Steganography

Efe ÇİFTCİ
May 2011

What is ...

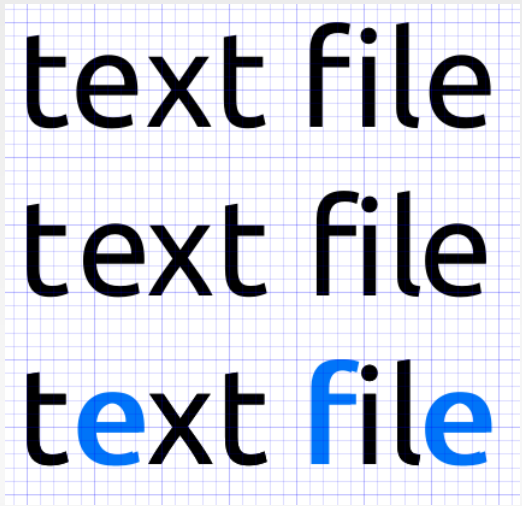
- Steganography is the art and science of hiding information using any kind of a carrier media.
- The word “steganography” comes from Greek:
  - “steganos” = “protected”
  - “graphei” = “writing”[1]
- This method is chosen when a secret information that is related to few people is required to be transmitted without other people detecting the secret information.
- The embedded information is usually hidden to senses and the carrier media do not attract attention to itself.
- Any person who is not directly involved with the hidden data will usually find only an ordinary letter, picture, etc.
- Stegonagraphy is not new. For example it is known that in 500 ~ 400 BC;
  - Messages that were directly carved on tablets were coated with wax later, causing the message to be undetectable beneath the wax surface.
  - Messages were painted on shaved heads of slaves and when hair was fully grown, slaves were sent away to deliver the message.
- Along with traditional media, steganography is also very popular in digital media.

Known Examples

- As a recent example, a college student has embedded lyrics of a Rick Astley song, which is most commonly used as an internet joke nowadays, into his paper.
- Other methods are also popular in text media:
  - Randomly placed uppercase letters in a text written in lowercase letters can hold a message, which is obviously very easy to detect.
  - Letters in a specific position of a text (e.g. 2nd letter of each word) can be grouped together to form a meaningful hidden message.
  - Positions of some letters in a text can be tilted in very little amounts to any direction. When this text is overlapped with the original text, the hidden message reveals itself.

Since the first concoction of a nexus of computational processing power in the late 1960s, never has the practicality of networks been bought into question due to the advancements of on-going assemblages excogitating advantageous intimations for the ever changing cycle of headway to the modern day network. Providing valuable resources to organisations, innumerable technicians give their time to creating and perfecting a cornucopia of networks.

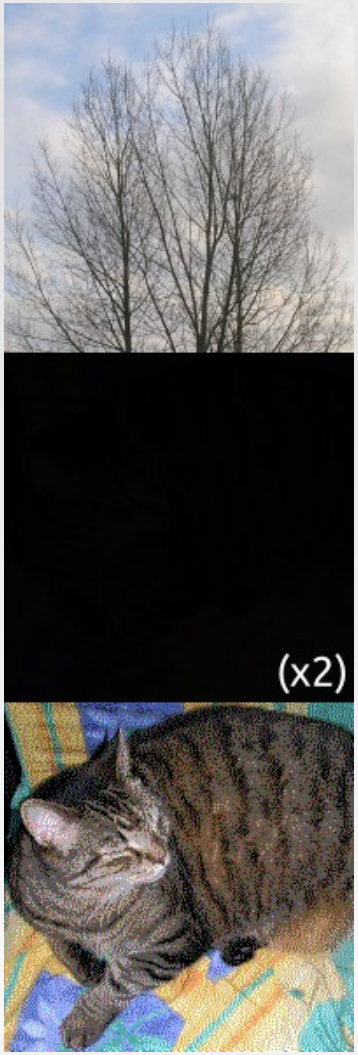
The advantages of networks are prominent and numerous, and very well documented. So you might be asking yourself why there is debate over aspects of networks, from home networks up to large corporate networks. This is due to the widespread fear that networks are essentially never safe, due to the interlacing of computers providing an ideal environment for viruses which are going to exploit a security loophole to contaminate multiple computers, which ultimately prevails to high costs for companies. Once one computer in a network is infected, the virus can competently let itself in to other computers on the network; it only takes one computer linked to yours to infect you. This has led to concerns over the security of organisations having a system which can be taken down with just one file.



