# Commercial Data Steganography Systems Using Public-Key Cryptography

Sudasawan Ngammongkolwong [1], Suwilai Phumpho [2]

[1] Master of Science, Faculty of Science and Technology
Southeast Bangkok College
Bangkok, Thailand
e-mail: sudasawan@southeast.ac.th
[2] Master of Science, Faculty of Science and Technology
Southeast Bangkok College
Bangkok, Thailand
suwilai@gmail.com

***Abstract*—Involving the application of public-key cryptography have the objective to camouflage commercial data because piracy is happening all over the world at present. RSA is an asymmetric key encryption algorithm using modular arithmetic. Public-key cryptography is popular in electronic transactions. The authors prioritize piracy and develop a steganography system using commercial image processing technology to prevent piracy. The program will camouflage texts in images and apply RSA to encode images to prevent piracy. The program will encode and decode for security. From the efficiency test of the steganography system using commercial image processing technology, users can camouflage data comfortably, easily, quickly, and efficiently. This is suitable for ordinary users who want to use the program to camouflage commercial data. One suggestion is that the system can include different encoding techniques such as AES, DES, and Chaos Key.**

***Keywords-component; camouflage, image decode, security, public-key cryptography***

## I. INTRODUCTION

The main components of communications are sender, receiver, channel, and message. They all affect the success of communications. Communications may fail because of unclear language by senders. An attempt to solve problems creates an evaluation of communication by applying technology such as an attempt to use a computer to translate, use of a telephone to receive audio signals, and use of fax to receive image data. Data security is also important. Due to internet communication which is very popular, there are four issues that users should consider which are: 1) confidentiality or the prevention of disclosure of data to unauthorized persons; 2) data integrity or the ability to check whether data are correct, complete, and not edited; 3) authentication or identification of senders, and 4) non-repudiation or the ability to prevent senders from denying that they have sent electronic data [1]

At present, data are very important, especially confidential data. Confidential data are usually accessed in different ways which can cause leaks. Camouflage is to conceal and prevent people from seeing data, and can be done in different ways such as hiding data in images, audio, or video. Data security is important in the present to protect data and is applied in agencies whose data are sensitive. In the present, data security is used to prevent data access in many ways. Therefore, we design and develop a program prototype. We choose to use image processing for camouflage and RSA which is a key-encoding approach using modular arithmetic based on an integer. However, the integer in the system will reverse in the same way as the clock hands when values reach defined values. These values are the modulus. In other words, values that exceed the modulus will be changed to fractions of those values divided by the modulus to test data encryption in images and decode. [2]

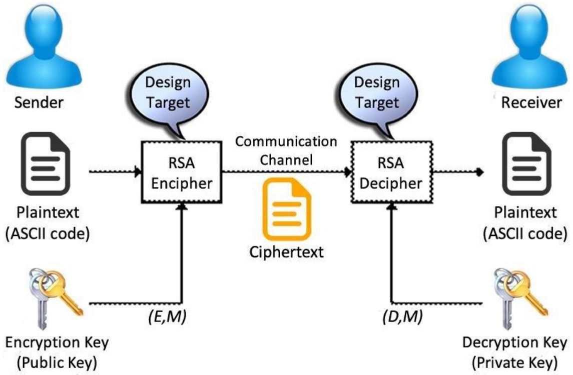


Figure 1. RSA algorithm structure [2]

Public Key is a key that is compatible with Private key asymmetric cryptography. The decryption method requires two keys for entry and decryption, one is Private Key and the other is Public Key. Having two keys allows public key cryptography. Compare secret key cryptography where the recipient and sender use different keys. There is no need to know each other's secrets to be able to send information to each other safely. The public key of the software developer is stored in the application or operating system, and the software update is only performed if the digital signature on the update is verified for that public key. Signature schemes also provide message integrity, message authentication, and non-repudiation. Other important applications of public key cryptography are key exchange and key transport for secure communication [3].

