Université de Genève

Multimedia Security and Privacy
14x016

TP 5 : Watermarking Perfomance and evaluation

Author: Deniz Sungurtekin

E-mail: Deniz.Sungurtekin@etu.unige.ch

May 2021

UNIVERSITÉ DE GENÈVE
FACULTÉ DES SCIENCES
Département d'informatique

1 Introduction

In this work, we will asses the performance of the watermark detection model build in the previous work (Watermarking detection). To do so, we will assume two hypothesis:

H_0 where the marked image is only define by x + z, x is the original image:

Figure 1: Original image

and z an additive white Gaussian noise.

H_1 where the marked image is only define by x + z + w, w is a watermark with uniform distributed value with a given magnitude.

So, with H_0 there is no watermark and with H_1 we have a watermark. First, we will see the performance of the watermark detection by a non-blind detection where we have access to the host image to estimate the watermark. To do this, we will compute the mean and standard deviation of the correlation with different set of parameters. Then, we will try different threshold value and observe the resulting probabilities of false alarm and miss. Finally, we will display the ROC curve for the binary threshold test.

In the second part, we will use the same methodology but we will estimate the watermarking blindly by estimating the host image by computing the local mean of the marked image v.

2 Non-blind watermark detection

First, we will compute the mean and standard deviation of the linear correlation under hypothesis H_0 and H_1 for 100 realisations each:

	$\sigma_{\text{noise}} = 50$				$\sigma_{\text{noise}} = 100$			
	$\theta_N = 0.1$		$\theta_N = 0.3$		$\theta_N = 0.1$		$\theta_N = 0.3$	
	$\gamma = \pm 1$	$\gamma = \pm 5$	$\gamma = \pm 1$	$\gamma = \pm 5$	$\gamma = \pm 1$	$\gamma = \pm 5$	$\gamma = \pm 1$	$\gamma = \pm 5$
$\mu_{\rho\|H_0}$	-0.298				0.028			
$\sigma^2_{\rho\|H_0}$	0.039				0.090			
$\mu_{\rho\|H_1}$	1.074	24.79	1.023	25.28	1.09	26.67	1.03	25.15
$\sigma^2_{\rho\|H_1}$	0.004	0.104	0.002	0.043	0.019	0.39	0.005	0.85

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

where σ is the standard deviation of our white Gaussian noise, θ the density of the watermark and γ the magnitude of our uniform distribution.

Globally the more the standard deviation of the noise is big the less are the chance to obtain the max correlation value which is γ^2 because even by subtracting the original image to the marked image the noise will remain. Also, the variance of the correlation will generally be bigger because of the bigger value of the noise. In regards of the watermark's strength, it defines the range of the obtained correlation given by the mean of the squared value of the watermark. However, it has no impact on the correlation obtained with hypothesis H_0 because there is no watermark in the image. Also, we can see that the mean and variance of the correlation value are very good under H_1 which shows a good approximation of the watermark.

We will evaluate the following numerically for the non-blind detection with J = 100 realizations of each hypothesis and plot the estimated curves of these probabilities as functions of a threshold.

Here are the value for the different set of parameters:

