An Overview of Image Steganography

Security using Image Processing

Tianhao Lee

School of Information
North China University of Technology

November 5, 2022

Outline

Introduction

- Trend: Machine learning $\times$ Image Processing
- Relation: Digital Image Processing & Computer Vision
- Application of Digital Image Processing
  - Face recognition
  - Iris recognition
  - Fingerprint detection
  - Tracking a person in a camera
  - Recognizing a person over multiple cameras
  - Activity detecting
  - ... ...

Introduction

Figure: Iris Recognition

Introduction

Figure: Face Recognition

Introduction

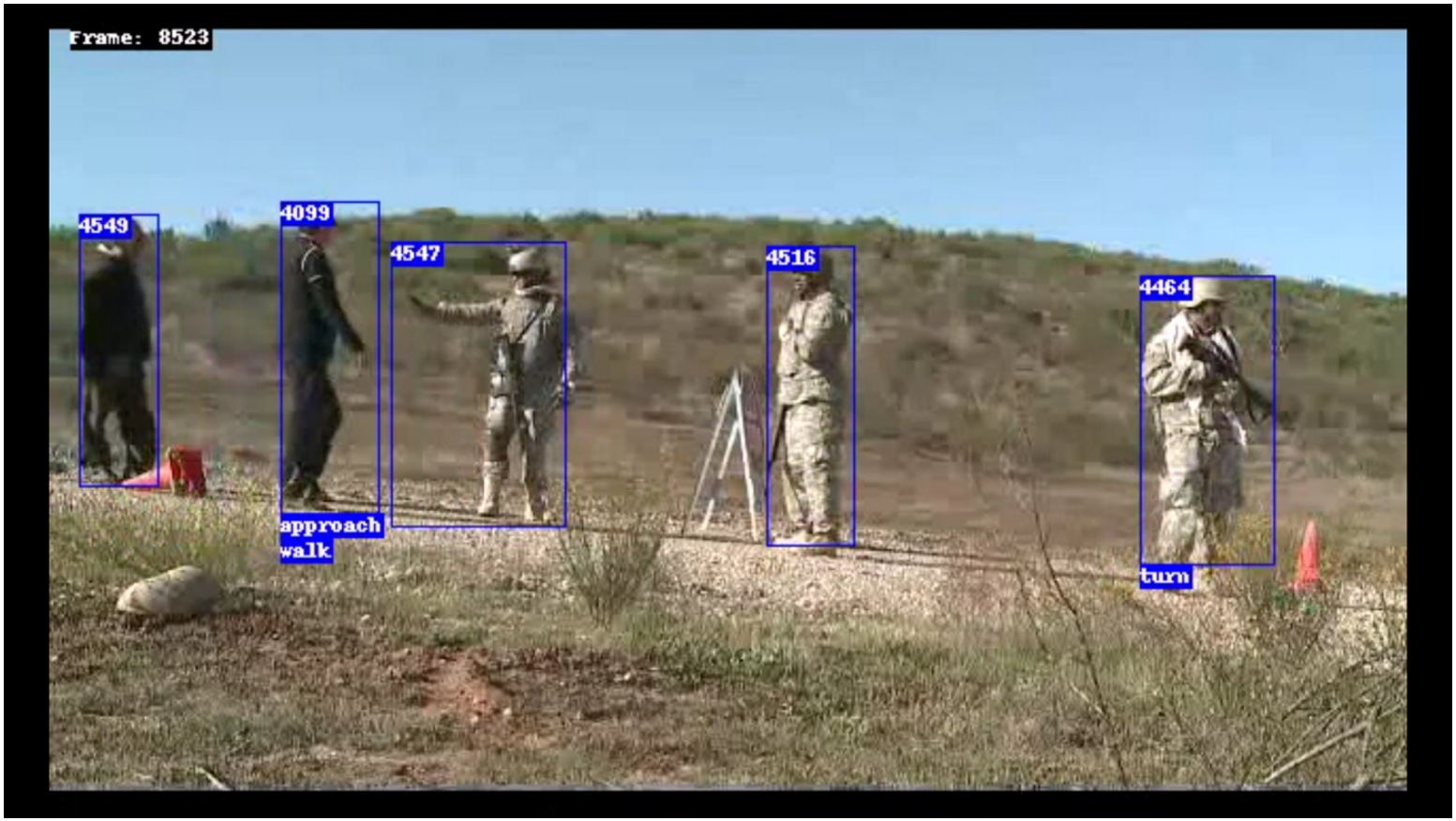


Figure: Activity Recognition

Introduction to Steganography

- Techniques Before Steganography
  - Digital Watermarking
  - Visual Cryptography
- Embed data or another image within the image
  - Spatial Domain
  - Frequency Domain
  - Compressed Data Domain

