CNS M1L4

Introduction: Some Simple Cryptosystems

- <6> Permutation Cipher
  - Cryptosystem 1.6: Permutation Cipher
    - m is a positive integer
    - $\mathcal{P} = \mathcal{C} = (Z_{26})^m$
    - $\mathcal{K}$ consist of all permutations of {1,…,m}
    - For a key(a permutation) π

$$d_\pi(y_1,\ldots,y_m) = (y_{\pi^{-1}(1)},\ldots,y_{\pi^{-1}(m)})$$

  - $e_\pi(x_1,\ldots,x_m)=(x_{\pi(1)},\ldots,x_{\pi(m)})$

where π^{-1} is the inverse permutation to π

Introduction: Some Simple Cryptosystems

- e.g.: Suppose m=6
  - Plaintext: CYBERFORMULA
  - Ciphertext: BRCFEYMLOAUR

x	1	2	3	4	5	6
$\pi(x)$	3	5	1	6	4	2

plaintext	**C**	**Y**	**B**	**E**	**R**	**F**	**O**	**R**	**M**	**U**	**L**	**A**
ciphertext	**B**	**R**	**C**	**F**	**E**	**Y**	**M**	**L**	**O**	**A**	**U**	**R**

Introduction: Some Simple Cryptosystems

- <7> Stream Ciphers
  - Block ciphers

    Plaintext string $x = x_1 x_2 \ldots$ (each x_i is a plaintext)

    Ciphertext string $y = y_1 y_2 \ldots = e_K(x_1) e_K(x_2) \ldots$

  - Stream ciphers
  - Plaintext string $x = x_1 x_2 \ldots$

    Generate a keystream (by using some K) $z = z_1 z_2 \ldots$

    Ciphertext string $y = y_1 y_2 \ldots = e_{z1}(x_1) e_{z2}(x_2) \ldots$

Introduction: Some Simple Cryptosystems

- Definition 1.6: A synchronous stream cipher is a tuple $(\mathcal{P},\mathcal{C},\mathcal{K},\mathcal{L},\mathcal{E},\mathcal{D})$ with a function g
  - $\mathcal{P}$: a finite set of possible plaintexts
  - $\mathcal{C}$: a finite set of possible ciphertexts
  - $\mathcal{K}$: a finite set of possible keys
  - $\mathcal{L}$: a finite set called the keystream alphabet
  - g: the keystream generator
    - Input: K
    - g generates an infinite string $z_1 z_2 \ldots$

Introduction: Some Simple Cryptosystems

- Definition 1.6 (cont.)
  - For each $z \in \mathcal{L}$, there is an encryption rule $e_z \in \mathcal{E}$ and a corresponding decryption rule $d_Z \in \mathcal{D}$
    - $e_K : \mathcal{P} \to \mathcal{C}$
    - $d_K : \mathcal{C} \to \mathcal{P}$
    - $d_z(e_z(x))=x$ for every plaintext $x \in \mathcal{P}$

Introduction: Some Simple Cryptosystems

- Vigenère Cipher can be defined as a synchronous stream cipher
  - $\mathcal{K} = (Z_{26})^m$
  - $\mathcal{P} = \mathcal{C} = \mathcal{L} = Z_{26}$
  - $e_z(x)=(x+z) \bmod 26$
  - $d_z(y)=(y-z) \bmod 26$
  - Keystream $z_1 z_2 \ldots$

$$= k_1 k_2 .. k_m \; k_1 k_2 .. k_m \; k_1 k_2 .. k_m \ldots$$

$$z_i = \begin{cases} k_i & \text{if } 1 \le i \le m \\ z_{i-m} & \text{if } i \ge m+1 \end{cases}$$

Introduction: Some Simple Cryptosystems

- Keystream can be produced efficiently in hardware using a LFSR (Linear Feedback Shift Register)
  - k_1 would be tapped as the next keystream bet
  - $k_2, \ldots k_m$ would each be shifted 1 stage to the left
  - The new value of km would be

