Lecture 2. Embedding in the least significant bits

Model of CO:

pgm(grey *L*-scale image).

(typically *L* = 8 or 16 (for medical images)).

Presentation of n-th pixel luminance in binary base :

$$C(n)=\sum_{i=0}^{L-1} c_i(n)2^i,$$

where $c_i(n)$ - binary coefficients (0 or 1).

Example: $217 = 1\cdot 2^0 + 0\cdot 2^1 + 0\cdot 2^2 + 1\cdot 2^3 + 1\cdot 2^4 + 0\cdot 2^5 + 1\cdot 2^6 + 1\cdot 2^7$

$c_0 \quad c_1 \quad c_2 \quad c_3 \quad c_4 \quad c_5 \quad c_6 \quad c_7$

Embedding procedure (LSB - replacing)*:*

$$C_w(n)=\sum_{i=1}^{L-1} c_i(n)2^i + b(n),$$

where $b(n)$ - message bit (0 or 1) to be embedded in the n-th pixel.

Example: $C(n) = 21 = 00010101$

If $b(n)=0, C_w(n)=00010100=20$

If $b(n)=1, C_w(n)=00010101=21$

Extraction procedure : it is apparent if errors are absent.

Advantages of SG-LSB:
- Simple implementation.
- Small distortion of CO.
- It seems to be secure at single glance against its detection because LSBs are close to equally likely and they are looking as independent on other bits and pixels , whereas *b(n)* is also i.i.d. owing encryption procedure .
- It provides large embedding rate (1 bit per pixel).
- There exists an extension where secret information is embedded not in all pixels but in some of them which are determined by secret *stegokey* (but of course it decreases the embedding rate).

Defects of SG-LSB:
- It is not secure in fact (can be detected by more sophisticated methods than direct observation).
- Embedded information can be easily removed without significant distortion of CO by “randomization” of LSB in suspicious CO.

Improved SG-LSB:
We will consider in the sequel such SG-LSB which are less vulnerable to simple stegoanalysis (see Jsteg , F5 and Outguess).
SG-LSB described above are called *primitive SG-LSB*.

Methods of steganalysis for primitive SG-LSB:

1. Visual attack
2. First order statistical attack (*histogram-based* attack)
3. High order statistical attacks (in particular *sample pair analysis*)

Consider the main attacks.

1.Visual attack:

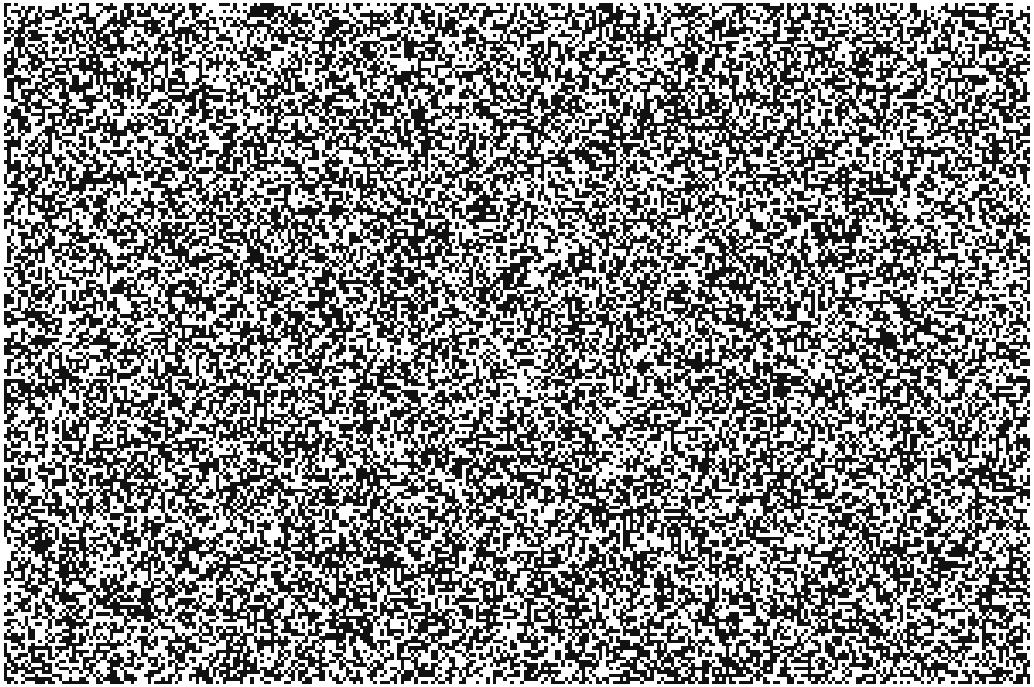
Transform grey scale image into black-white image by the rule:

$$C(n) = \begin{cases} \text{white if} & c_0(n) = 1; \\ \text{black if} & c_0(n) = 0; \end{cases}$$

Then if the an embedding is absent it results in visible contours of the original image; if it is not the case then we can see only noise area.