Known Examples

- An another example which can be found on Wikipedia demonstrates how images can be used as a carrier media for hidden data.
- In this example, the pixels of the tree image is modified in such a way that the 7th and 8th bits of each color channel hold a very darkened image of a cat.
- When observed with human eye, any difference on these last two bits of a color value do not cause a significant change.
- If these bits are filtered and their values are multiplied by 85, the hidden image reveals itself.
- Sample C code fragment:

```
pixel[red]   = (pixel[red]   & 0x03) * 85;
pixel[green] = (pixel[green] & 0x03) * 85;
pixel[blue]  = (pixel[blue]  & 0x03) * 85;
```

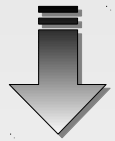


Steganography or Encryption?

- Steganography methods are used for hiding information in an unsuspected cover media.
- Encryption is used for converting meaningful data into meaningless garbage which can only be converted back to its original form by applying decryption methods.
- Steganography does not necessarily require the hidden information to be encrypted but it can be combined with encryption to strengthen data protection further.

Microsoft has a majority market share in the new desktop PC marketplace. This is a bug, which Ubuntu is designed to fix.

Non-free software is holding back innovation in the IT industry, restricting access to IT to a small part of the world's population and limiting the ability of software developers to reach their full potential, globally. This bug is widely evident in the PC industry.



RNHWTXTKY MFX F RFOTWNYD RFWPJY XMFWJ NS YMJ SJB IJXPYTU UH RFWPJYUQFHJ. YMNX NX F GZL, BMNHM ZGZSYZ NX IJXNLSJI YT KNC.

STS-KWJJ XTKYBFWJ NX MTQINSL GFHP NSSTAFYNTS NS YMJ NY NSIZXYWD, WJXYWNHYNSL FHHJXX YT NY YT F XRFQQ UFWY TK YMJ BTWQI'X UTUZQFYNTS FSI QNRNYNSL YMJ FGNQNYD TK XTKYBFWJ IJAJQTUJWX YT WJFHM YMJNW KZQQ UTYJSYNFQ, LQTGFQQD. YMNX GZL NX BNIJQD JANIJSY NS YMJ UH NSIZXYWD.

Steganography or Watermarking?

- A common mistake is accepting steganography and watermarking are the same. Although these two methods are similar in some ways, in fact they are not the same.

- Purpose is different:
  - Steganography is used for hiding information.
  - Watermarking is used for protecting the ownership of an art.
- Target audience is different:
  - Steganography is usually involved between very limited amount of people, only two in many cases.
  - Watermarked products can be distributed freely among large groups of people.

Steganography or Watermarking?

- A common mistake is accepting steganography and watermarking are the same. Although these two methods are similar in some ways, in fact they are not the same.

- Methods are different:
  - In steganography, information is hidden using methods for the chosen media. Steganalysis of a suspected media is required to detect hidden data.
  - In watermarking, information is usually imprinted directly on to media and it is visible to senses. But once imprinted, it is difficult to remove it or revert the media back to its original form.

Comparison[2]

Criteria	Steganography	Watermarking	Encryption
Carrier	Any media	Mostly image & audio	Mostly text
Secret Data	Payload	Watermark	Text
Objective	Secret communication	Copyright	Data protection
Result	Stego-file	Watermarked file	Cipher-text
Attack Method	Steganalysis	Data processing	Cryptanalysis
Visibility	Invisible	Mostly visible	Visible
Fail Condition	Detection	Removal	Decipher

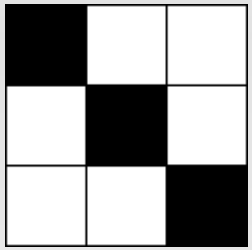
Image Steganography

- Common steganography methods applied on image media are as follows[3]:
  - Exploiting Image Format
    This method is applied by inserting data after original image data has reached EOF.
  - Spatial Domain Methods
    Most commonly used on LSB of each pixel.
  - Frequency Domain Methods
    Discrete Cosine Transform (DCT), Fourier Transform (FT), Discrete Wavelet Transform (DWT).
  - Adaptive Steganography.