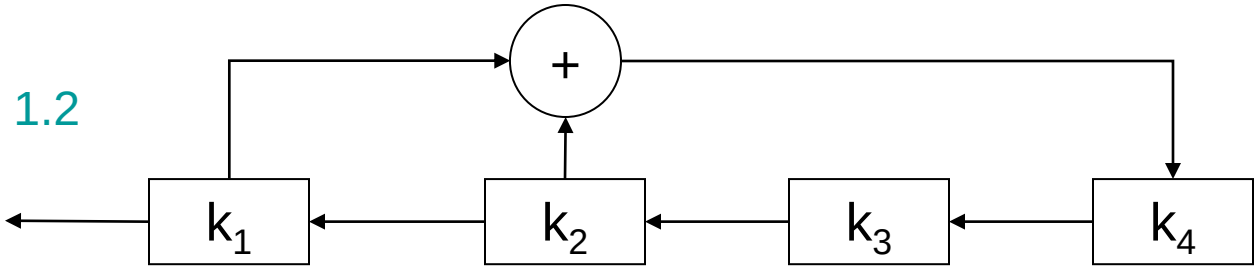
$$\sum_{j=0}^{m-1} c_j k_{j+1}$$

    this is "linear feedback" (see Figure 1.2)

  - This system is modulo 2

Introduction:
Some Simple Cryptosystems

Figure 1.2



- e.g.: in Figure 1.2,suppose K=(1,0,0,0)
  - c_0=1, c_1=1, c_2=0, c_3=0
  - The keystream is

    1000100110101111…

Introduction: Some Simple Cryptosystems

- Non-synchronous stream cipher:
  - Each keystream element zi depends on previous plaintext or ciphertext elements
- Cryptosystem 1.7: Autokey Cipher
  - $\mathcal{P} = \mathcal{C} = \mathcal{K} = \mathcal{L} = Z_{26}$
  - $z_1 = K$, $z_i = x_{i-1}$ for all $i > 1$
  - For $x, y, z \in Z_{26}$
    - $e_z(x) = (x+z) \bmod 26$
    - $d_z(y) = (y-z) \bmod 26$

Introduction:
Some Simple Cryptosystems

- e.g.: Suppose K=8
  - Plaintext: student
  - Ciphertext: ALNXHRG

plaintext	**s**	**t**	**u**	**d**	**e**	**n**	**t**
	18	**19**	**20**	**3**	**4**	**13**	**19**
keystream	**8**	**18**	**19**	**20**	**3**	**4**	**13**
ciphertext	**0**	**11**	**13**	**23**	**7**	**17**	**6**
	A	**L**	**N**	**X**	**H**	**R**	**G**