SG image with LSB embedding in every pixel

SG image above after its transform to binary image



SG image with embedding
in 50% randomly chosen pixels

SG image above after its
transform into binary image

SG image with embedding in 25% randomly chosen pixels

SG image above after its transform into binary image

SG image with embedding in 10% randomly chosen pixels

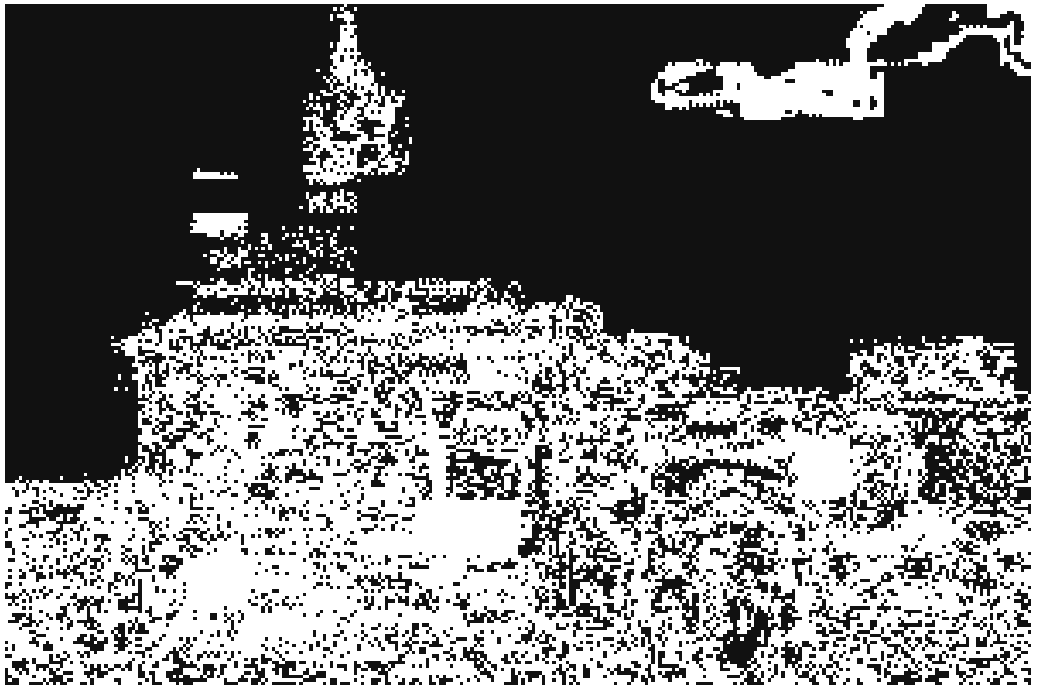
SG image above after its transform into binary image

SG image with embedding in 5% randomly chosen pixels

SG image above after its transform into binary image

Image without embedding

Image above after its transform into binary image



2.Histogram-based attack:

Definition. Image histogram is a distribution of luminances on all pixels of the image, that is:

$$V(i) = \frac{\#\{n : c(n) = i\}}{N}, \quad i = 1,2...L,$$

N – is the total number of pixels in the image;
L – the number of luminances.

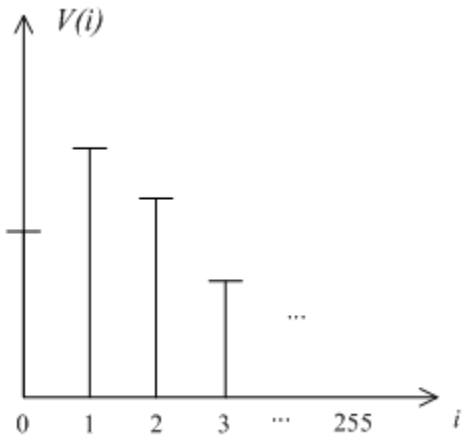
Properties of SG-LSB:

$$2i \begin{array}{l} \overset{0}{\rightarrow} 2i \\ \overset{1}{\rightarrow} 2i+1, \end{array} \qquad 2i+1 \begin{array}{l} \overset{1}{\rightarrow} 2i+1 \\ \overset{0}{\rightarrow} 2i, \end{array} \qquad 2i \not\rightarrow 2i-1, 2i+1 \not\rightarrow 2(i+1),$$