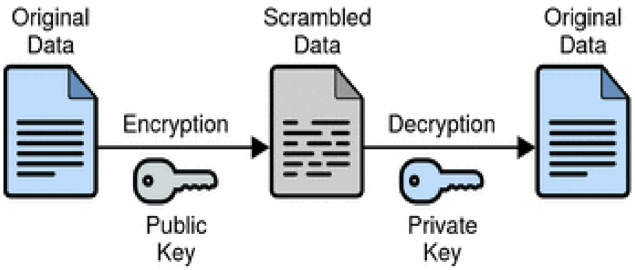


Figure 2. Public-Key Encryption [4]

1.To develop a prototype of a commercial steganography system using public-key cryptography

## II. Methodology

The authors did the literature review and reviewed programs used for camouflage. The program applies RSA to encode images. RSA is the approach for public-key encryption which is the first approach known as a suitable method for digital signatures and encoding. It is a big step to encode as public-key encryption.[5] RSA uses a protocol for electronic commerce and it is believed that it is secure when the keys are long enough. We use two keys to encode images.

1.Flow chart of camouflage using public-key cryptography

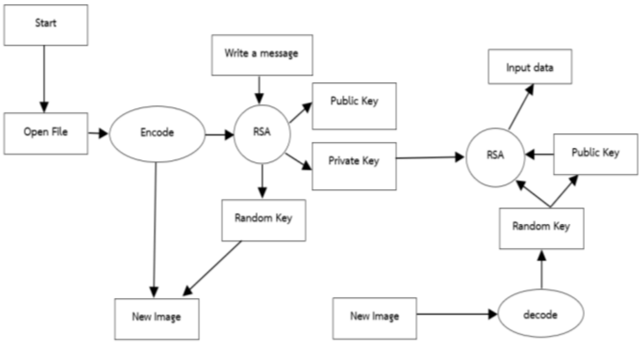


Figure 3. Flow chart of camouflage using image processing technology

2. Steganography system design screen

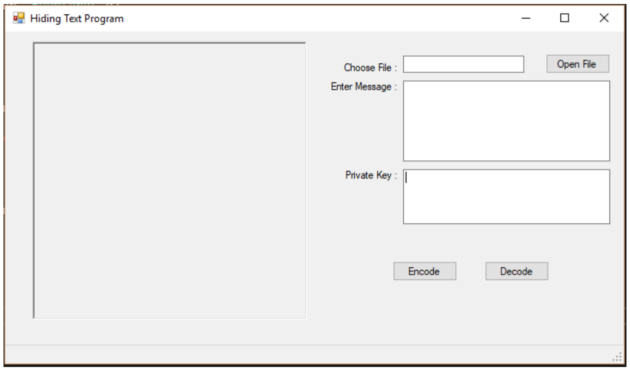


Figure 4. Steganography system design screen

3. System workflow

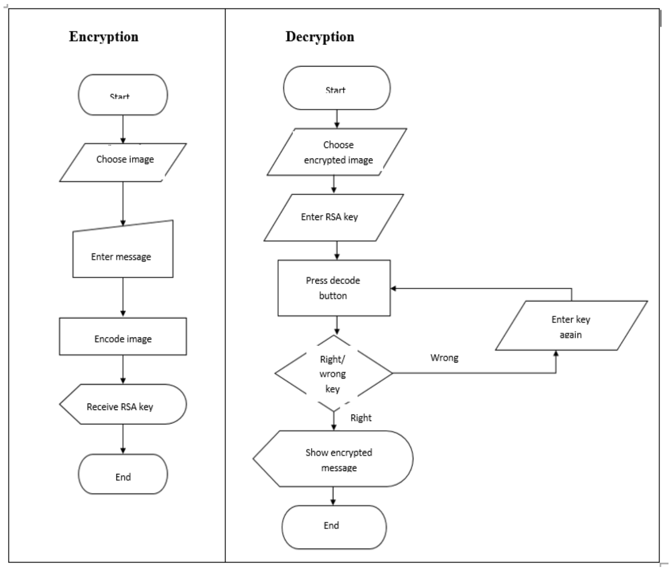


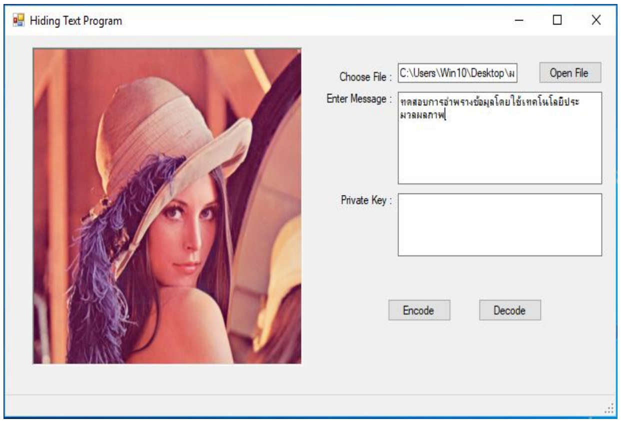
Figure 5. Encryption and Decryption

## III. RESULTS

For the completion of camouflage, the authors test an image and encode data. Keys are entered correctly and incorrectly to demonstrate the result screen. The authors use histograms to verify the differences between two images for which camouflage is done.

