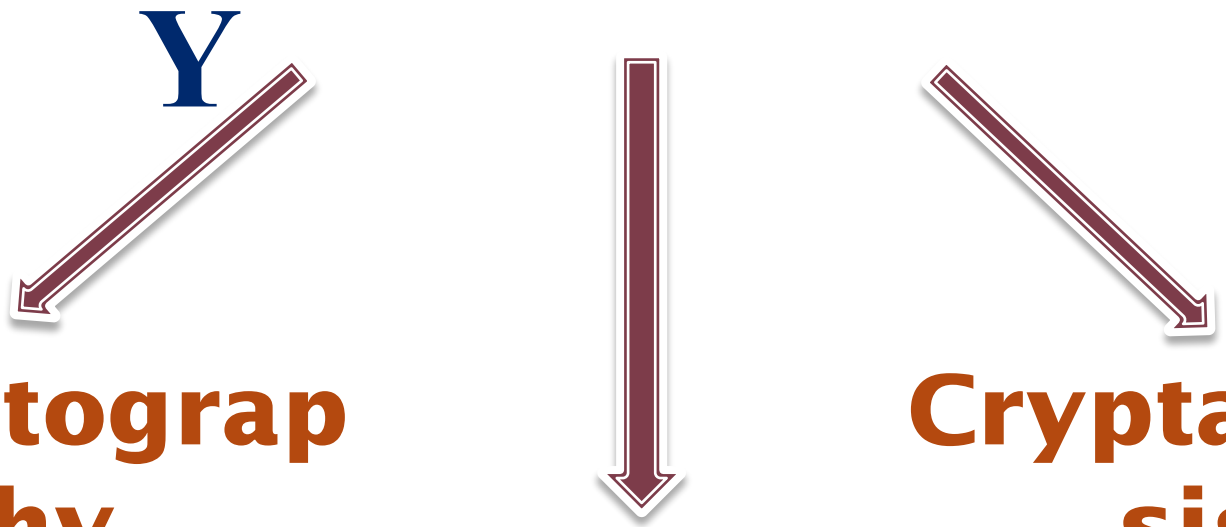
Steganography

By

Tukenov Ilyas & Tleuov Adilet

TABLE OF CONTENTS

CRYPTOLOGY



Cryptography

Steganography

Cryptanalysis

STEGANOGRAPHY

- Derived from the Greek words, Steganos (Covered) & Grapto (Writing)
- Practice of hiding private or sensitive information within something that is usually not suspected
- Steganography in the modern day sense refers to information or a file that has been concealed inside a digital Picture, Video or Audio file
- Science of hiding information in such a way that no one suspects the information exists
- Steganography is usually combined with Cryptography