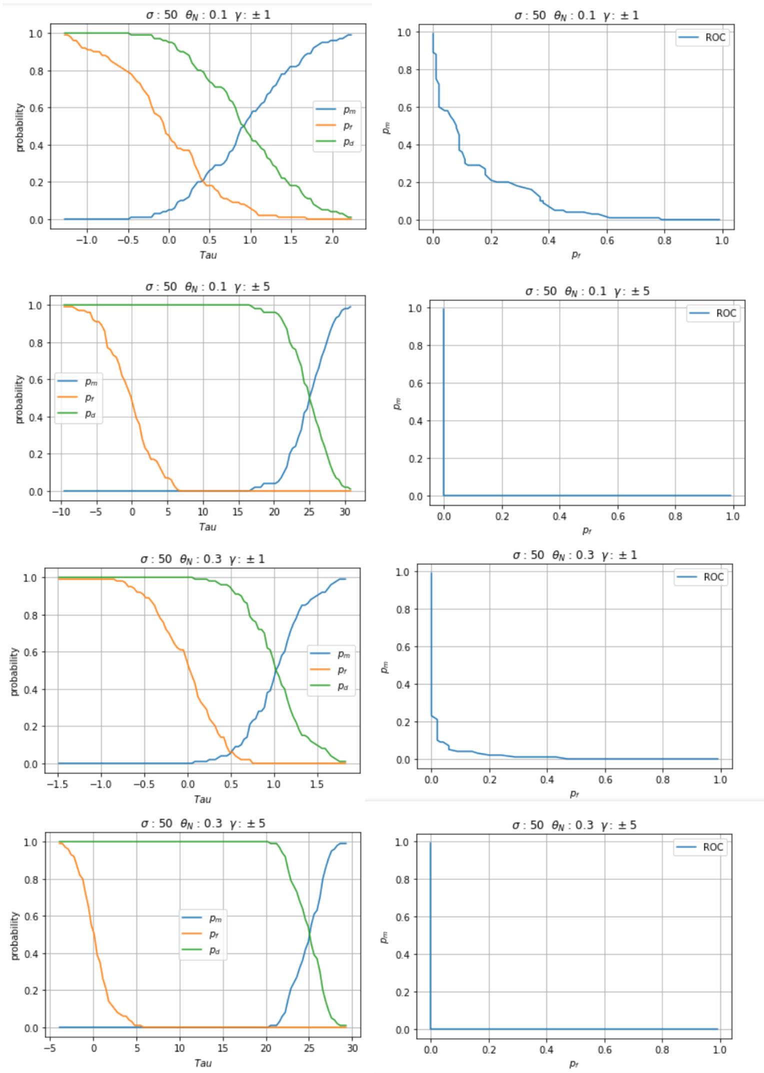

Figure 2: Sigma 50

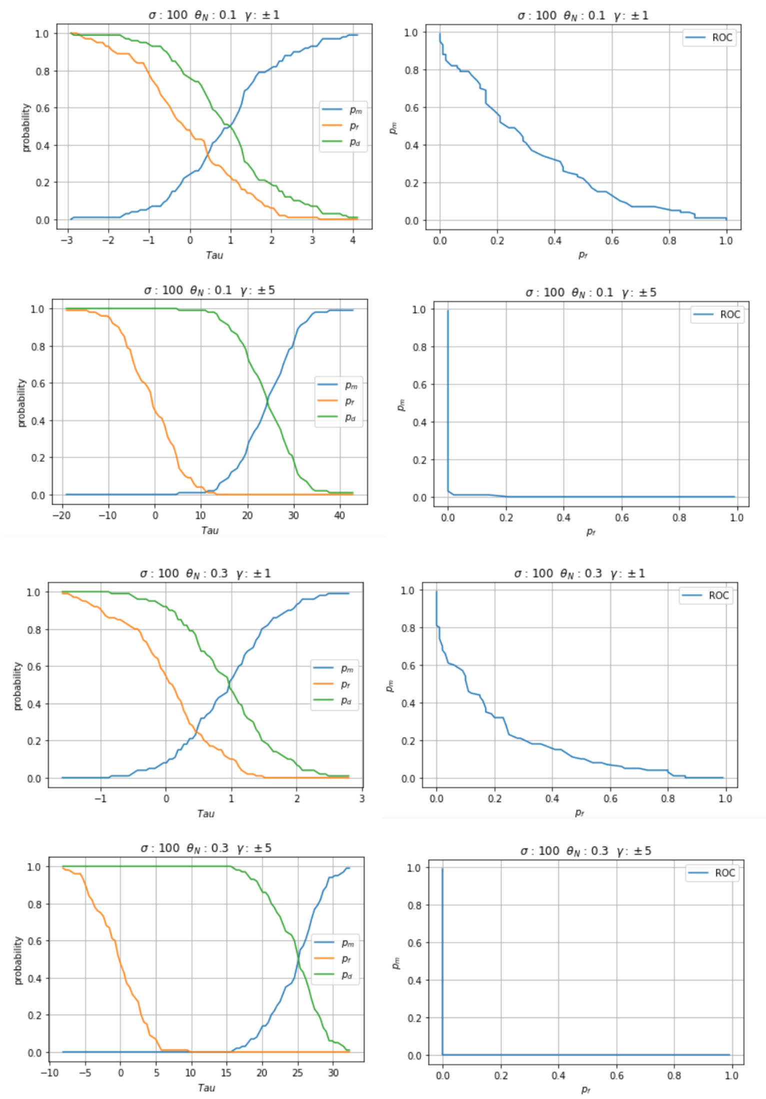

Figure 3: Sigma 100

3 Blind watermark detection using maximum likelihood

Now, we will compute the mean and standard deviation of the linear correlation under hypothesis H_0 and H_1 for 100 realisations each:

	$\sigma_{\text{noise}} = 50$				$\sigma_{\text{noise}} = 100$			
	$\theta_N = 0.1$		$\theta_N = 0.3$		$\theta_N = 0.1$		$\theta_N = 0.3$	
	$\gamma = \pm 1$	$\gamma = \pm 5$	$\gamma = \pm 1$	$\gamma = \pm 5$	$\gamma = \pm 1$	$\gamma = \pm 5$	$\gamma = \pm 1$	$\gamma = \pm 5$
$\mu_{\rho\|H_0}$	0.133				0.058			
$\sigma^2_{\rho\|H_0}$	0.054				0.036			
$\mu_{\rho\|H_1}$	0.85	22.63	0.89	21.99	0.88	23.07	0.854	22.10
$\sigma^2_{\rho\|H_1}$	0.006	0.159	0.001	0.031	0.017	1.24	0.019	0.106

Table 2 – Data for *blind* watermark detection

Obviously, because we don't have access to the host image, the correlation obtained under H_1 are less good as the estimated watermark is less accurate.

Here are the evaluation of the following numerically for the blind detection shown with J = 100 realizations of each hypothesis.