Steganography

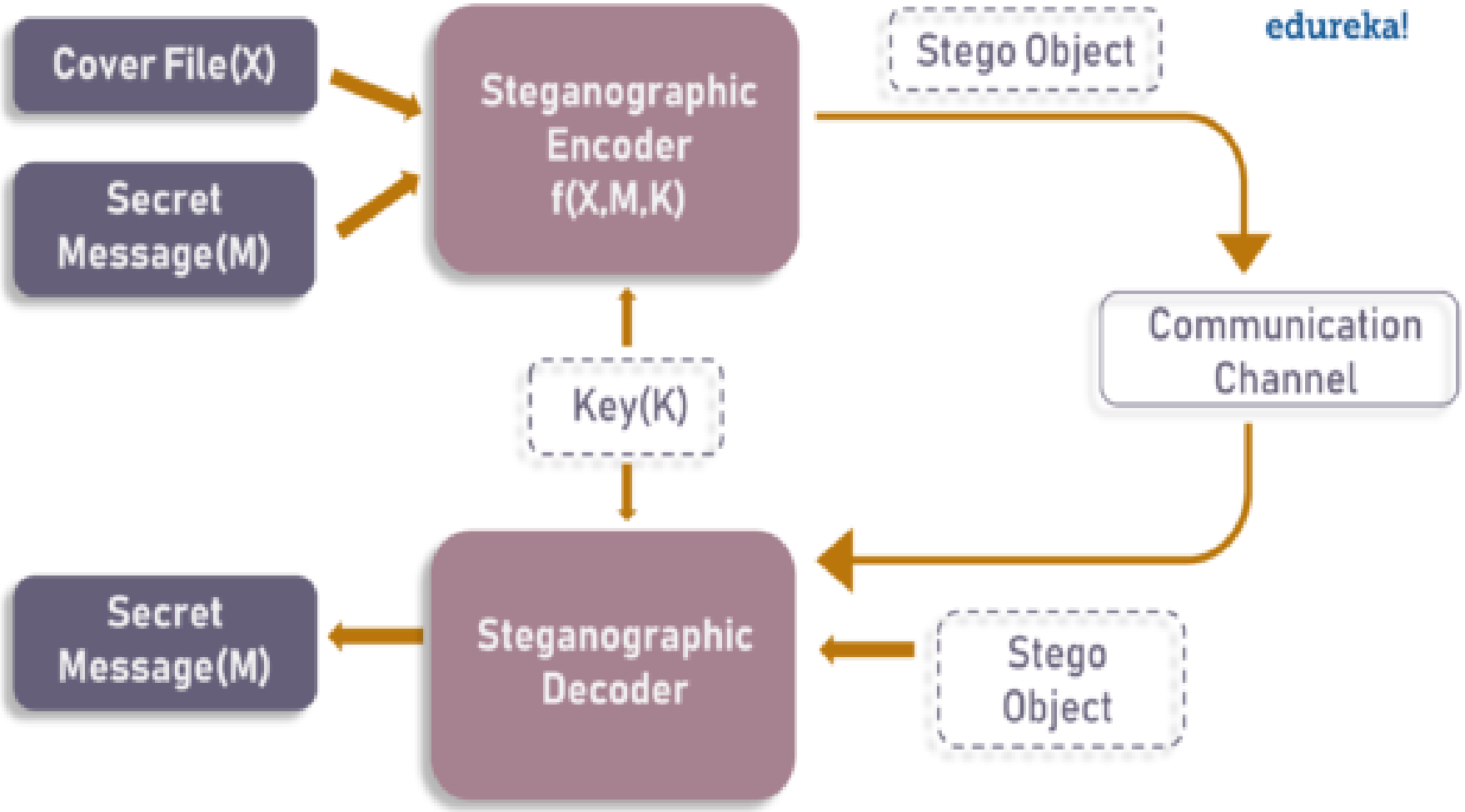
Steganography is the technique of hiding secret data within an ordinary, non-secret, file or message in order to avoid detection; the secret data is then extracted at its destination.

The use of steganography can be combined with encryption as an extra step for hiding or protecting data.

What is Steganography?

Steganography is the art and science of embedding secret messages in a cover message in such a way that no one, apart from the sender and intended recipient, suspects the existence of the message