HISTORY

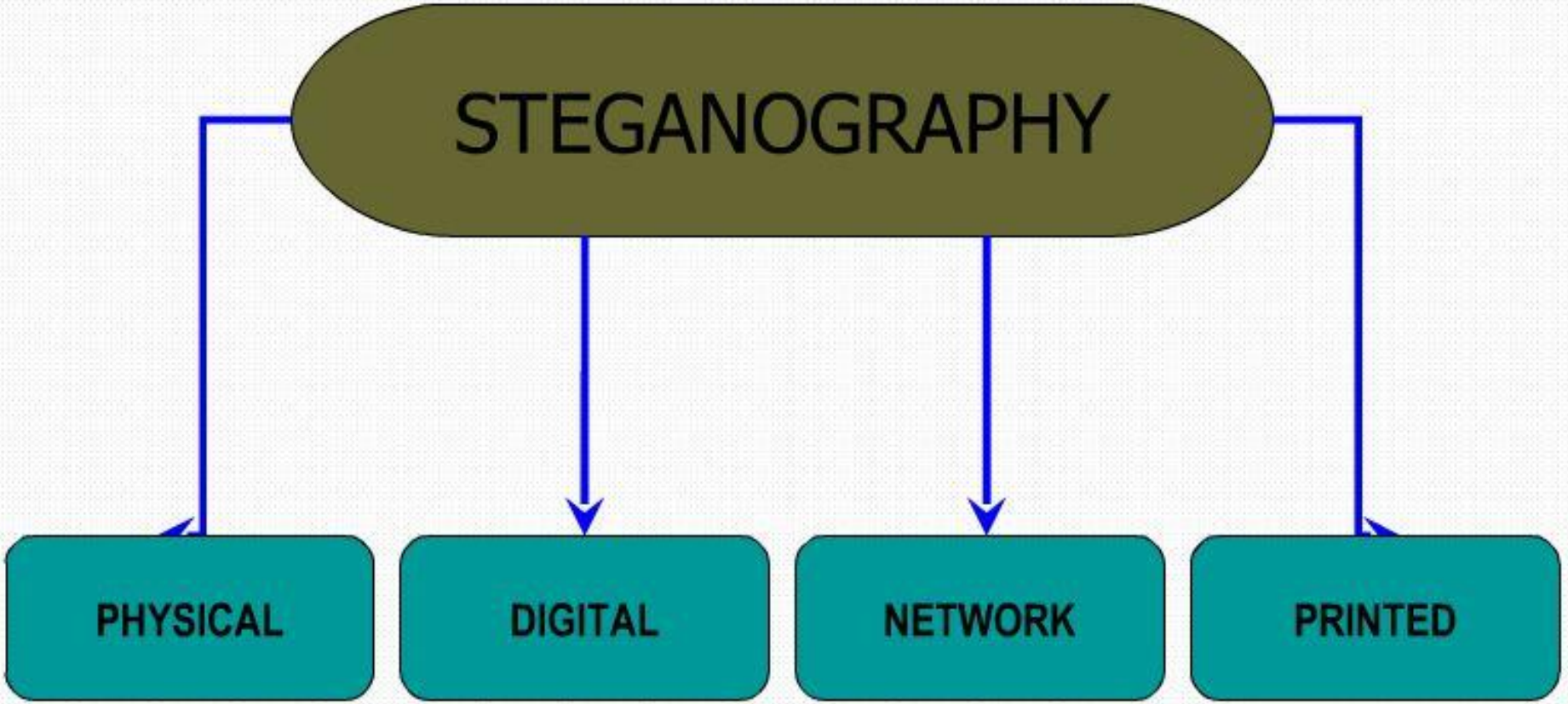
- Earlier invisible ink was used to write information on pieces of paper
- Head of messengers were shaved so, a message could be written on it
- Wax tablet was peeled on which message was to be written & refilled

"**P**RESIDENT'S **E**MBARGO **R**ULING **S**HOULD **H**AVE **I**MMEDIATE **N**OTICE. **G**RAVE **S**ITUATION **A**FFECTING **I**NTERNATIONAL **L**AW. **S**TATEMENT **F**ORESHADOWS **R**UIN **O**F **M**ANY **N**EUTRALS. **Y**ELLOW **J**OURNALS **U**NIFYING **N**ATIONAL **E**XCITEMENT **I**MMENSELY."

