Steganography encrypting and decrypting

Li-Wei Yang, supervisor: Ta-Te Lin

ABSTRACT

Image steganography has been used in many area. In this paper, we propose a well-organized steganography application to do various method of steganography. The encrypting part of the application would include LSB steganography, DCT steganography, DFT steganography and DWT steganography; the hidden message would be encrypted with an AES key in 16 char as well as an IV (initial vector) for block cypher. The decrypting part of the application would include not only the decryption part with key and IV, but also some of the famous strategy used to detect steganography, such as histogram examination, image subtraction.

Keywords: Image Steganography, Stego file, AES128, Block cypher, Cryptology, references

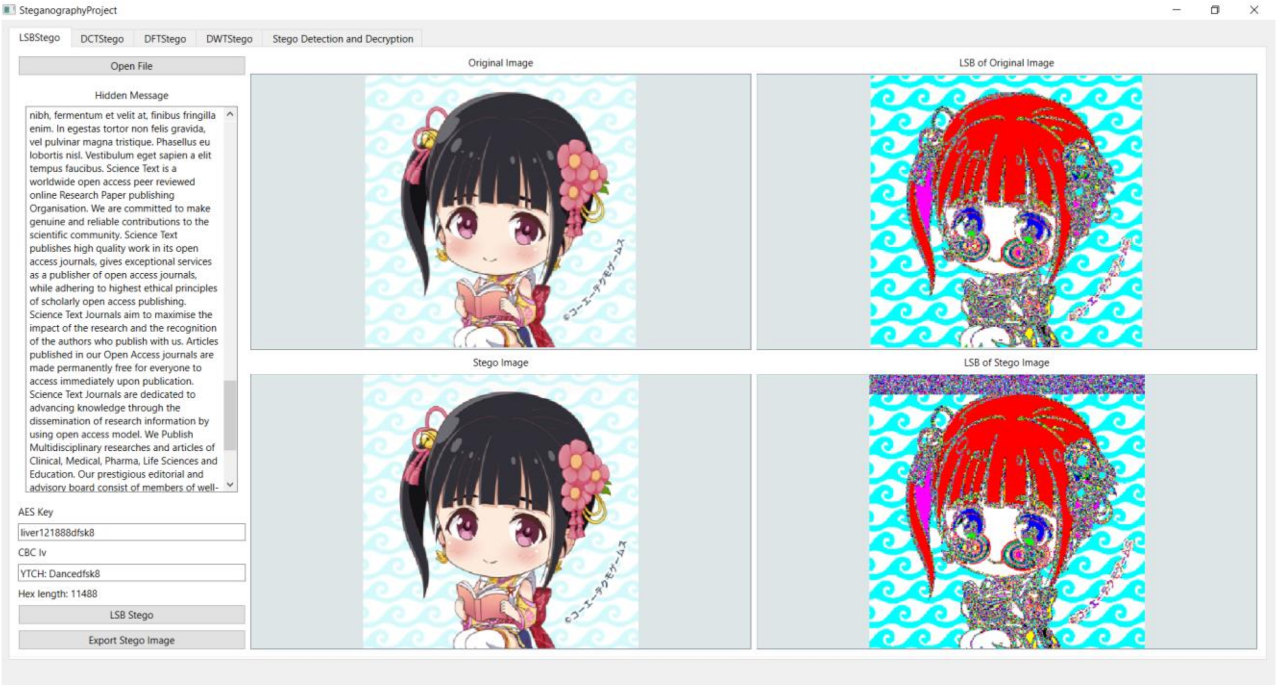
1. INTRODUCTION

In this section, I would explain the limitation of current other study and why this paper matters.

2. METHODS

2.1 User interface

The user interface is quite straightforward: the user can use tab to switch between different steganography methods, and for the last part the user can examine a stego image or decrypt it. For the LSB stego part, the LSB plan of the original image and the stego image are extracted to show that the method works. The user can export the stego image in PNG format and send the image to others. The stego image looks the same as the original image in human eyes.