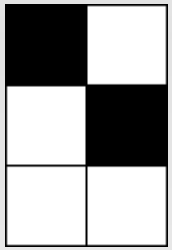
Least Significant Bit (LSB) Method

- This method involves changing the value of LSB bit of a pixels color channels in an image.
- When grouped together, the changed bits can be read into or interpreted as the hidden information.
- Any change on LSB (0 to 1 or vice versa) do not cause a great change in color information to the human eye. Because of this, various methods involving around LSB has been developed.
- But each of these methods have weaknesses. For example;
  - A lossy image format (e.g. JPEG) can't keep record of correct color information of each pixel.
  - Image operations such as rotating, resizing or cropping can cause parts of the hidden information to be lost.
  - Changing bit values in a smooth region (all pixels having exactly the same color) will cause noises, allowing a steganalysist to easily detect the hidden information.
  - Images having a large variety of colors are suitable for LSB method but advanced LSB steganalysis methods (especially based on statistics) can still cause detection.

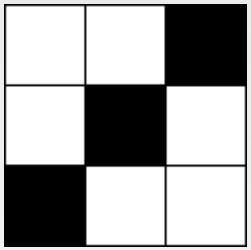
Least Significant Bit (LSB) Method



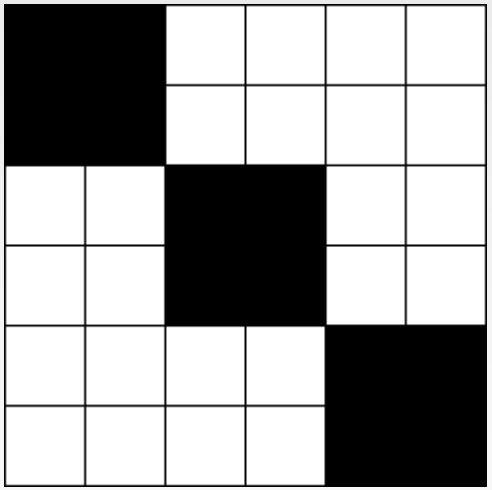
Original Pattern
011
101
110



Cropped Pattern
01
10
11

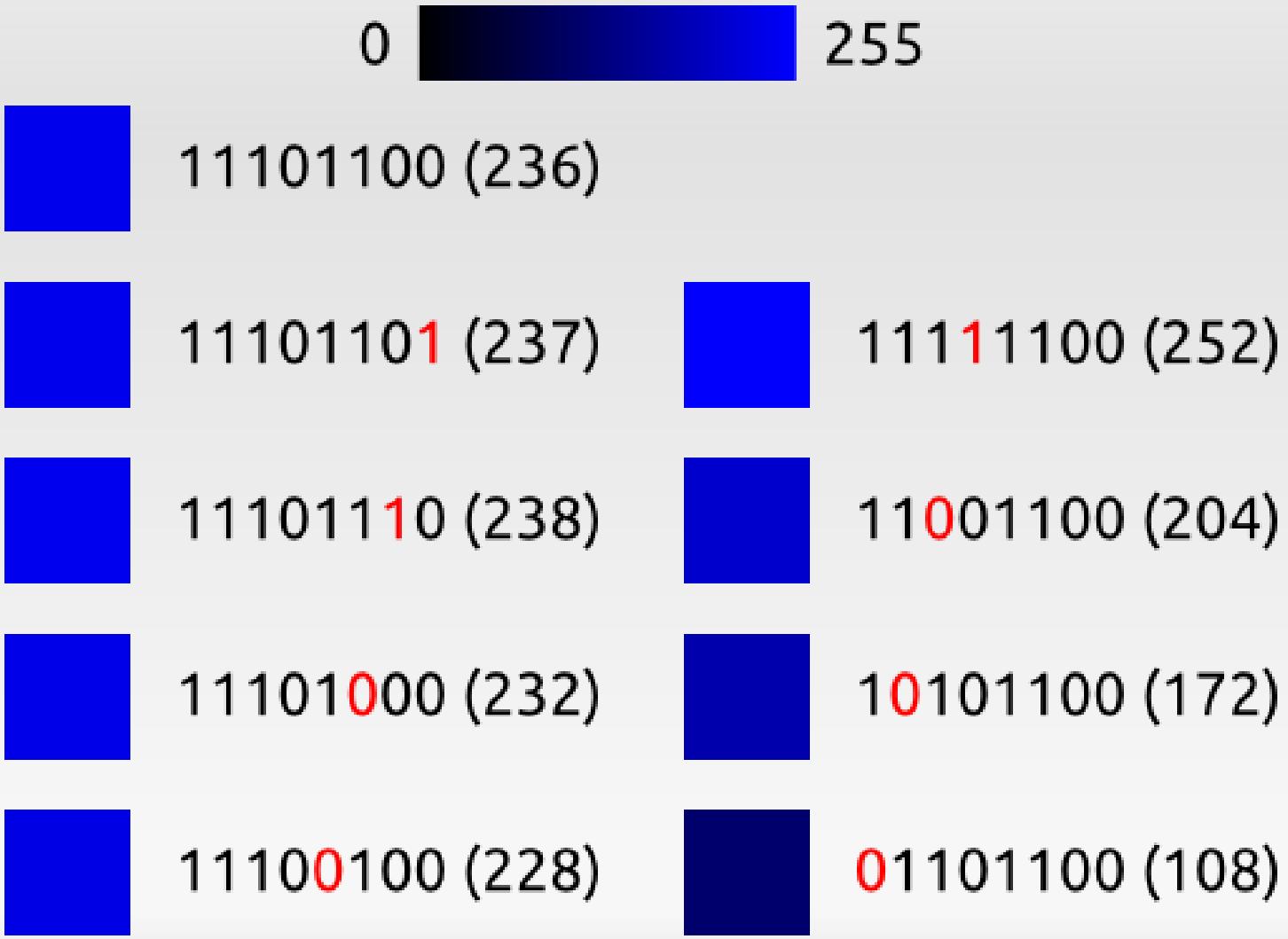


Rotated Pattern
110
101
011



Resized Pattern
001111
001111
110011
110011
111100
111100

Least Significant Bit (LSB) Method



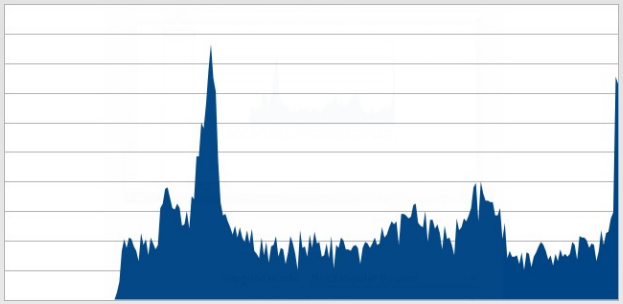
LSB Demonstration

- As a demonstration of LSB method, a sample grayscale image with dimensions 100x100 had been chosen.
- A random text (“*Lorem ipsum dolor sit amet...”*) with 1.250 bytes (=10.000 bits) had been generated.
- Bits of this text had been applied upon original image, leaving no pixels untouched.
- Unless carefully inspected, original and stego images seem the same to the human eye.
- But comparison of original and stego image's histograms clearly shows that the stego image contains more noise than the original image.