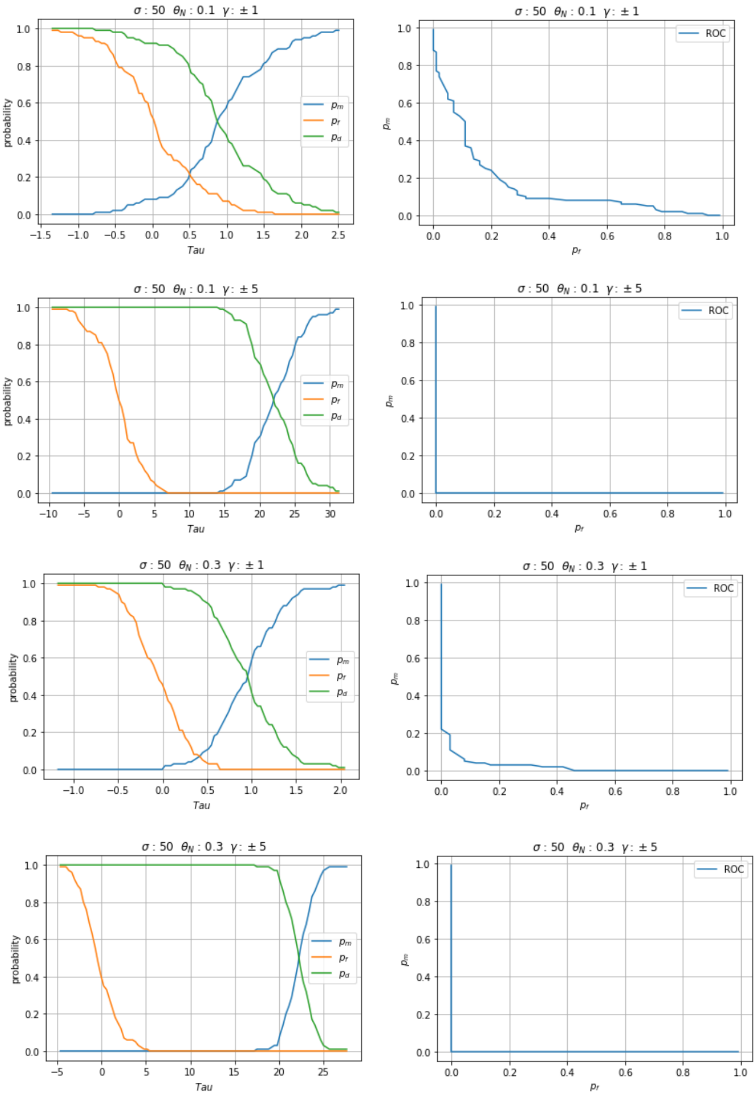

Figure 4: Sigma 50

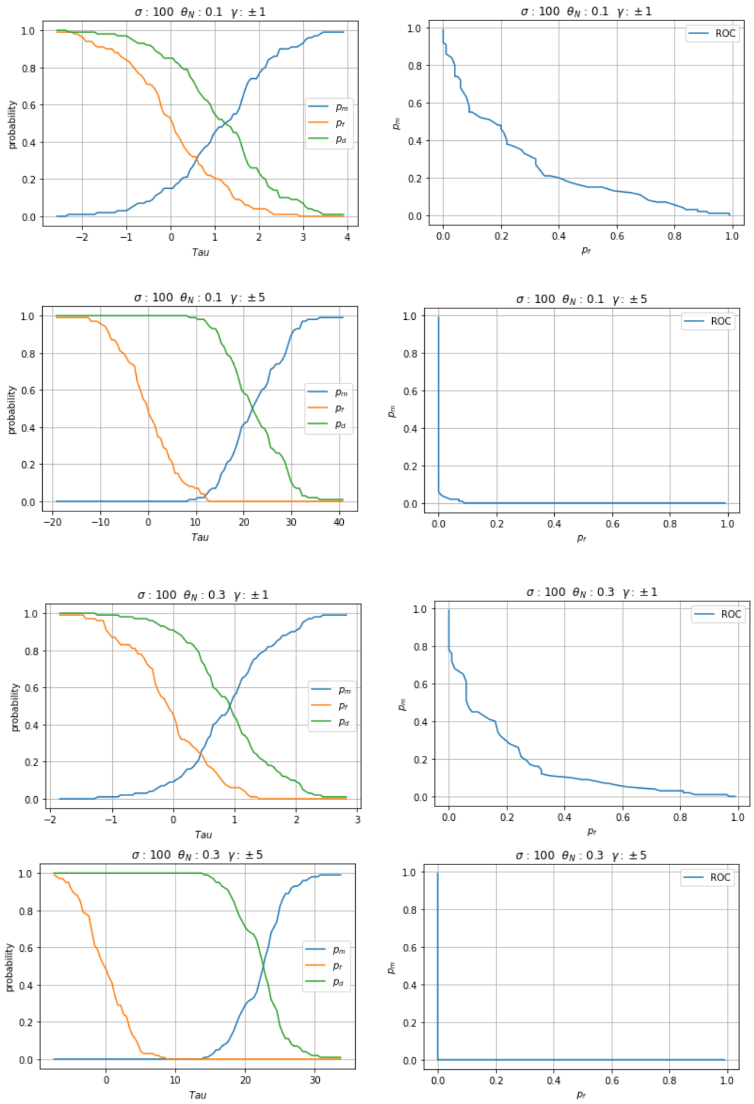

Figure 5: Sigma 100

Globally, the results are very similar for blind and non-blind detection, it is explained by the fact that even if we have a more accurate estimation of the watermark with non-blind detection, the correlations value under H_0 and H_1 are enough different to find a good threshold. The good thresholds are generating low value of false alarm probability and missing probability, the more their intersection is at a small value in the y axis the better it is.

Moreover, we can understand the impact of the parameters on the detection. Clearly, the more the watermark has a strong magnitude the best is our model because we have much bigger correlations value. In addition, the density have also a good effect on the model because it favors a better stability in the correlations since the uniform distribution have a mean of 0. However, the intensity of the noise isn't good since it remain in H_0, we have more variation in the correlations value which is not good to establish a good threshold.