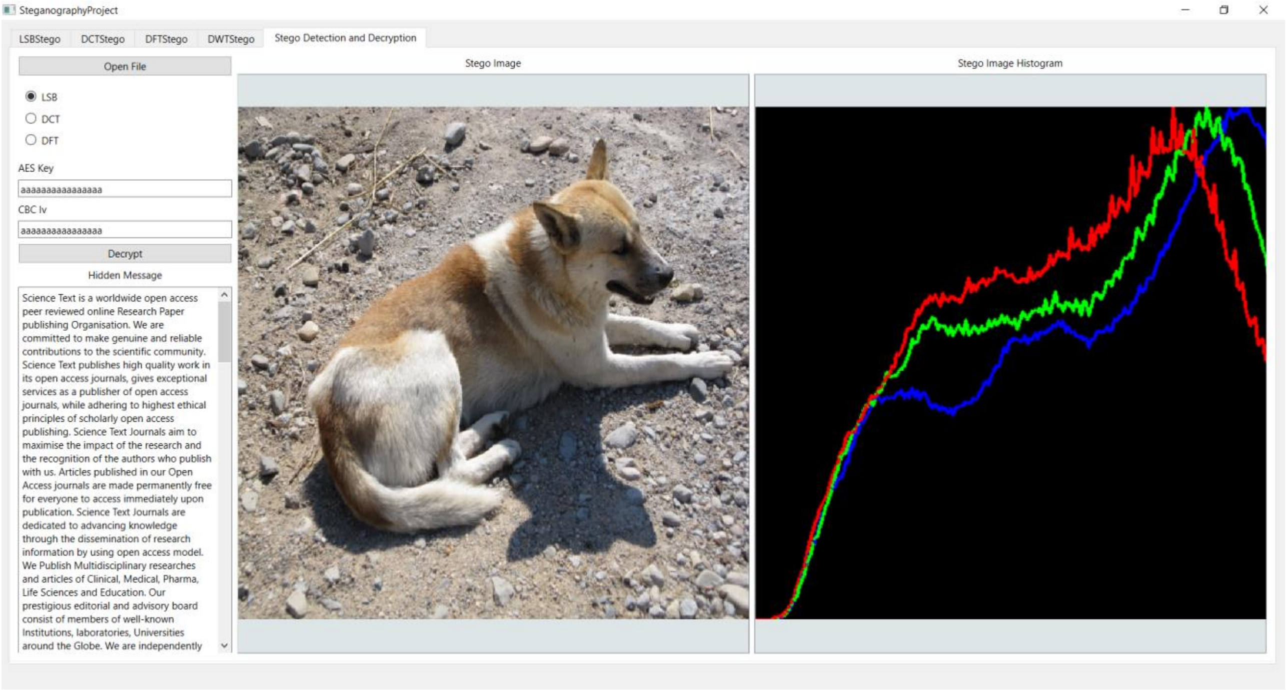
nibh, fermentum et velit at, finibus fringilla enim. In egestas tortor non felis gravida, vel pulvinar magna tristique. Phasellus eu lobortis nisl. Vestibulum eget sapien a elit tempus faucibus. Science Text is a worldwide open access peer reviewed online Research Paper publishing Organisation. We are committed to make genuine and reliable contributions to the scientific community. Science Text publishes high quality work in its open access journals, gives exceptional services as a publisher of open access journals, while adhering to highest ethical principles of scholarly open access publishing. Science Text Journals aim to maximise the impact of the research and the recognition of the authors who publish with us. Articles published in our Open Access journals are made permanently free for everyone to access immediately upon publication. Science Text Journals are dedicated to advancing knowledge through the dissemination of research information by using open access model. We Publish Multidisciplinary researches and articles of Clinical, Medical, Pharma, Life Sciences and Education. Our prestigious editorial and advisory board consist of members of well-

AES Key: liver121888dfsk8

CBC Iv: YTCH: Dancedfsk8

Hex length: 11488

For detection and decryption part, the user can choose the corresponding decrypting method to decrypt the hidden message, using the same key and IV as before. The user can see the histogram of the image to find anomaly.