## IV. IMAGE ENCODING

1. Choose an image and enter a message.
2. Press the Encode button to encode the image and save a new image.
3. Copy Private Key

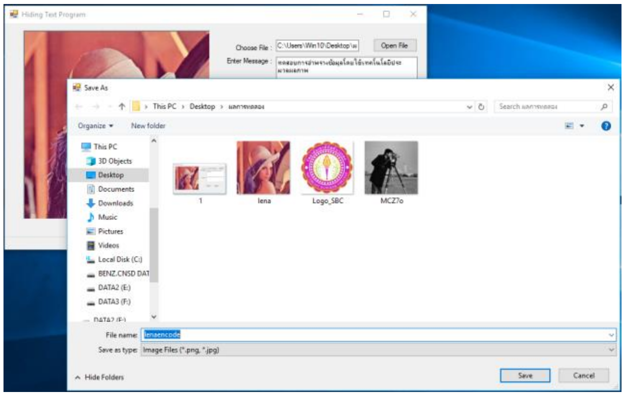


Choose File : C:\Users\Win10\Desktop\ผ

Enter Message : ทดสอบการอำพรางข้อมูลโดยใช้เทคโนโลยีประมวลผลภาพ

Private Key :

Figure 6. Choose an image and enter a message



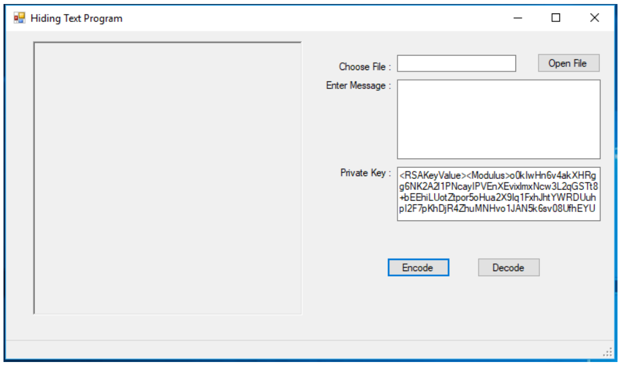
Choose File : C:\Users\Win10\Desktop\ผ

Enter Message : ทดสอบการอำพรางข้อมูลโดยใช้เทคโนโลยีประมวลผลภาพ

File name: lenaencode

Save as type: Image Files (*.png, *.jpg)

Figure 7. Press the Encode button to encode the image and save a new image



Choose File :

Enter Message :

Private Key : <RSAKeyValue><Modulus>o0kIwHn6v4akXHRgg6NK2A2l1PNcayIPVEnXEvixlmxNcw3L2qGSTt8+bEEhiLUotZtpor5oHua2X9lq1FxhJhtYWRDUuhpI2F7pKhDjR4ZhuMNHvo1JAN5k6sv08UfhEYU

Figure 8. Copy Private Key

What is needed to be sent to receivers are:

- Private Key
- Encoded image

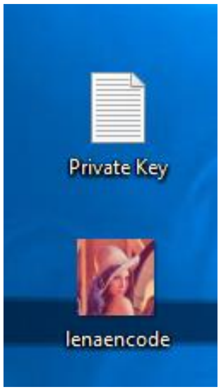


Figure 9. Files that need to be sent to receivers

## V. IMAGE DECODING

- Choose image
- Enter Private Key and press the Decode button
  If successful Message will show
  If not successful A text box shows "Decoding is not complete, please try again".