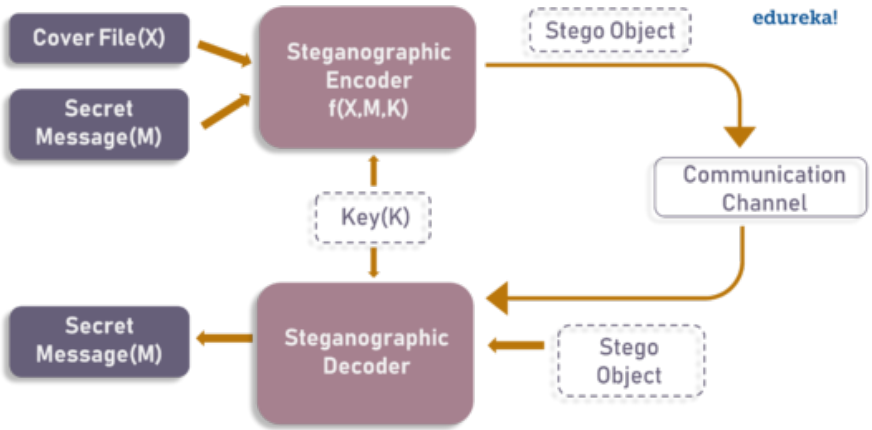


Figure: Steganography

Existing System

- Various system are available for information hiding in an image, but they have some drawbacks
  - No encryption, hide only
  - Weak encryption using weak algorithm
  - Same key for both encryption and decryption
  - Using strong algorithm but easily distinguishable by naked human eyes
- Make image smooth and more realistic
  - Multiband blending
  - Gain compensation
  - Automatic straightening

Proposed System

- The steganography process are divided into four phases
  - Encryption phase: AES Algorithm
  - Embedding phase: LSB Replacement
  - Hidding phase: Kekre's Median Codebook Generation (KNCG) Algorithm
  - Stiching Phase: K-Nearest Neighbour (KNN) Algorithm
- The phases are as above breaking an image of size w*h into n sub-image of size x*y can be done using blkproc function in Matlab

Encrypting Phase

The message to be sent is encrypted using AES algorithm.

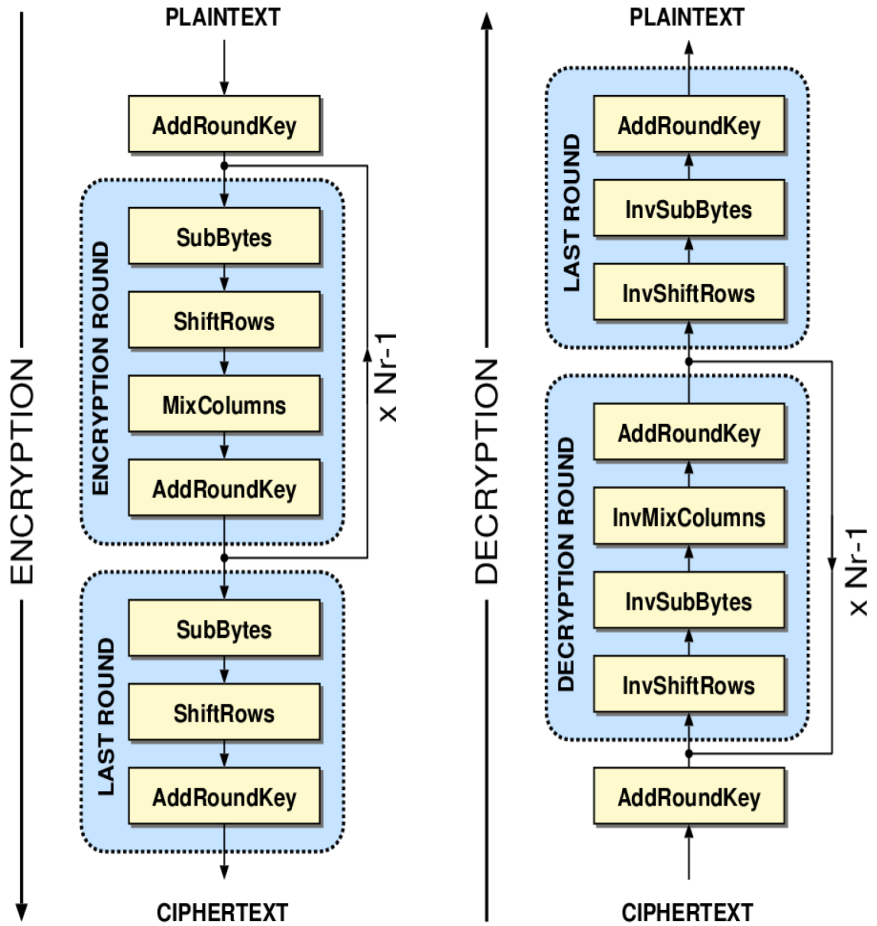


Figure: AES Algorithm

Encrypting Phase

AES algorithms essentially take basic data and change it into a ciphertext.