● LSB
○ DCT
○ DFT

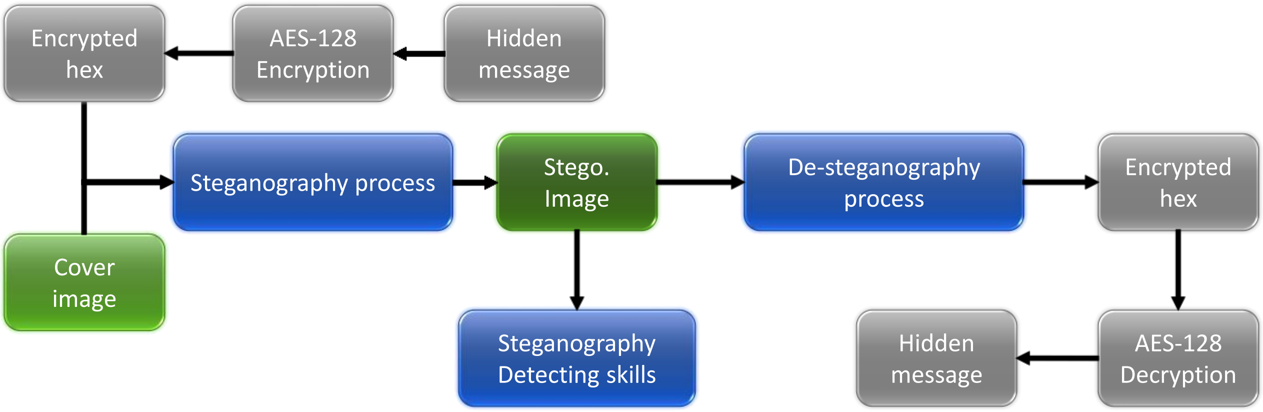
AES Key: aaaaaaaaaaaaaaaa

CBC Iv: aaaaaaaaaaaaaaaa

Hidden Message

Science Text is a worldwide open access peer reviewed online Research Paper publishing Organisation. We are committed to make genuine and reliable contributions to the scientific community. Science Text publishes high quality work in its open access journals, gives exceptional services as a publisher of open access journals, while adhering to highest ethical principles of scholarly open access publishing. Science Text Journals aim to maximise the impact of the research and the recognition of the authors who publish with us. Articles published in our Open Access journals are made permanently free for everyone to access immediately upon publication. Science Text Journals are dedicated to advancing knowledge through the dissemination of research information by using open access model. We Publish Multidisciplinary researches and articles of Clinical, Medical, Pharma, Life Sciences and Education. Our prestigious editorial and advisory board consist of members of well-known Institutions, laboratories, Universities around the Globe. We are independently

2.2 Application block disagram



The hidden message is first turn into hex, then embedded into the image. The stego image can later be decrypted to obtain the hidden message, or be examined by various steganography detecting techniques.

2.3 Encryption method

The encryption of the plain text is using AES-128, that is, encryption with a 16 bytes key and initial vector. The encryption implementation we used is Crypto++ library. AES-128 is a highly secure encryption method, the purpose of the encryption is to prevent others to find the plain text easily—even if they know how the embedded process of the steganography is, and extracted the hex, they cannot decrypt it to know what the hidden message is.

The detail of encryption is not the focus of this paper, but the AES encryption does permutation, XOR manipulation so the data is encrypted thoroughly.