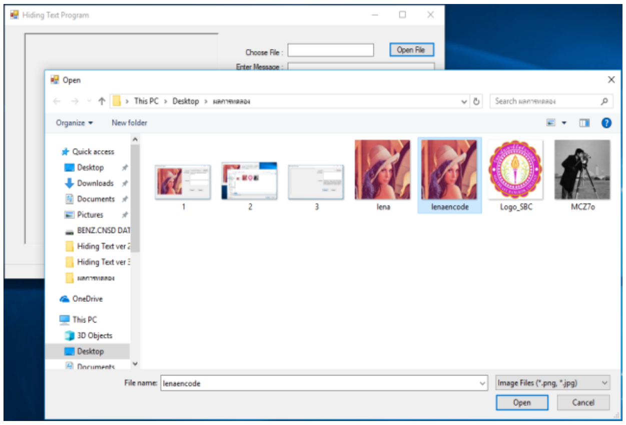
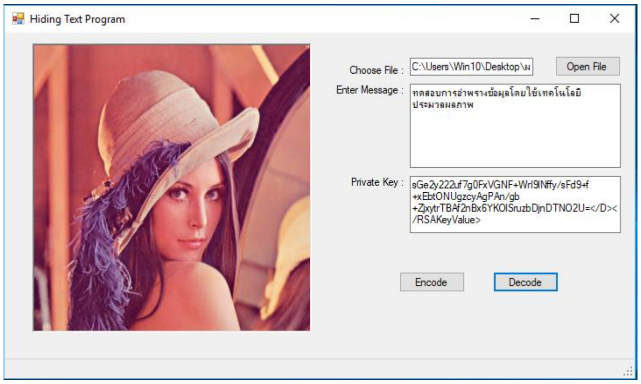


Figure 10. Choose image

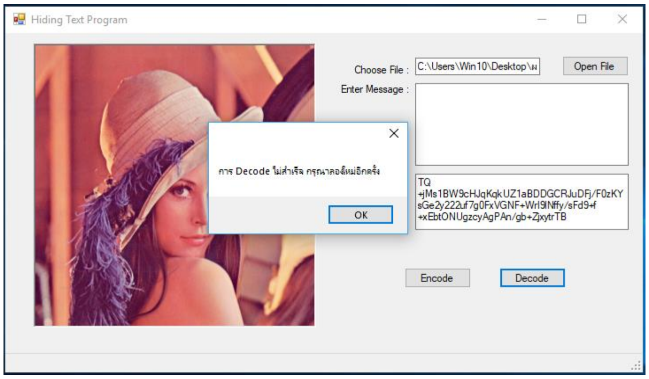


Choose File : C:\Users\Win10\Desktop\ผ

Enter Message : ทดสอบการอ่าพรางข้อมูลโดยใช้เทคโนโลยี
ประมวลผลภาพ

Private Key : sGe2y222uf7g0FxVGNF+Wrl9INffy/sFd9+f
+xEbtONUgzcyAgPAn/gb
+ZjxytrTBAf2nBx6YKOISruzbDjnDTNO2U=</D><
/RSAKeyValue>

Figure 11. Enter Private Key and press the Decode button, the message will show if successful



Choose File : C:\Users\Win10\Desktop\ผ

Enter Message :

การ Decode ไม่สำเร็จ กรุณาลองใหม่อีกครั้ง

TQ
+jMs1BW9cHJqKqkUZ1aBDDGCRJuDFj/F0zKY
sGe2y222uf7g0FxVGNF+Wrl9INffy/sFd9+f
+xEbtONUgzcyAgPAn/gb+ZjxytrTB

Figure 12. Enter Private Key and press the Decode button, a text box will show

“Decoding is not complete, please try again” if not successful Histograms showing two images with different sizes when the same message is added 128x128 pixel images