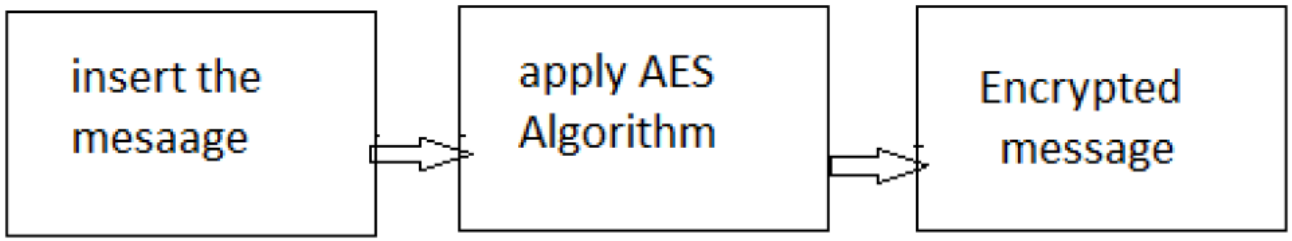


Figure: Crypto Module

For Crypto Module the following steps are considered for encrypting the data:

- Insert text for encryption
- Apply AES algorithm using 128 bit key
- Generate Cipher Text in hexadecimal form

Embedding Phase

In this phase the encrypted message is embedded on to a part of the secret image.

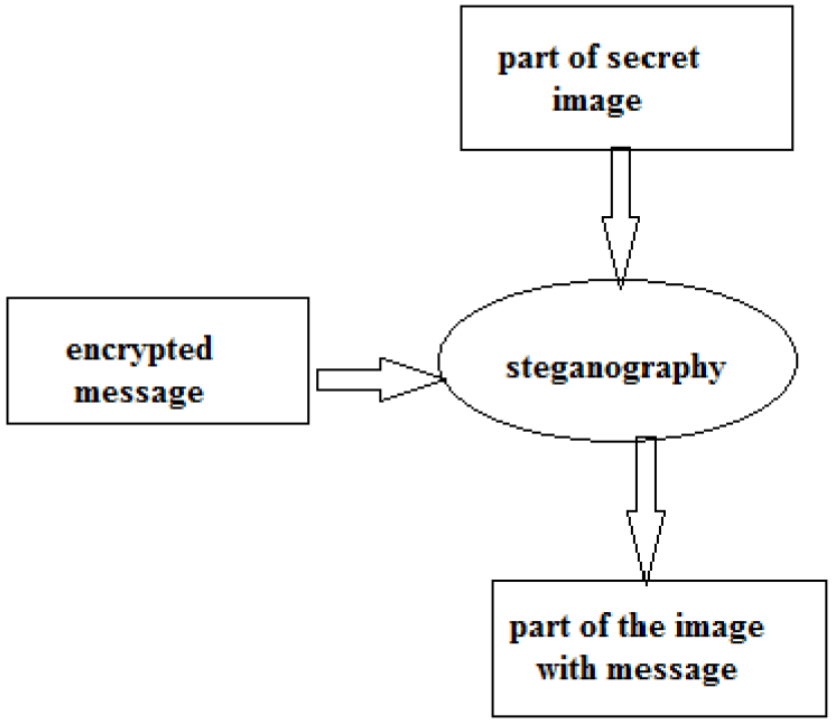


Figure: Embedding Process

How to embed? Use LSB Replacement!

