Lecture 12

Public versus Private Watermarking

I. Public digital watermark can be detected and read by anyone not having access to certain secret information where the private watermark can be detected and read by someone who has access to an appropriate detected software with certain secret information.

II. The private watermark/stegano renders the detection of the watermark difficult or impossible without the secret information

III. The private watermark only allows someone who has the ownership secret information to view the content.

IV. Private watermarking scheme can be used to only to demonstrate ownership of the content once its owner discovers its illicit use.

V. Private watermarking technique requires the original or a reference image in the watermarking detection procedure are less suitable for such applications.

VI. The public watermarking technique are attractive for many applications since it allows many tools to perform identity check.

Open Questions.

1. Give **THREE(3)** new ideas on practical uses of public watermarks
   Light background ambient natural sounds which add intrinsic value to cover media.
   Add a reference address link to original content
   Background light movement or motion, motion JPEG.

2. Give an offensive idea to watermarking technique in an unchartered territory.
   Add a viral code to a watermark
   Add an advertisement link to a media.
   Add a virus to a large song/video.

   Multimedia Security
   Security = Watermarking + Encryption
   Light Watermarking + Robust Watermarking
   Light Watermarking + Full Encryption

Warden Theory

A scenario in Prison

Bob goes into jail. Alice is his wife. Bob is a rich criminal. Alice will always try to communicate with Bob under covert channel by sending images and audio message through watsapp. The wifi channel is being observed by the warden called Eve. The warden has an assistant, a spy scanner called Wendy.

If the warden Eve thinks that Alice's watsap to Bob is innocuous/clear, she may simply forward it to Bob.

Alternatively, Eve may intentionally distort the content (e.g., apply lossy compression or strong compression to the image and audio/voice file) in the hope that such a distortion will remove any secret message that just might be present.

If the warden Eve thinks Alice's message to Bob hides a covert communication, then she may block the communication/watsapp entirely and hide behind wifi service interruption.

Naturally, Eve cannot block the watsap service entirely due to serious complain from the inmate family group.

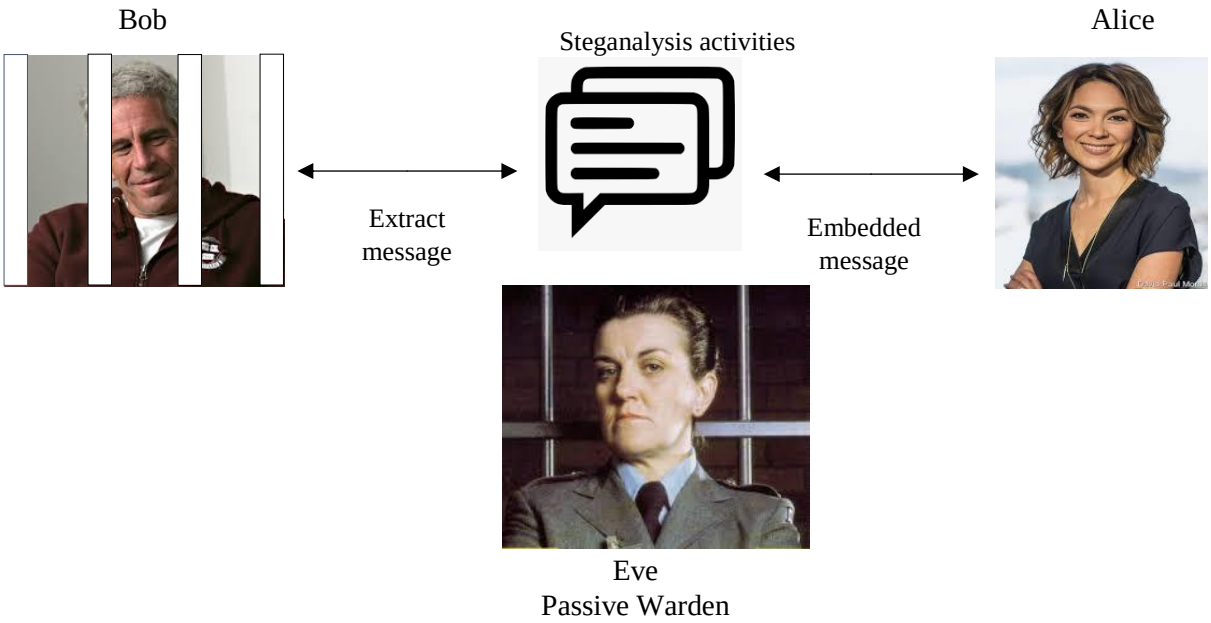
Give 3 typical scenario under Passive, Active and Malicious warden.

Passive Warden

i. The warden is called passive if she is restricted from modifying the content sent by Alice prior to receipt by Bob (i.e., the warden can only prevent or permit delivery of Alice's message).
ii. In this scenario, the warden Eve tests each communication from Alice for the presence of a covert message and if the warden's test is negative, the communication is relayed to Bob, otherwise it is blocked.
iii. This passive mode is the most commonly assumed scenario and why most steganographic algorithms are not designed to be robust unlike watermarking algorithm.

a. The warden Eve will let or block the watsap service only.
b. There is no Wendy to check, distort or change the content of the watsap messages.
c. Eve cannot afford to buy a program to detect any stega message …

d. She can download a free steganography detection software.
e. In this typical scenario, a steganographic algorithm reachable to Bob is not designed to be robust.