2.4 LSB Steganography method

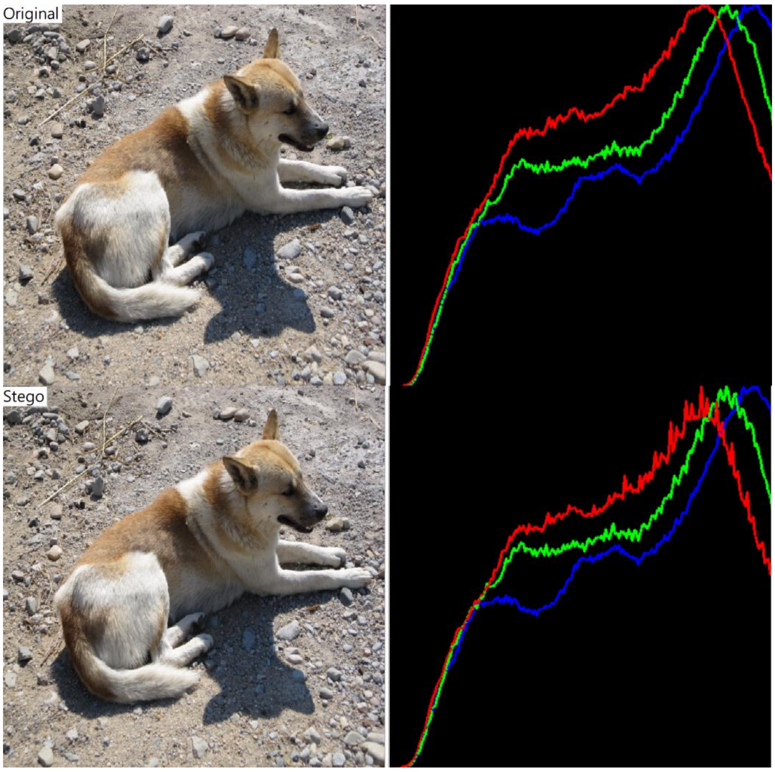
The Hidden message would first go through the encryption above to get a hex. The length of the hex would be shown in the UI, the length should never exceed the pixel number in the cover image. The hex is then turned into ASCII code, and the 7 bits code is separate to (3, 2, 2) bits. These bits would then be embedded into the LSB of the cover image in the order of (B, G, R), so the blue plane would experience a larger difference. After all the message is embedded, we add the ETX (ASCII code: 3) to notify the reader here is the End-of-Text, stop decrypting. The decrypting process is the revesre—we first extract the LSB of the stego image and turn them into hex, stop decrypting when decrypts out a ETX. The hex would be decrypted using the secret key and the IV exchanged privately by the sender and the receiver (here, we just copy-and-paste it from different tab), then the hidden message can be obtained.

2.5 DCT Steganography method

DCT Steganography method is robust when it comes to jpg format. Jpg format compress the image using DCT, so the message stored in the LSB would distorted. DCT Steganography embedded hidden message in DCT coefficients so the jpg compression process cannot destroy the hidden message. In the application, after we get the hex, we first DCT the cover image, and embed the hex in the SE corner of the DCT coefficients. Because most of the energy of the image is concentrated at the NW corner of the DCT coefficients, the embedded hex would not cause the image to change a lot. Then, we IDCT the DCT coefficients to get the stego image. The decryption of the message is the reverse process of the encryption.

2.6 Steganography detection method

The LSB Steganography is pretty easy to detect once we got the original image—we only have to subtract two images then we can tell the image is different and may be embedded with message. As a result, never use online photo as cover image or do not leak the original image out. The histogram of the image may also infer that the image is stego image. The figure below compares the histograms of original image and the stego image. Stego image has a lot of discrete jump in histogram, especially in R plane (because the plan store the 2 LSB of hidden message, and it basically change when the parity of the number change), this is the proof of LSB stego.



3. FUTURE WORKS

When working on DCT steganography, the DCT and IDCT are not fully reversible, so the embedded data would be lost. The DFT and DWT are likely to meet the same problem. I would try my best to address this issue, hope I can finish the project in time. The detection part of image subtraction would be realize shortly.

REFERENCE LINKING

Websites:

[1] “AES Explained (Advanced Encryption Standard) - Computerphile”
https://youtu.be/O4xNJsjtN6E (22 November 2019).

[2] “Almost All Web Encryption Works Like This (SP Networks) – Computerphile”
https://youtu.be/DLjzI5dX8jc (14 August 2019).

[3] “Secrets Hidden in Images (Steganography) - Computerphile”
https://youtu.be/TWEXCYQKyDc (4 May 2015).

REFERENCES

[1] Lin Y-K. A data hiding scheme based upon DCT coefficient modification. Computer Standards & Interfaces. 2014;36.

[2] Channalli S, Jadhav A. Steganography An Art of Hiding Data. arXiv pre-print server. 2009.

[3] Mazumder JA, Hemachandran K. Study of Image steganography using LSB, DFT and DWT. INTERNATIONAL JOURNAL OF COMPUTERS & TECHNOLOGY. 2013;11(5):2618-27.

[4] Baby D, Thomas J, Augustine G, George E, Michael NR. A Novel DWT Based Image Securing Method Using Steganography. Procedia Computer Science. 2015;46:612-8.

[5] Chaitanya C, Reddy CN, Vignesh KS, Krishna PR, Roshini A, Swetha K, editors. Enhanced Hash Based Image Steganography Technique to Increase Data Integrity and Confidentiality2021: IEEE.