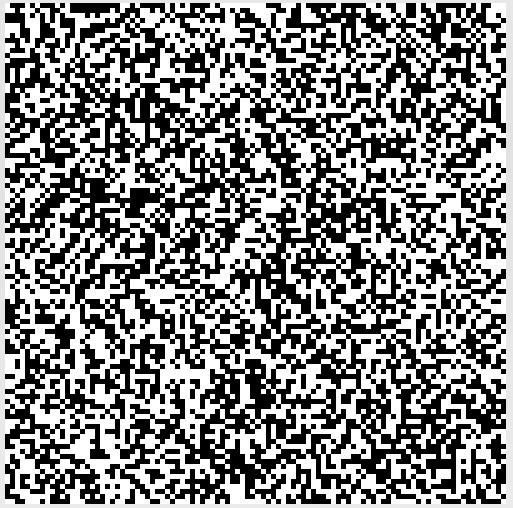
LSB Demonstration

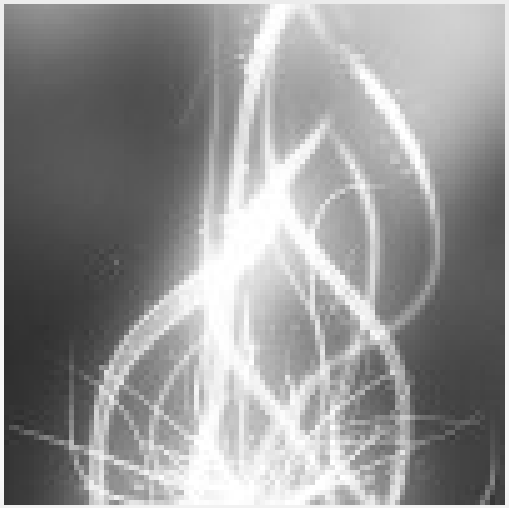
original image

histogram of original image

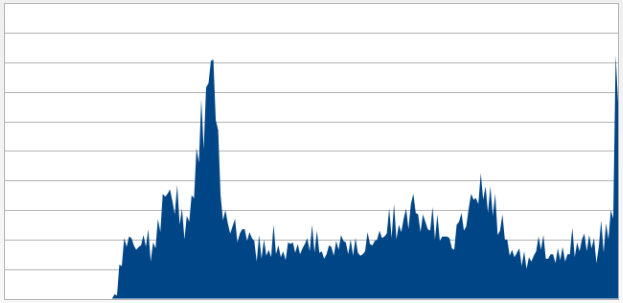


LSB's of original image

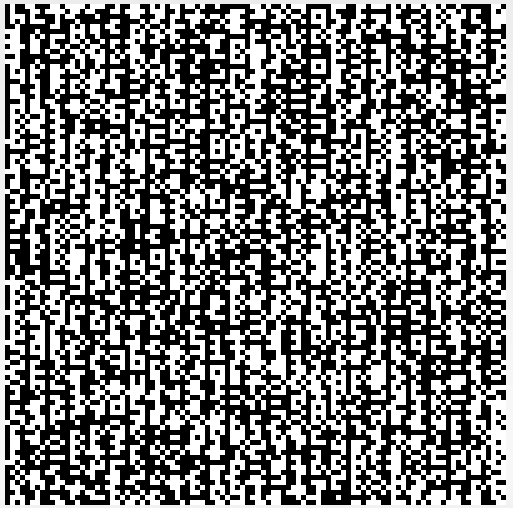




stego image

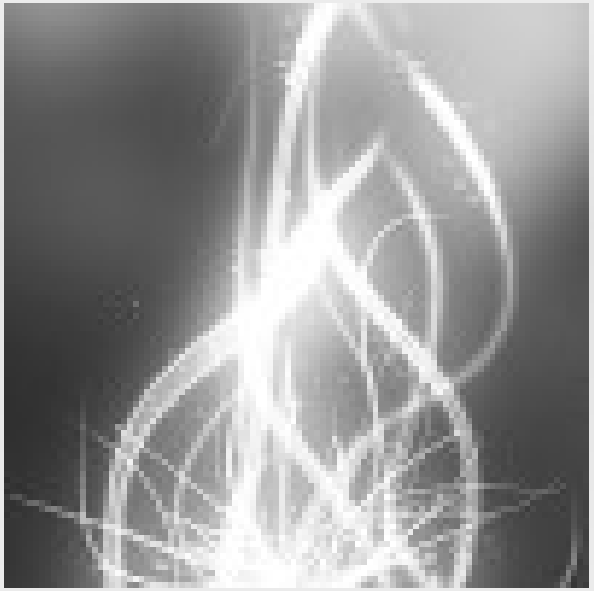