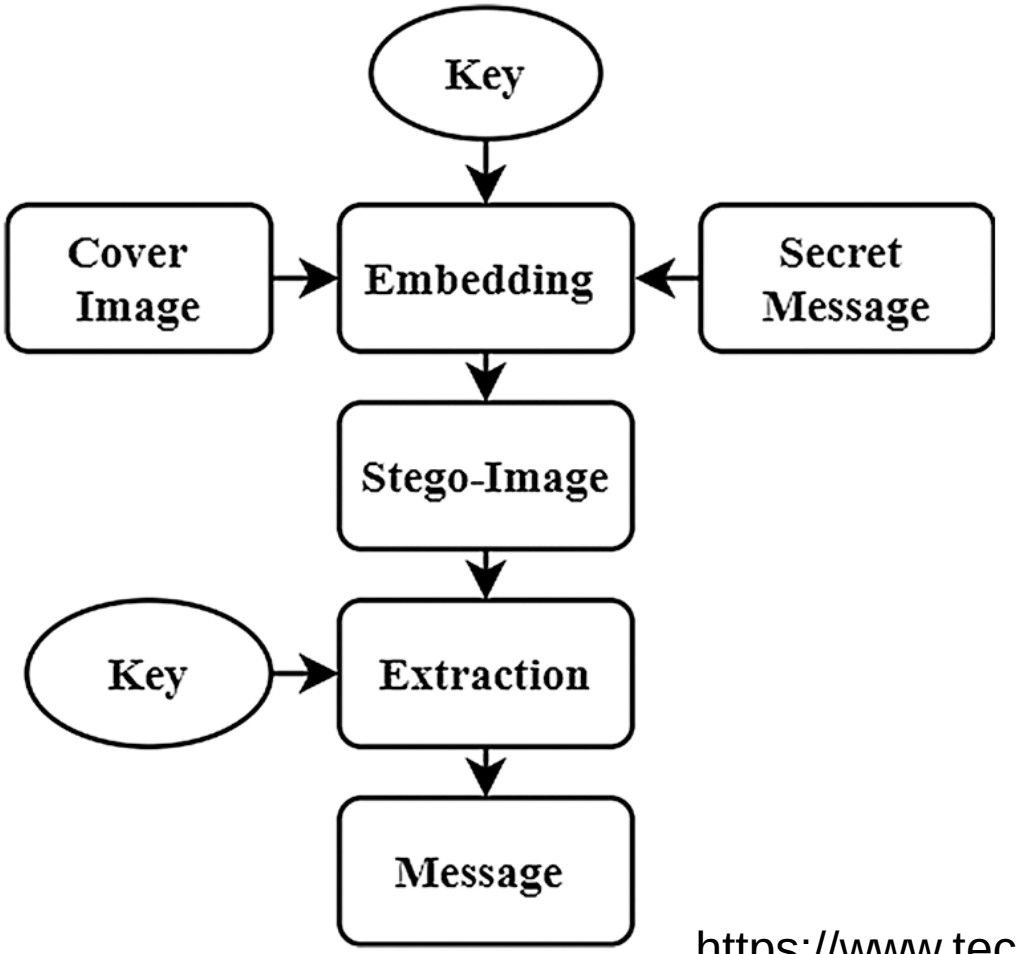
Basic Steganographic Model.