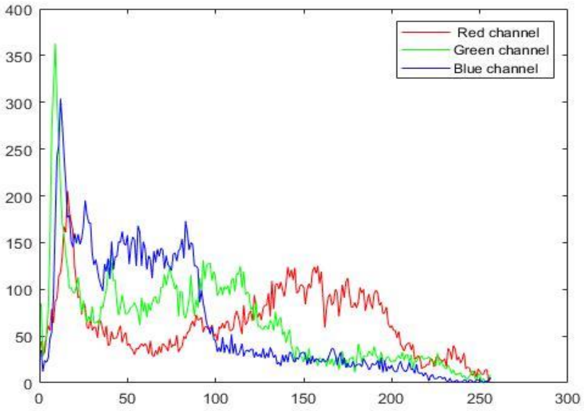


Figure 13. Histogram of the original image

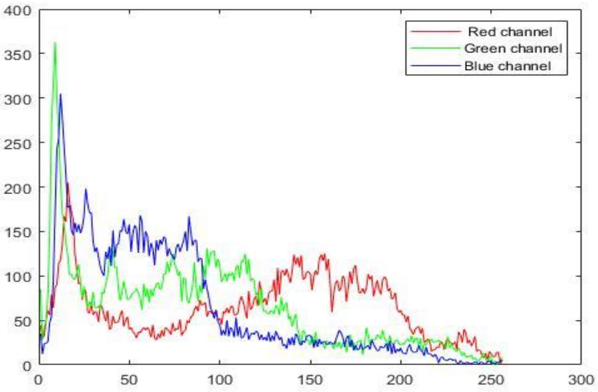


Figure 14. Histogram of the encoded image

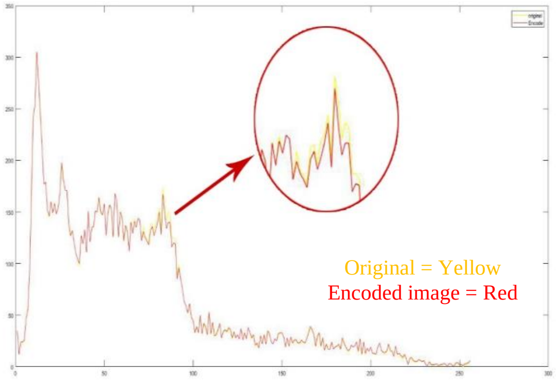


Figure 15. Difference of blue in both images 256 x 256 pixel images

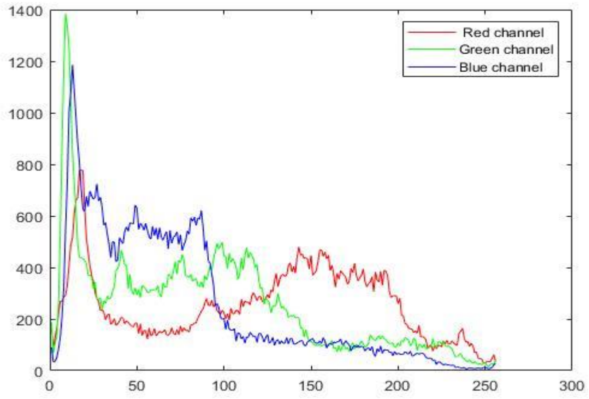


Figure 16. Histogram of the original image

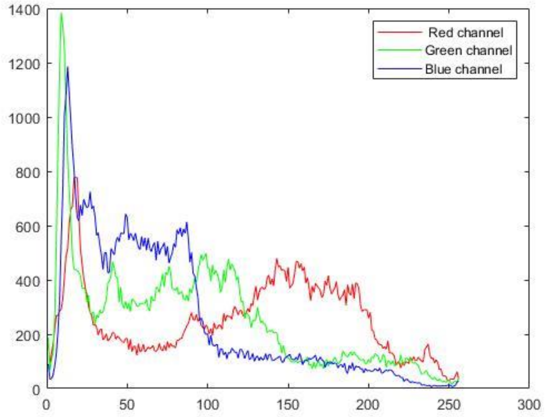
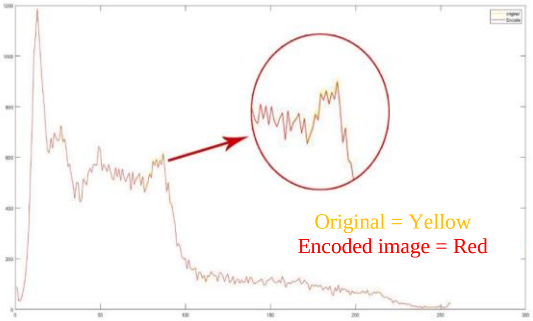