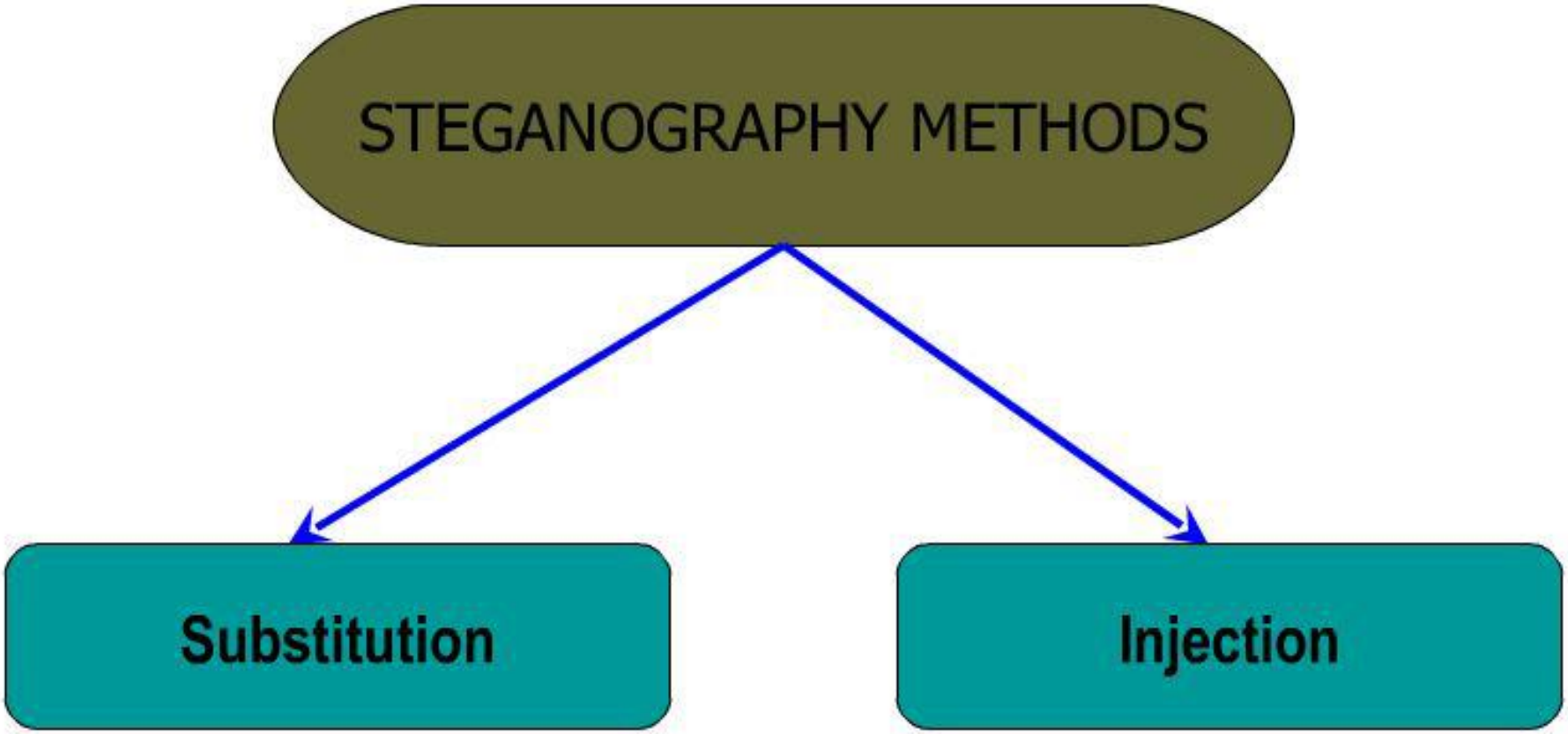
(Taking the first letter in each word of message reveals the hidden text.)

" ***PERSHING SAILS FROM NY JUNE 1"***

CLASSIFICATION



WORKING PRINCIPLE



SUBSTITUTION

Altering/Replacing The LSB

- When files are created there are usually some bytes in the file that aren't really needed, or are unimportant
- These areas of the file can be replaced with the information that is to be hidden, with out significantly altering the file or damaging it
- This allows a person to hide information in the file and make sure that no human could detect the change in the file
- The LSB method works best in Picture files that have a high resolution and use many different colors, and with Audio files that have different sounds and are of a high bit rate
- It usually does not increase file size, but depending on size of the information that is to be hidden, the file can become noticeably distorted