Active Warden

i. Bob is a millionaire. The warden Eve is called active if she intentionally modifies the content sent by Alice prior to resending to Bob.
ii. In this scenario, the warden Eve may not be entirely confident or competent of her steganalysis program.
iii. Thus, even though her tests are negative, the warden may alter the content, hoping that the modification will destroy any steganographic message that might be present.
iv. The types of modification an active warden might apply include lossy recompression of images and audio clips, low-pass filtering, and other procedures that slightly degrade the content.

a. Eve is an active observer of the watsap/telegram/IM/IRC-Internet Relay Chat channel.
b. Eve hires a new graduate Wendy from UTeM to modify the content sent by Alice prior to receipt by Bob.
c. Wendy may apply lossy recompression of images and audio clips, low-pass filtering, add noise to every image and video content and other procedures that slightly degrade the content.

Suppose you are applying for a job as Wendy:

Sample Question: In a job interview for Wendy, as a new graduate from UTeM, What can you do to assist Eve with minimum budget?

Audio Processing

Today, a voice message via watsapp is popular. It is almost free in verbal mode with acceptable/bearable delay.

Give **FIVE(5)** operations that you can do in assisting Eve.

Wendy can compress and decompress such as using MP3 encoder and decoder on an audio object.

Wendy can apply low pass filtering on an audio object to erase any message embedded within high frequency signals.

Wendy can add noise to an audio object.

Wendy can detect and delete any echoes within to an audio object.

Wendy can apply any frequency/wavelet transform and delete some coefficients then take its inverse to an audio object.

Image Processing

Today, it is common to send an image via a watsapp/telegram.

Give **FIVE(5)** operations that you can do in assisting Eve.

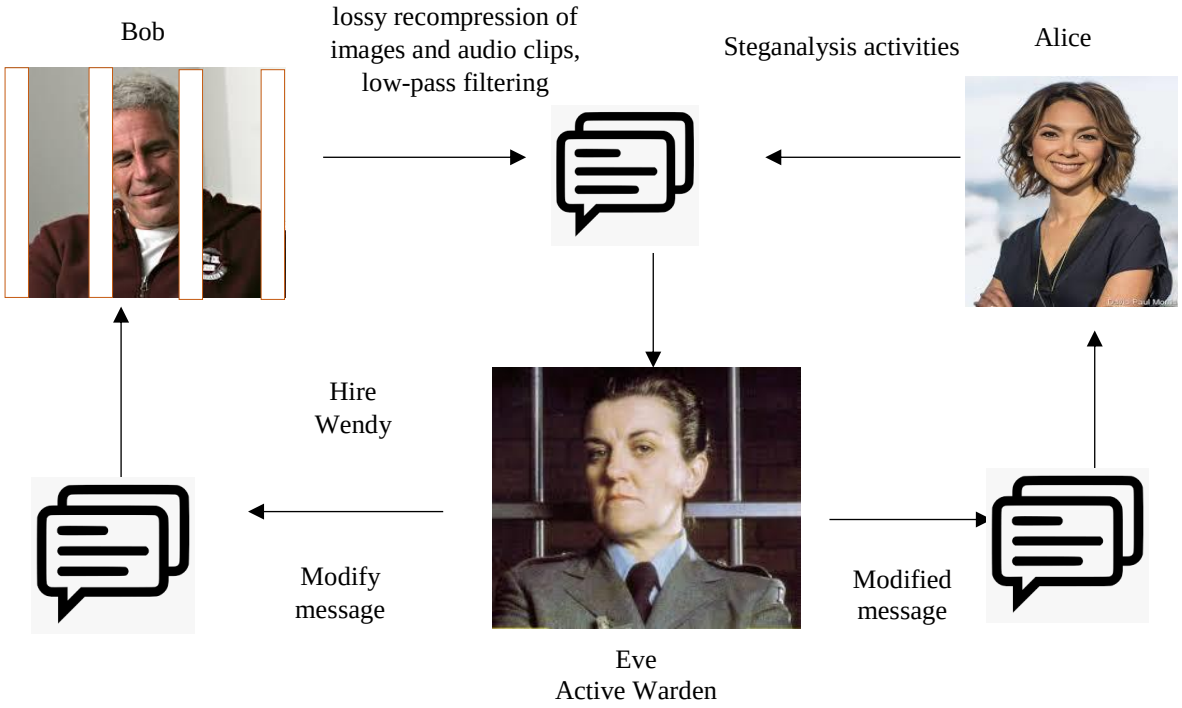
Wendy can compress and decompress via JPEG with higher quantization tables on an image object.

Wendy can apply low pass filtering on an image object to erase any message embedded within high frequency signals.