Figure 17. Histogram of the encoded image



Original = Yellow
Encoded image = Red

Figure 18. Difference of blue in both images 512x512 pixel images

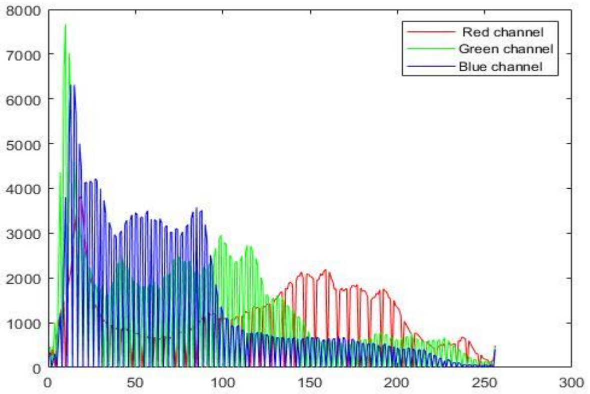


Figure 19. Histogram of the original image

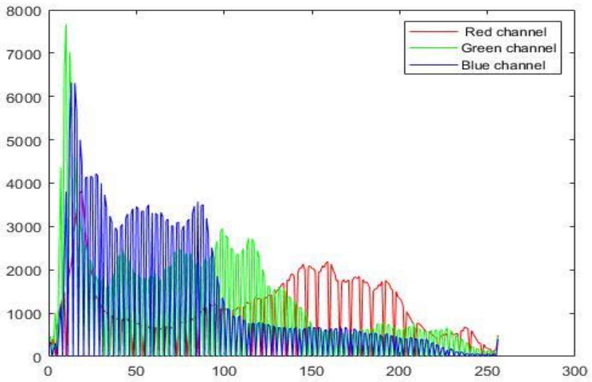
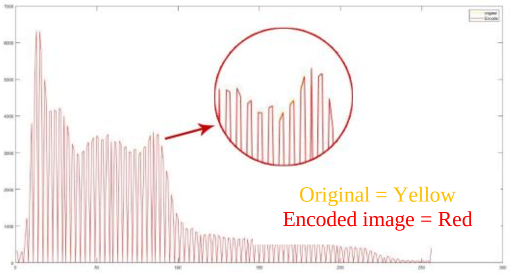


Figure 20. Histogram of the encoded image



Original = Yellow
Encoded image = Red

Figure 21. Difference of blue in both images

It can be seen that the differences are in the blue channel. Camouflage uses the concept of converting the message to bytes and replacing the new value in the blue channel. Then, a new image is saved. The new image will have a different color channel and camouflage is difficult to detect.

From the literature review about the steganography system using image processing technology and tests to find mistakes, many problems are found. The authors then solve them. After that, the system can work according to the objective and target. Users can use it with ease, comfort, speed, and efficiency which is suitable for ordinary users who want to use camouflage.

## SUGGESTIONS

1) Develop the program for more detail to make it more secure using the Least Significant Bit Algorithm for Image Steganography (LSB)
2) Develop the program to be able to encode audio in images
3) Apply different keys such as AES, DES, and Chaos Key

## REFERENCES

[1] ETDA Recommendation on ICT Standard for Electronic Transactions. Electronic Transactions Development Agency, Ministry of Digital Economy and Society,2017.

[2] Hüseyin Bodur, Resul Kara, "Secure SMS Encryption Using RSA Encryption Algorithm on Android Message Application",3RD International Symposium on Innovative Technologies in Engineering and ScienceAt : Valencia, June 2015.

[3] Steven D Galbraith, "Mathematics of Public Key Cryptography Version 2.0",October 31, 2018." [Online].Available:https://www.math.auckland.ac.nz/~sgal018/crypto-book/main.pdf. [Accessed: Sep. 7, 2020].

[4] Public-KeyEncryption.2010, Oracle Corporation and/oritsaffiliates.[Online].Available:https://docs.oracle.com/cd/E19656-01/821-1507/aakfv/index.html. [Accessed: July.10, 2020].

[5] G.-H. Chiou and W.-T. Chen, "Secure broadcasting using the secure lock." IEEE Transactions on Engineering, Vol.15, No. 8, pp. 929-934, 1989