INJECTION

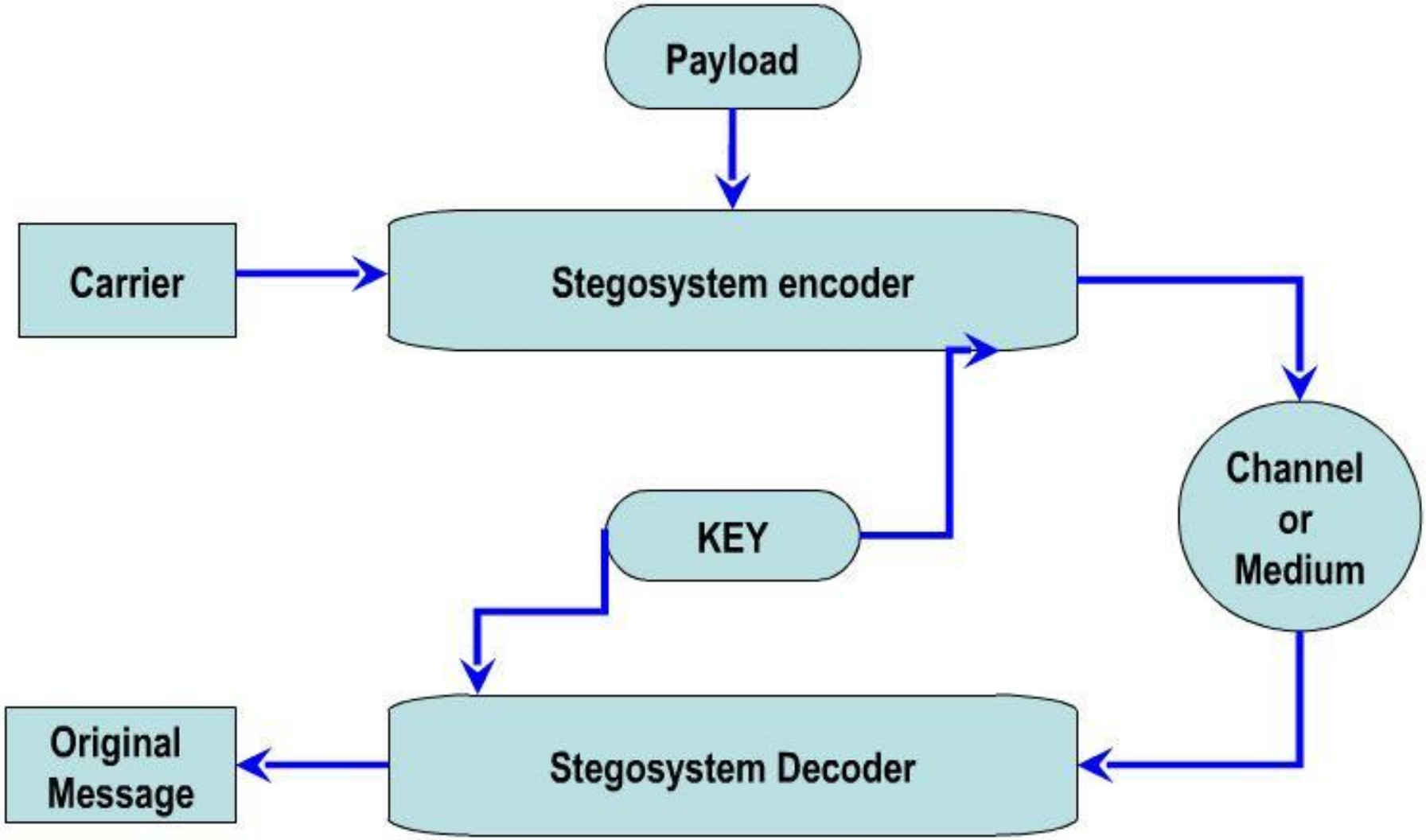
Injection

- Injection is a relatively simple method than altering the Least Significant Bit (LSB) technique
- Injection method involves directly injecting the secret information into the carrier file
- The Payload and Carrier message are directly fed into the specially designed Stegosystem encoder
- The main problem with this method is that it can significantly increase the size of the carrier file

TERMINOLOGY

- Carrier File - A file which has hidden information inside it
- Steganalysis - Process of detecting hidden information inside a file
- Stego-Medium - The medium in which the information is hidden
- Payload - The information which is to be concealed
- Redundant Bits - Pieces of information inside a file which can be overwritten or altered without damaging the file

FLOW CHART


Payload
Carrier
Stegosystem encoder
Channel
or
Medium
KEY
Original
Message
Stegosystem Decoder

STEGANOGRAPHY PROCESS

Three basic ways to encode data in steganography:

1. Image as a carrier
2. Pixel representation in RGB
3. Bandwidth reduced file transfer

1.IMAGE AS CARRIER:

It is an efficient technique for steganography, An image is used as cover for hiding the actual data. Digital images are a preferred media for hiding information due to their high capacity and low impact on visibility.

2.PIXEL REPRESETATION IN RGB:

Basic RGB color model, every pixel is represented by the four bytes namely Alpha, red, green, blue Alpha: degree of transparency Red: intensity of red color Green: intensity of green color Blue: intensity of blue color

The alpha bit is used to carry the data, as it has no much importance in image representation.

3.BANDWIDTH REDUCED TRANSMISSION:

If an image data takes six minutes to transfer between two systems and a text file takes 3 minutes. One can use steganography technique in order to reduce the time taking by embedding the text in the image and the total content will be transferred in six minutes.