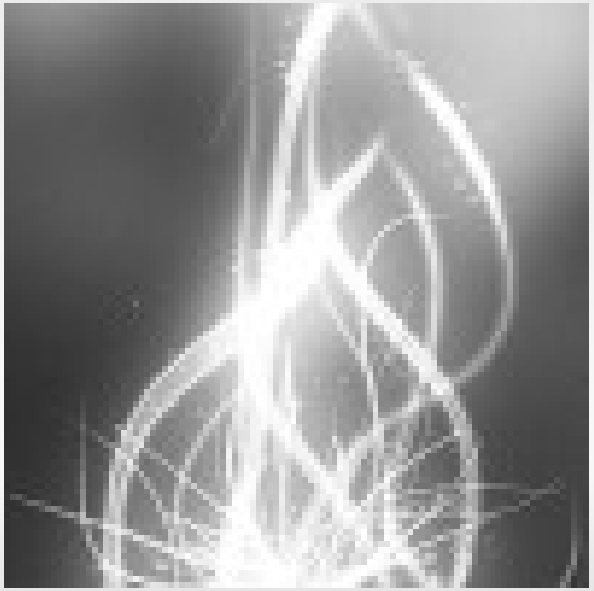
histogram of stego image



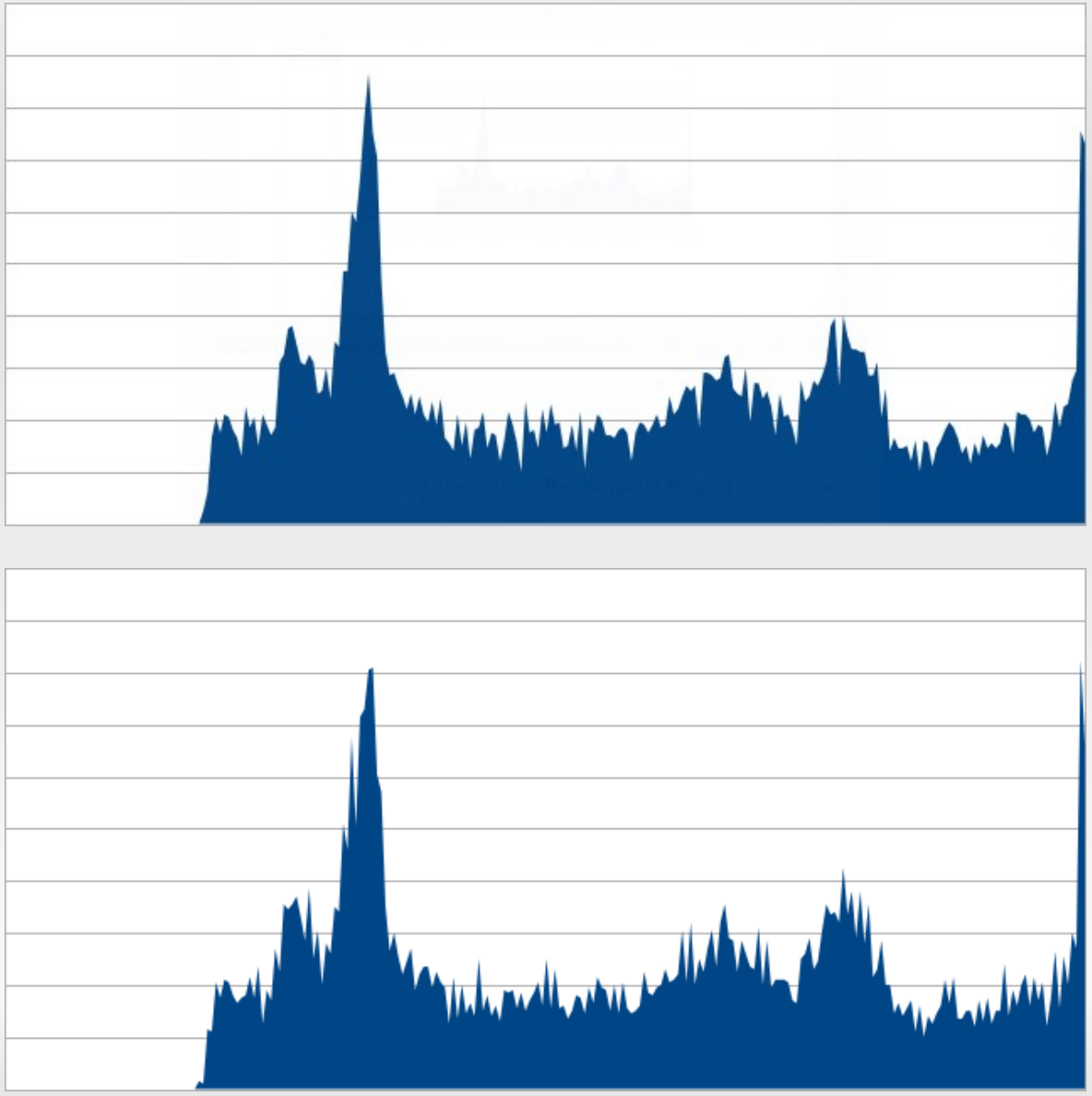
LSB's of stego image

LSB Demonstration

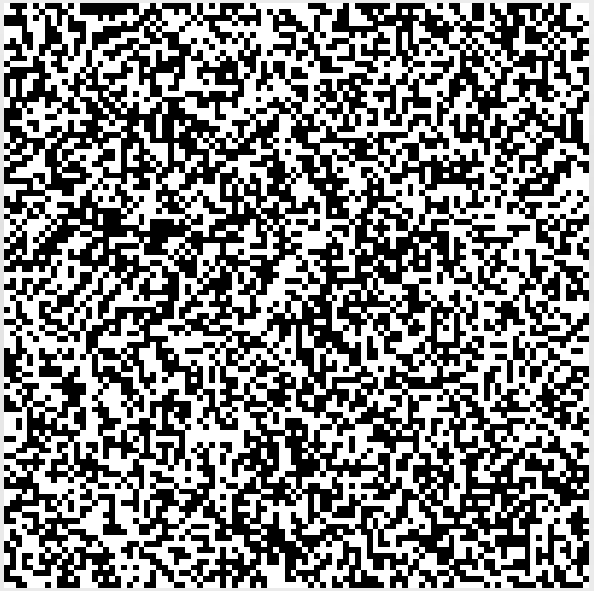


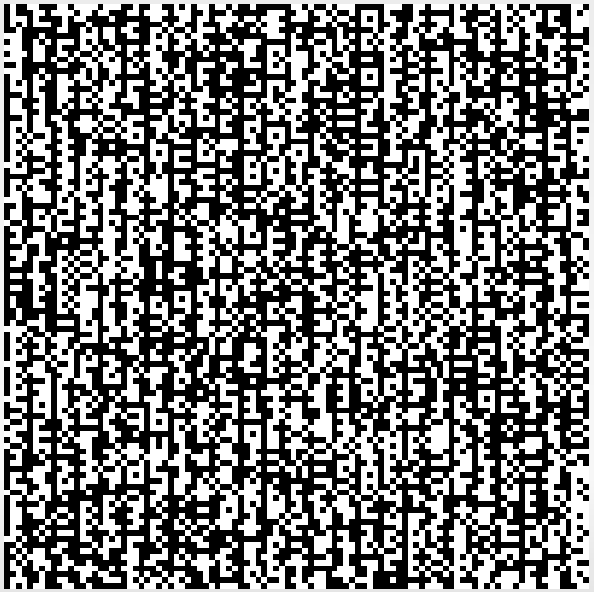


LSB Demonstration



LSB Demonstration





Resources & References

[1] Steganography, Wikipedia
http://en.wikipedia.org/wiki/Steganography

[2][3] Digital Image Steganography: Survey and Analysis of Current Methods
Abbas Cheddad, Joan Condell, Kevin Curran, Paul Mc Kevitt
Signal Processing, Elsevier, Volume 90, Issue 4, Pages 727 - 752, 2010

Thanks for listening!

Any questions?