Steganography Techniques

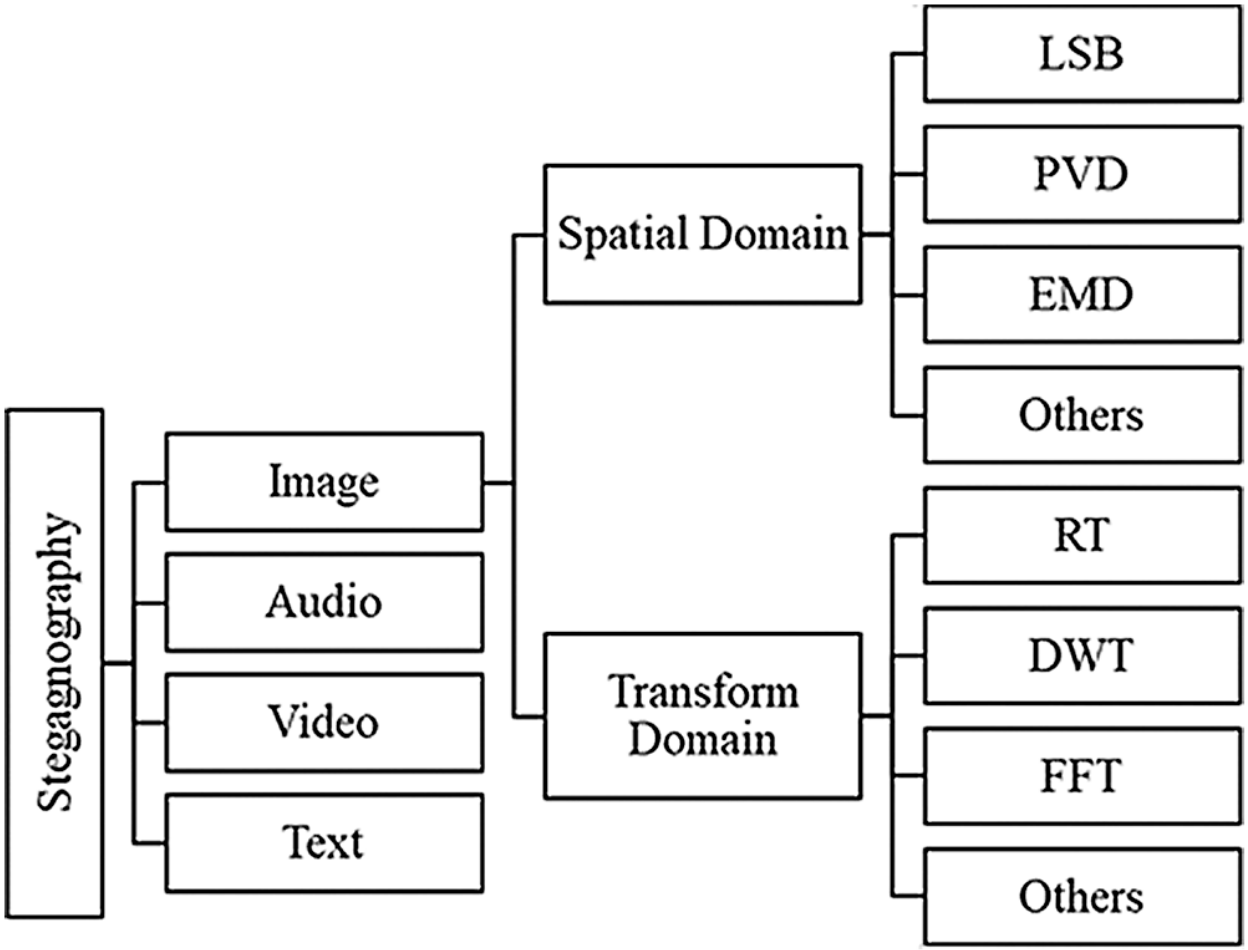
1. Text Steganography
2. Image Steganography
3. Video Steganography
4. Audio Steganography
5. Network Steganography

Image steganography steps



https://www.techscience.com/cmc/v68n3/42497/html

Classification of steganography techniques



Steganography different from Cryptography ?

	STEGANOGRAPHY	CRYPTOGRAPHY
Definition	It is a technique to hide the existence of communication	It's a technique to convert data into an incomprehensible form
Purpose	Keep communication secure	Provide data protection
Data Visibility	Never	Always
Data Structure	Doesn't alter the overall structure of data	Alters the overall structure of data
Key	Optional, but offers more security if used	Necessary requirement
Failure	Once the presence of a secret message is discovered, anyone can use the secret data	If you possess the decryption key, then you can figure out original message from the ciphertext

Question Bank

1. What is the OSI security architecture?
2. What is the difference between passive and active security threats?
3. List and briefly define categories of passive and active security attacks.
4. List and briefly define categories of security services.
5. List and briefly define categories of security mechanisms.
6. What are the essential ingredients of a symmetric cipher?
7. What are the two basic functions used in encryption algorithms?
8. How many keys are required for two people to communicate via a cipher?
9. What is the difference between a block cipher and a stream cipher?
10. What are the two general approaches to attacking a cipher?

Question Bank

11. List and briefly define types of cryptanalytic attacks based on what is known to the attacker.
12. What is the difference between an unconditionally secure cipher and a computationally secure cipher?
13. Briefly define the Caesar cipher.
14. Briefly define the monoalphabetic cipher.
15. Briefly define the Playfair cipher