Two basic algorithms used for steganography are

1. Text on Image algorithm.
2. Image on Image algorithm.

BASIC ALGORITHMS

Two basic algorithms used for steganography

1. Text on Image algorithm.
2. Image on Image algorithm.

BASIC ALGORITHMS

Text on Image technique block diagram:

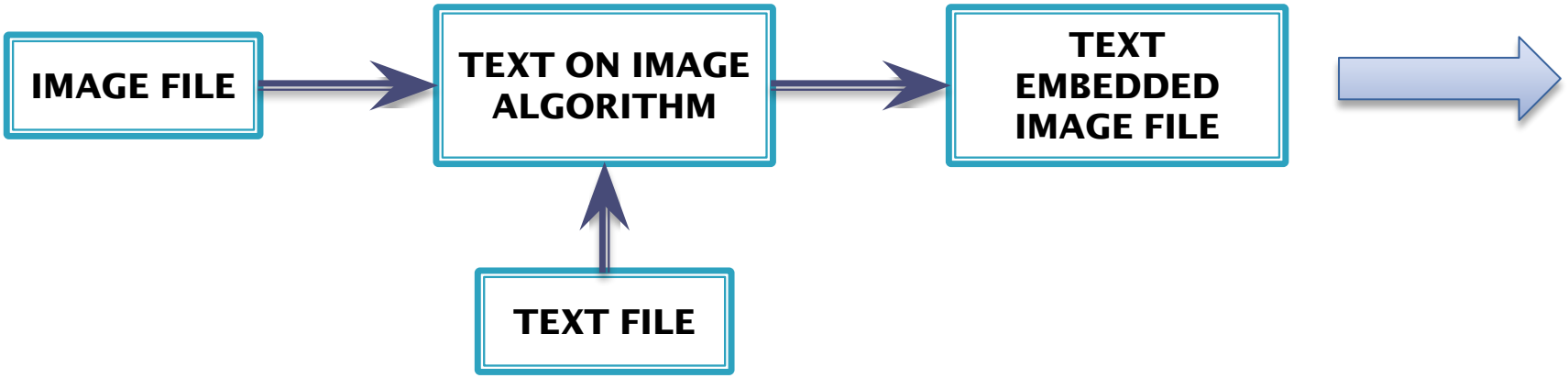
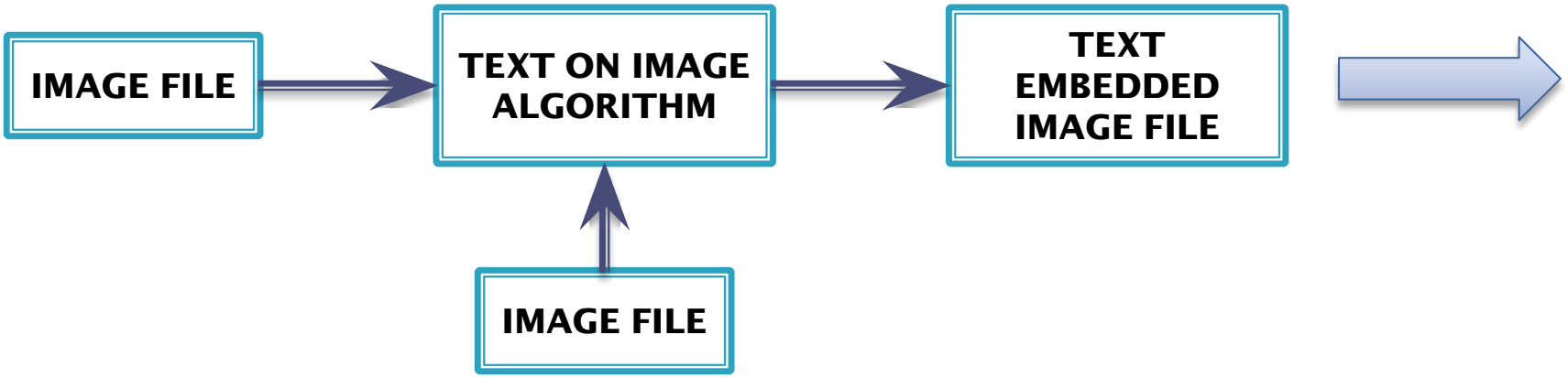
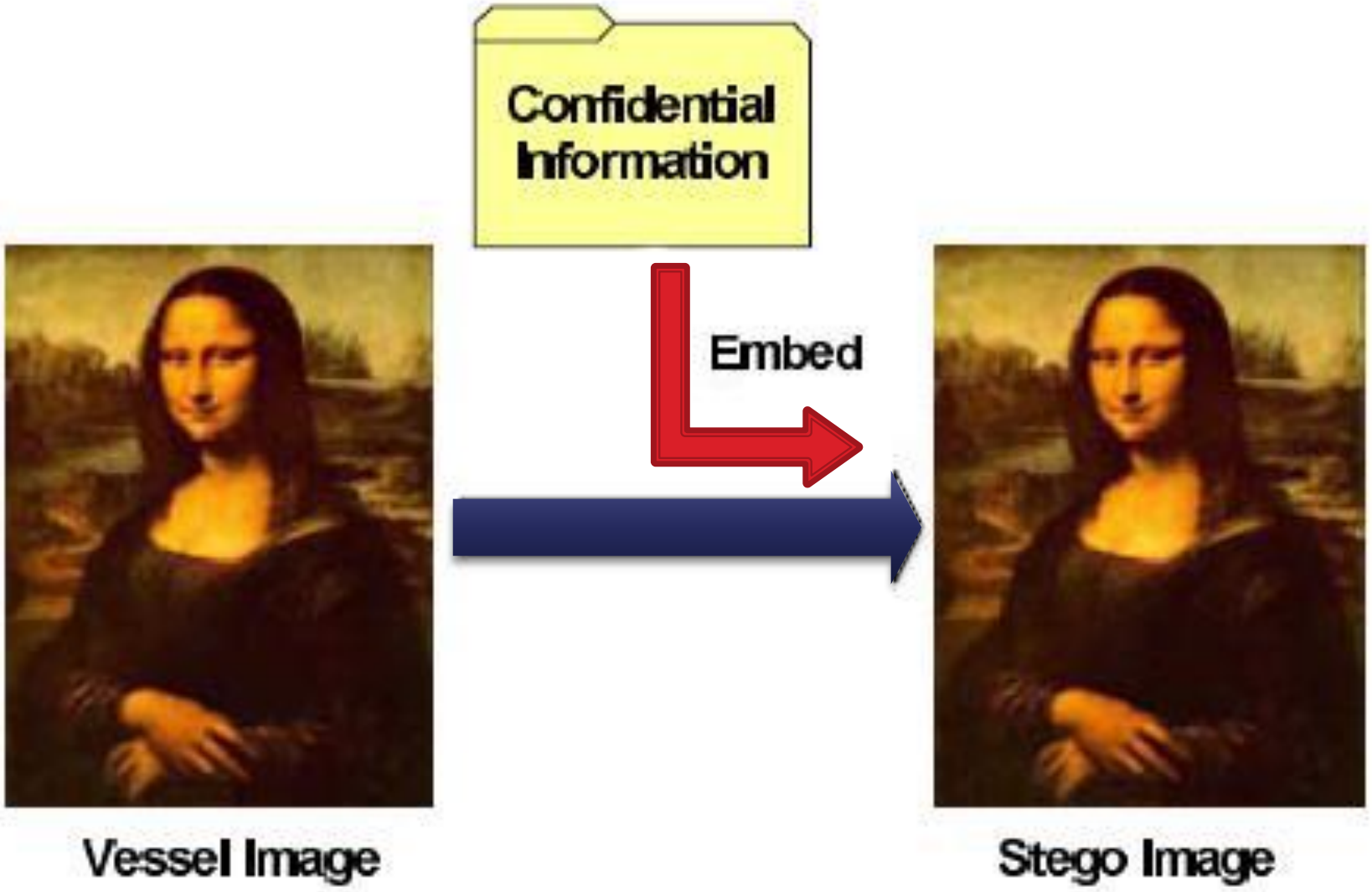


