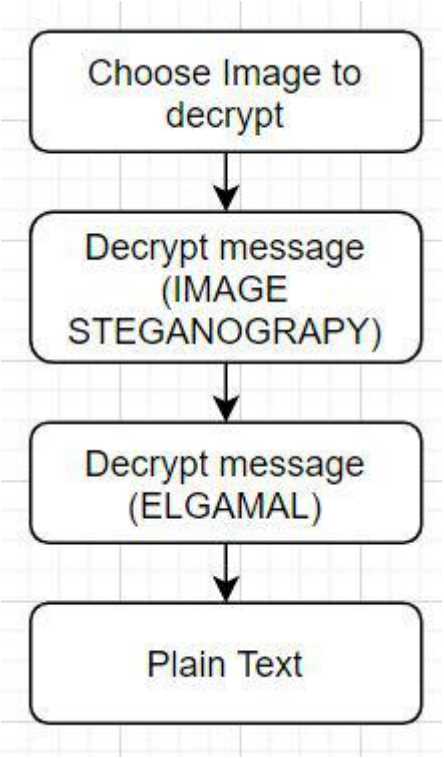
2.2.2 Steganography Decryption

To decode, three pixels are read at a time, till the last value is odd, which means the message is over. Every 3-pixels contain binary data, which can be extracted by the same encoding logic. If the value is odd the binary bit is 1 else 0.

3. Working Details

The user will enter his/her secret message into the text box and choose an image into which the message has to be encrypted. The message is first encrypted using ElGamal cryptosystem after which the encrypted message is further encrypting the message with steganography. The resulting image is finally saved. The output image can later be decoded and the decrypted message can be retrieved by selecting the image. First steganography decryption is carried out, after which ElGamal decryption is done





4. Proof of Work

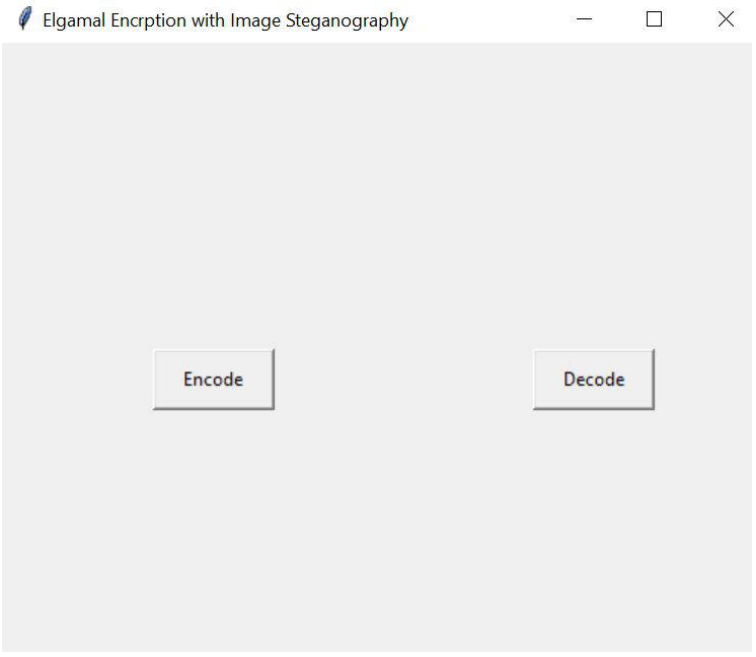


Fig 4.1 UI for landing screen

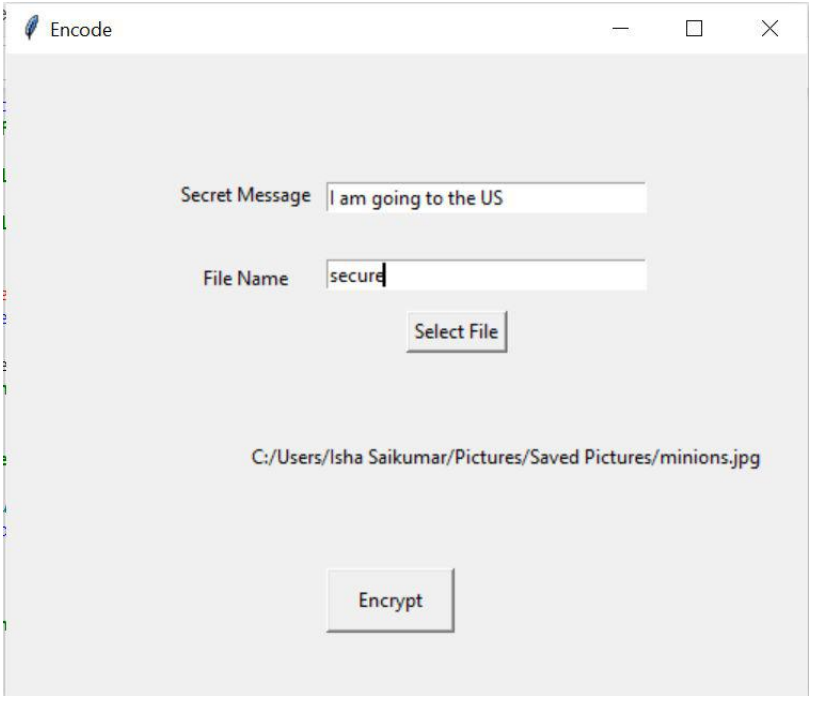


Fig 4.2 UI for user input

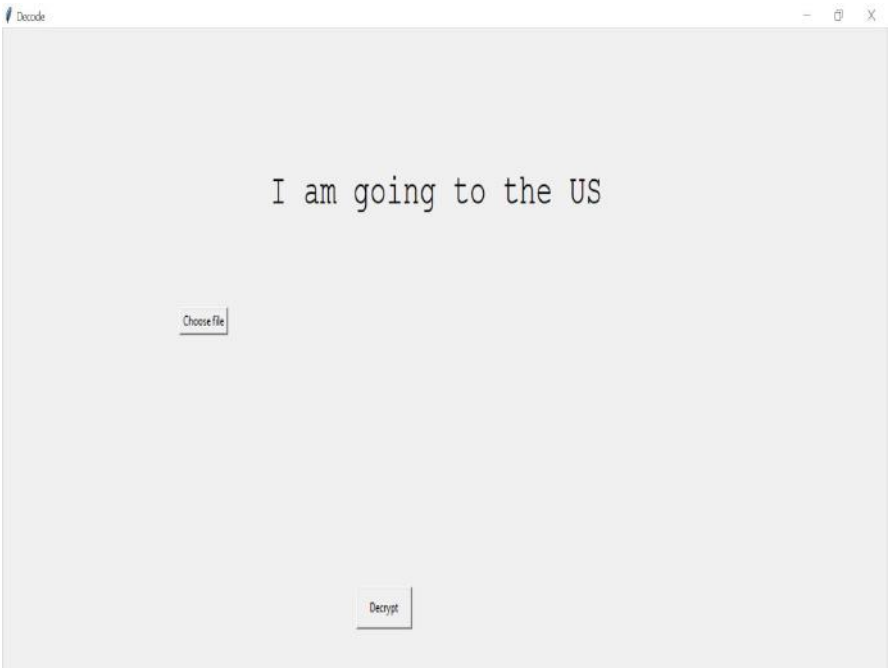


Fig 4.3 Final decrypted message

Fig 4.4 Image not distorted after encrypting message

5. References

- Image based Steganography using Python
- Steganography: The Art & Science of Hiding Things in Other Things - Part 1
- Section 16.3 ElGamal Encryption System
- Public Key Encryption