Multimedia Security and Privacy

TP5: Watermark performance evaluation

Prof. Sviatoslav Voloshynovskiy,
Roman Chaban <roman.chaban@unige.ch>,
Denis Ullmann <denis.ullmann@unige.ch>.

Stochastic Information Processing Group

May 6, 2021

UNIVERSITÉ DE GENÈVE
FACULTÉ DES SCIENCES
Département d'informatique

SIP stochastic information processing

Submission

Please archive your report and codes in "Name_Surname.**zip**" (replace "Name" and "Surname" with your real name), and upload to "`Assignments/TP5: Watermark performance evaluation`" on `https://moodle.unige.ch` before Wednesday, May 19 2021, 23:59 PM. Note, **the assessment is mainly based on your report, which should include your answers to all questions and the experimental results**.

In this TP work you will assess the performance of the watermark detection model that was build in the previous TP.

1 Non-blind watermark detection

1.1 Exercise

Read the image `cameraman.tif` in. It will serve as host image $\mathbf{x}$.
For given hypothesis:

$$\begin{cases} H_0: & \mathbf{v} = \mathbf{x} + \mathbf{z} \\ H_1: & \mathbf{v} = \mathbf{x} + \mathbf{w} + \mathbf{z} \end{cases}$$

where $\mathbf{x}$ is the host image, $\mathbf{v}$ is the marked image, $\mathbf{w}$ is the watermark and $\mathbf{z}$ is additive white Gaussian noise, i.e. $\mathbf{Z} \sim \mathcal{N}(\mathbf{0}, \sigma^2_{\text{noise}}\mathbf{I})$

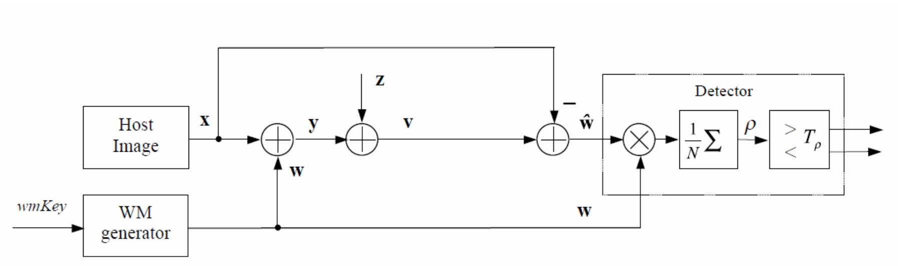

Figure 1 – Non-blind watermark detection

1.2 Exercise

1. Fill out Table 1 with all results, where $\mu_{\rho|H_0}$, $\sigma_{\rho|H_0}$, $\mu_{\rho|H_1}$ and $\sigma_{\rho|H_1}$ are the means and variances of the linear correlation ρ under hypothesis H_0 and H_1 for J realizations each. They can be ascertained as follows:

$$\mu_{\rho|H_0} = \frac{1}{J}\sum_{k=1}^{J}\rho_k^{H_0} \tag{1}$$

$$\mu_{\rho|H_1} = \frac{1}{J}\sum_{k=1}^{J}\rho_k^{H_1} \tag{2}$$

$$\sigma^2_{\rho|H_0} = \frac{1}{J}\sum_{k=1}^{J}\left(\rho_k^{H_0} - \mu_{\rho|H_0}\right)^2 \tag{3}$$

$$\sigma^2_{\rho|H_1} = \frac{1}{J}\sum_{k=1}^{J}\left(\rho_k^{H_1} - \mu_{\rho|H_1}\right)^2 \tag{4}$$

   Obviously, ρ^{H_0} and ρ^{H_1} need to be experimentally obtained. Note that only the noise and not the watermark has influence on hypothesis H_0, so the relevant cells have been grayed out.

   - For hypothesis H_0, ρ^{H_0} is determined $J = 100$ times, $k = \{1...J\}$ for noise realizations $\mathbf{z}$ with a fixed $\sigma_{\text{noise}} = 50$.
   - For hypothesis H_1 and ρ^{H_1} the watermark $\mathbf{w}$ is generated J times with a fixed strength $\gamma = \pm 1$ and a fixed density $\theta_N = 0.1$. The noise realization $\mathbf{z}$ is again fixed with $\sigma_{\text{noise}} = 50$.

2. What can you conclude about *non-blind* watermark detection given the strength of the watermark and the noise variance?