Image on Image technique block diagram:



ILLUSTRATION



APPLICATION

- ***Modern Printers***

  Steganography is used by leading manufacturers in digital & laser printers, including HP and Xerox. Here, tiny yellow dots are added to each page. The dots are barely visible and contain encoded printer serial numbers, as well as date and time stamps.

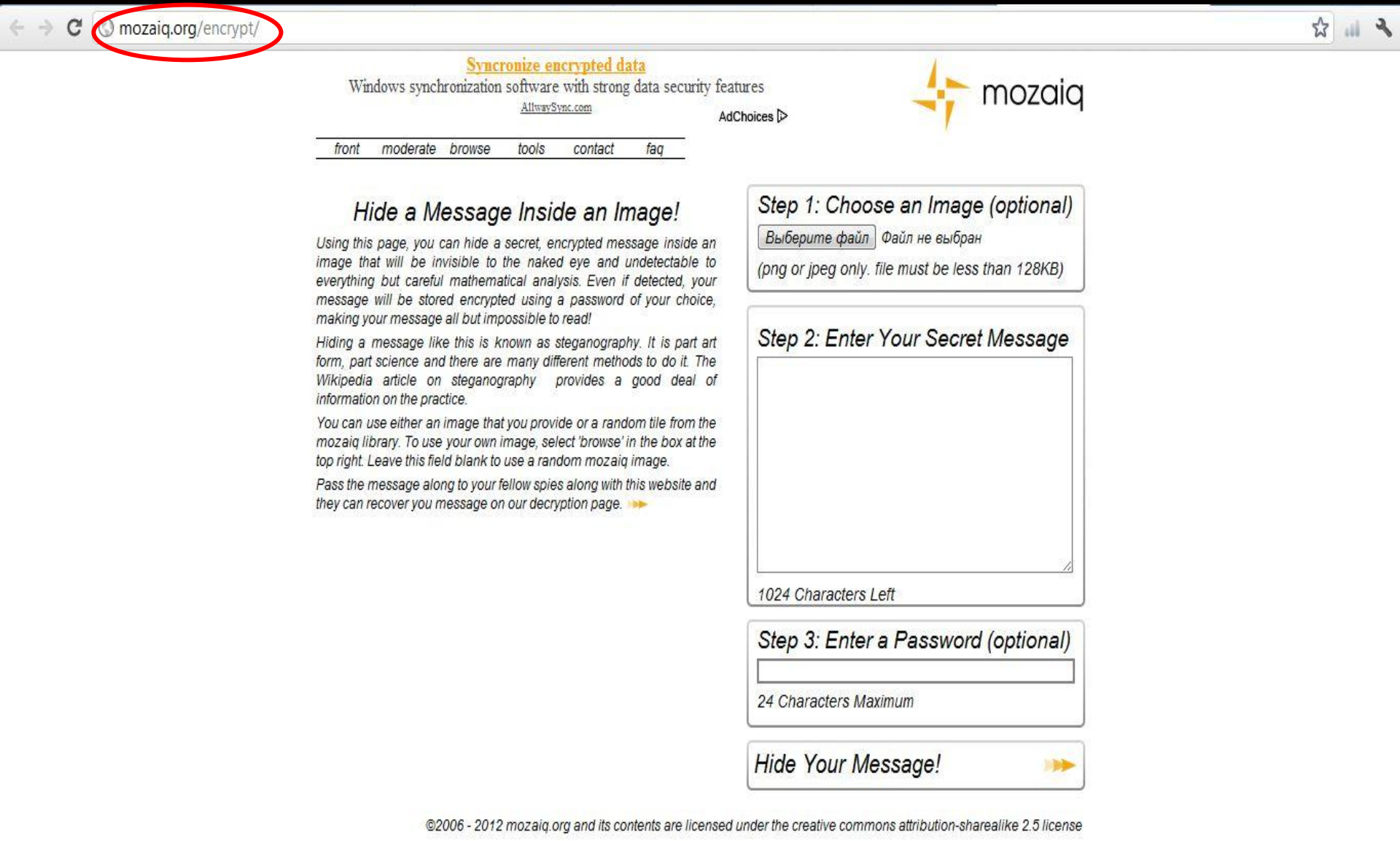
- ***Digital Watermarking***

  Steganography is used for digital watermarking, where a message is hidden in an image so that its source can be tracked or verified.

- ***e-mail Spam***

  e-mail messages is encrypted steganographically. Coupled with the "chaffing and winnowing" technique, a sender gets messages out and cover their tracks all at once.

http://mozaiq.org/encrypt/



ADVANTAGES

1. Internet privacy.

2. Secret communication between the organizations like boarder security force and defense organization.

3. Effective than that of cryptography.

4. Additional layer for security than cryptography.

ADVANTAGE OF STEGANOGRAPHY OVER CRYPTOGRAPHY

Messages do not attract attention to themselves

Protects both messages and communicating parties

CONCLUSION

- Steganography is the art of hiding sensitive data without generating unnecessary curiosity and suspision among foreign party
- Steganalysis is the technique to detect Steganography
- The research to device strong steganographic and steganalysis technique is a continuous process

THANK YOU!