LSB Steganography

- Human observers will be unable to distinguish between the orignal image and the encoded image
- The pixels of the encoded image will be, at most, 1 value separated from the original
- As you begin to encode using higher bits, severe degradation of the cover image occurs, defeating the purpose of encoding

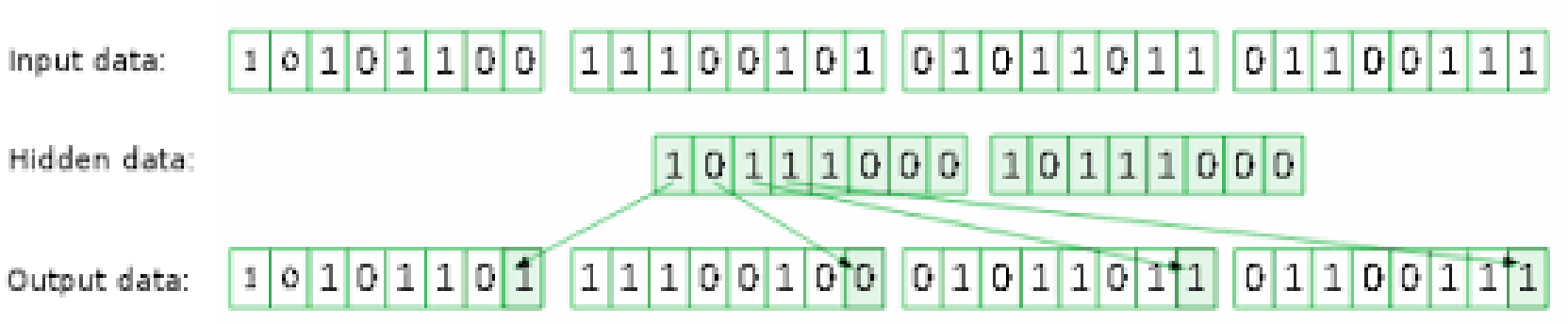


Figure: Least Significant Bit Steganography

LSB Steganography

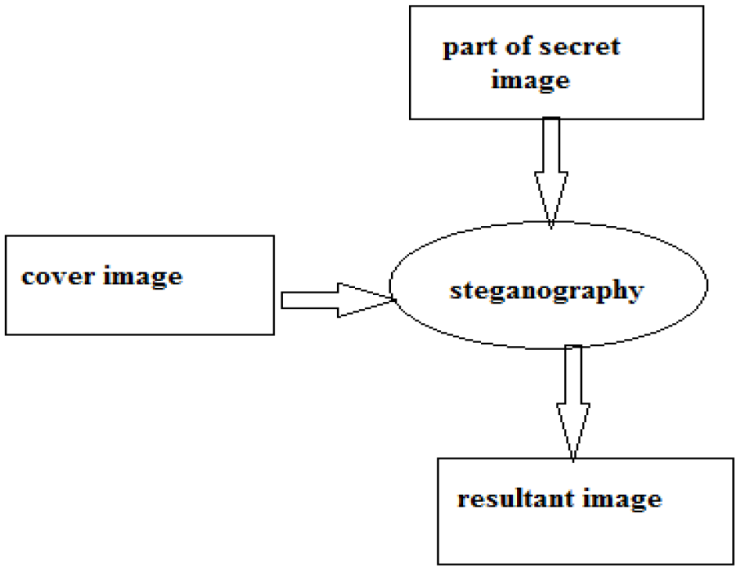
The LSB steganographic algorithm is used for hiding the cipher inside the image,. In this each bit of the cipher text (that has been converted into its binary equivalent) is exchanged with the last bit of each pixel value. Similarly for each pixel the last bit is replaced with the consecutive bits of the cipher text i.e. its binary equivalent. Therefore four possibilities of swapping are:

- '0' -> '0'
- '0' -> '1'
- '1' -> '0'
- '1' -> '1'

In case two and three, only LSB is going to be changed. Hence the resulting image resumble the orignal image.

Hiding Phase

The use of Kekre's Median Codebook Generation Algorithm (KNCG).



$$T = \begin{pmatrix} x_{11} & x_{12} & \dots x_{1K} \\ x_{21} & x_{22} & \dots x_{2K} \\ x_{M1} & x_{M2} & \dots x_{MK} \end{pmatrix}$$

Stiching Phase

Algorithm: Automatic Panorama Stitching

- Input: n unordered images
  1. Extract SIFT features from all n images
  2. For each feature find nearest- k -neighbours using a k-d tree
  3. For each image:
     1. Select m candidate matching images that have the most feature matches to this image
     2. Use RANSAC to find geometrically consistent feature matches to solve for the homography between pairs of images
     3. Using a probabilistic model verify image matches
  4. Find connected components of image matches
  5. For each connected component:
     1. Perform bundle adjustment to solve for the rotation _1, _2, _3 and focal length f of all cameras
     2. Render panorama using multi-band blending
- Output: Panoramic image(s)

Conclusion

- A novel system based on Digital Image Processing and Cryptography
- A novel system for data and image encryption using AES algorithm for cryptography, image steganography and image stitching.
- A novel system combines Cryptography based on text and Image Steganography - A highly secured method for data transactions.
- Application Prospect
  - Banking
  - Consultancies
  - Detecive Agencies