	$\sigma_{\text{noise}} = 50$				$\sigma_{\text{noise}} = 100$			
	$\theta_N = 0.1$		$\theta_N = 0.3$		$\theta_N = 0.1$		$\theta_N = 0.3$	
	$\gamma = \pm 1$	$\gamma = \pm 5$	$\gamma = \pm 1$	$\gamma = \pm 5$	$\gamma = \pm 1$	$\gamma = \pm 5$	$\gamma = \pm 1$	$\gamma = \pm 5$
$\mu_{\rho\|H_0}$								
$\sigma^2_{\rho\|H_0}$								
$\mu_{\rho\|H_1}$								
$\sigma^2_{\rho\|H_1}$								

Table 1 – Data for *non-blind* watermark detection

3. The detection threshold is denoted with $T_{\rho\text{ non-blind}}$, for each set of parameters, evaluate the following *numerically* for the non-blind detection shown in Figure 1 with $J = 100$ realizations of each hypothesis H_0 and H_1:

   - p_f, the probability of false alarm
   - p_m, the probability of miss
   - p_d, the probability of correct detection, defined as $1 - p_m$

   and plot the estimated curves of these probabilities as functions of $T_{\rho\text{ non-blind}}$.

4. Display the Receiver Operating Characteristic (ROC) curve of p_m VS p_f for the binary threshold test following the above mentioned experiment set up. The detection threshold is denoted with $T_{\rho\text{ non-blind}}$.

2 Blind watermark detection using the Maximum Likelihood estimate

This exercise will follow the same structure and tests as the previous one for *non-blind* watermark detection, except that this time you will *blindly* detect the watermark using the Maximum Likelihood estimate of $\mathbf{x}$ used in previous TP.

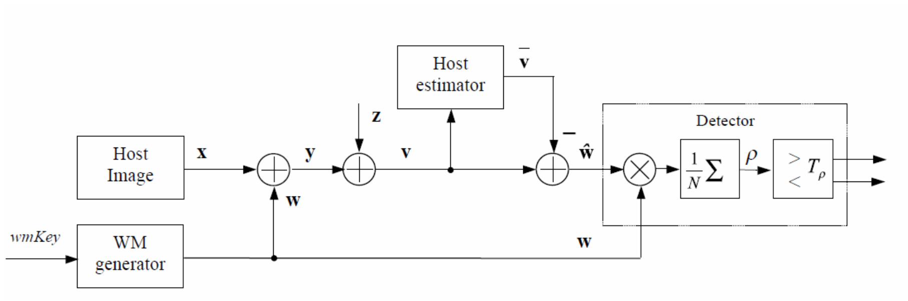

Figure 2 – Blind watermark detection

2.1 Exercise

For given hypothesis:

$$\begin{cases} H_0: & \mathbf{v} = \mathbf{x} + \mathbf{z} \\ H_1: & \mathbf{v} = \mathbf{x} + \mathbf{w} + \mathbf{z} \end{cases}$$

where $\mathbf{x}$ is the host image, $\mathbf{v}$ is the marked image, $\mathbf{w}$ is the watermark and $\mathbf{z}$ is additive white Gaussian noise, i.e. $\mathbf{Z} \sim \mathcal{N}(\mathbf{0}, \sigma^2_{\text{noise}}\mathbf{I})$,

1. Fill out Table 2 with all results. with all results. Again note that obviously only the noise and not the watermark has influence on hypothesis H_0, so the relevant cells have been grayed out.

2. What can you conclude about *blind* watermark detection given the strength of the watermark and the noise variance?

	$\sigma_{\text{noise}} = 50$				$\sigma_{\text{noise}} = 100$			
	$\theta_N = 0.1$		$\theta_N = 0.3$		$\theta_N = 0.1$		$\theta_N = 0.3$	
	$\gamma = \pm 1$	$\gamma = \pm 5$	$\gamma = \pm 1$	$\gamma = \pm 5$	$\gamma = \pm 1$	$\gamma = \pm 5$	$\gamma = \pm 1$	$\gamma = \pm 5$
$\mu_{\rho\|H_0}$								
$\sigma^2_{\rho\|H_0}$								
$\mu_{\rho\|H_1}$								
$\sigma^2_{\rho\|H_1}$								

Table 2 – Data for *blind* watermark detection

3. Evaluate *numerically* p_f, p_m and p_d using the same conditions as for the previous task and plot them as functions of $T_{\rho\text{ blind}}$.

4. Calculate and display the Receiver Operating Characteristic (ROC) curve of p_m VS p_f for the binary threshold test.

2.2 Exercise

Compare the ROC curves from the *non-blind* and *blind* watermark detection schemes. What can you conclude about their comparative performance?