Wendy can add noise to an image object.

Wendy can detect and delete any echoes within to an image object.

Wendy can apply any frequency/wavelet transform and delete some coefficients then take its inverse to an image object.



Malicious Warden

i. Bob is a billionaire. Eve is well funded. Eve can hire a researcher Wendy(a Phd student).
ii. Eve is in full control of internet service and wifi communication channels.
iii. The warden is called malicious if her actions are based on the specifics of the steganographic scheme and are aimed at catching the prisoners communicating secretly.
iv. This may include Wendy trying to impersonate as Alice or Bob or otherwise tricking them.
v. A malicious warden is usually considered in public-key steganography, where in this scenario, the stego key is known and anyone can extract the secret message.

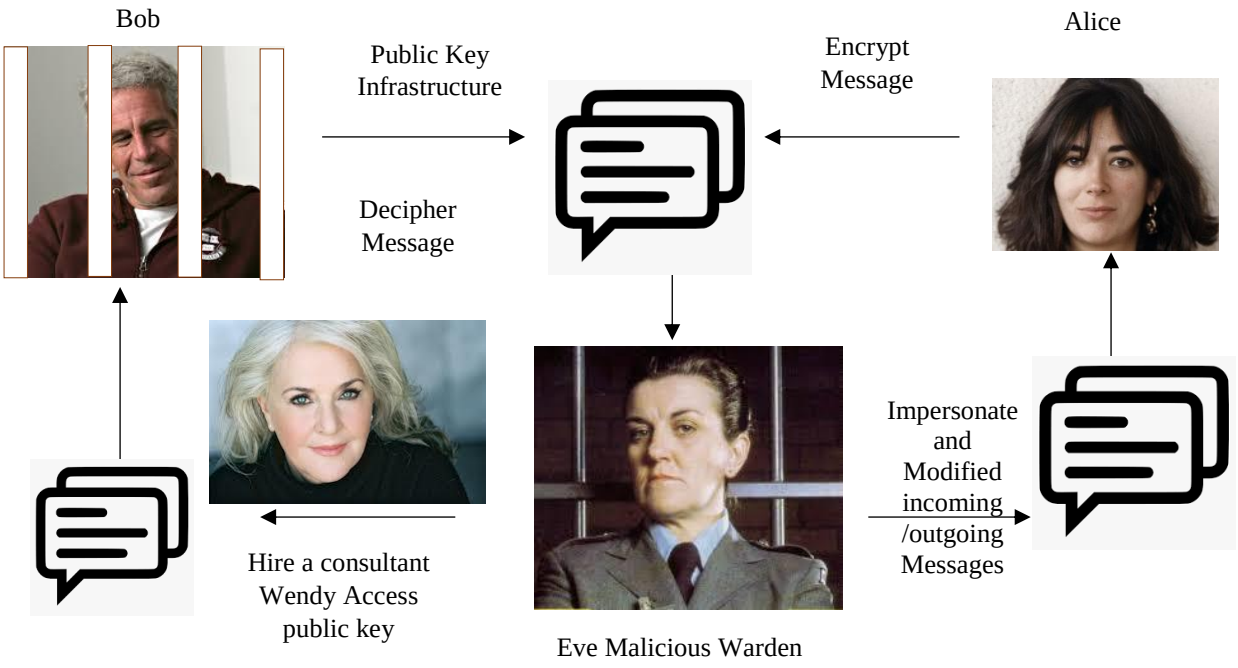
However, the message is encrypted using a public-key cryptosystem where only those who possess Bob's private key can decipher Alice's message.

Eve will observe and open a channel certain cryptographic services. However, the message is encrypted using a public-key cryptosystem where only those who possess Bob's private key can decipher Alice's message.

Even though the stego key is known, it is difficult to distinguish between an encrypted message and a random bit sequence extracted from a cover Work.

Nevertheless, since the Warden also knows the stego key, she has more options to attack the stego system.

a. Since Bob is known to save a lot of money, Eve is very determined to catch the prisoner's asset communicating secretly.
b. Wendy may impersonate and send a watsap to Bob as Alice from a network computer.
c. Eve also hire a consultant from UTeM on the matter of public-key steganography. Wendy has all the access to the public keys.



Open Question:
You are applying a short term contract job from Eve. Give **FIVE(5)** recommendation from your skill and capabilities to observe/catch Bob.
I can interact with Alice from outside.
I can impersonate as Bob's friend/accomplish.
I can send a Trojan to Bob's smart phone.
I can install a scanner to catch Bob's password.
I can threat Bob or make it appear as if I already kidnap Alice for ransom.
I will open a channel to a certain cryptographic service and lure Bob to use it and observe to catch Bob use/installation of the cryptographic service.

Write **FIVE(5)** criteria on a short job description a malicious Eve need to advertise for RM10K job to hire Wendy?

The person must be able to hack a smartphone.
The person must be able to catch someone's password.
The person must be able to send a watsap on other people's behalf.
The person must be able to make a deep fake video as Bob's friend.
The person must be able to imitate true caller ID as Bob's friend.