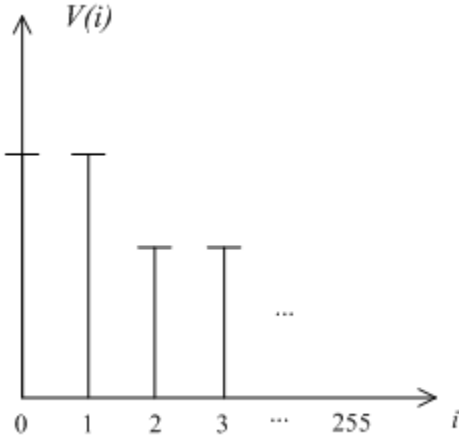
If we let that $P\{b(n)=0\} = P\{b(n)=1\} = 1/2,$ then

$$E\left(V_{SG}(2i)\right) = E\left(V_{SG}(2i+1)\right), \_ i = 0,1,...127,$$

thus we get the following histograms of $C(n)$ and $C_W(n)$:



a) Histogram of CO



b) Histogram of SG-LSB

Remark 1. Since in reality the embedded b*(n)* is not truly random value the histogram of SG image will differ from one shown in the Fig. b)

Remark 2. For embedding procedure with randomly chosen pixels with the probability *p* we get the following relation:

$$E\left(V_{SG}(2i)\right) = \frac{p}{2}\left(V_{CO}(2i) + V_{CO}(2i+1)\right) + (1-p)V_{CO}(2i)$$

$$E\left(V_{SG}(2i+1)\right) = \frac{p}{2}\left(V_{CO}(2i) + V_{CO}(2i+1)\right) + (1-p)V_{CO}(2i+1)$$

that results in inequality $E\left(V_{SG}(2i)\right) \neq E\left(V_{SG}(2i+1)\right)$ if p<<1.

Let us consider statistical criterion of SG-LSB detecting based on the proximity of neighbouring values of histogram : $V_{SG}(2i)$ and $V_{SG}(2i+1)$.

We let for simplicity that *p = 1* and consider so called χ^2 – *distribution* and corresponding to it χ^2 *test*. It is well known from the probability theory that if v_i, *i =1,2...*k,is a random vector for occurrences of some events with given probabilities p_1, $p_2 \ldots p_k$, then random value

$$\chi^2 = \sum_{i=1}^{k} \frac{(v_i - np_i)^2}{np_i}, n = v_1 + v_2 + \ldots + v_k$$

will have asymptotically *(n→∞)* so called χ^2 – distribution with *κ-1* degrees- of-freedom :

$$P\ \chi^2 \le x\ = \int_0^x \frac{1}{2^{\frac{k-1}{2}}\Gamma(\frac{k-1}{2})} x^{-\frac{k-1}{2}-1} e^{-\frac{x}{2}} dx,$$ where *Γ(·)* –is gamma function .

If we let $v_i = v_{SG}(2i)$, *i=0,1…(L-1)/2*. Then after LSB-based embedding we get :

$$p_i = \frac{1}{2}\left(V_{SG}(2i) + V_{SG}(2i+1)\right),$$

and χ^2 –statistic can be expressed as follows:

$$\chi^2 = \sum_{i=0}^{127} \frac{(V_{SG}(2i) - \frac{1}{2}\ V_{SG}(2i) + V_{SG}(2i+1)\ ^2}{\frac{1}{2}\ V_{SG}(2i) + V_{SG}(2i+1)} = \sum_{i=0}^{127} \frac{V_{SG}(2i) - V_{SG}(2i+1)\ ^2}{2\ V_{SG}(2i) + V_{SG}(2i+1)}.$$

χ^2 – criterion for SG-LSB detecting:

If $\chi^2 < \alpha$, then SG is presented,
If $\chi^2 \geq \alpha$, then SG is absent, where α is some threshold.
The probability of SG-missing can be calculated as follows:

$$P_m \leq \int_{\alpha}^{\infty} \frac{1}{2^{\frac{k-1}{2}}\Gamma(\frac{k-1}{2})} x^{-\frac{k-1}{2}-1} e^{-\frac{x}{2}} dx.$$

If P_m is given, then from relation above can be found the parameter α. A calculation of false alarm of SG presence P_{fa} can be performed by simulation of SG-LSB for different CO.

Image number	χ^2 for different probabilities of embedding					
	$P=1$	$P=0.5$	$P=0.1$	$P=0.05$	$P=0.01$	$P=0$
1	0.0003	0.1195	0.3909	0.4377	0.4751	0.4851
2	0.0005	0.1246	0.4009	0.4506	0.4873	0.5000
3	0.0003	0.1191	0.3827	0.4266	0.4654	0.4745
4	0.0005	0.1261	0.3983	0.4470	0.4871	0.4966
5	0.0004	0.1251	0.4034	0.4532	0.4880	0.4994

α		**0.49**	**0.48**	**0.47**	**0.45**	**0.43**	**0.40**	**0.37**	**0.30**	**0.15**	**0.10**
P_{fa}		0.34	0.29	0.22	0.14	0.10	0.07	0.05	0.04	0	0
$P=1$	P_m	0	0	0	0	0	0	0	0	0	0
$P=0.5$	P_m	0	0	0	0	0	0	0	0	0.02	0.88
$P=0.1$	P_m	0	0	0	0	0	0.35	0.81	0.95	0.99	1
$P=0.05$	P_m	0	0	0	0.20	0.72	0.87	0.94	0.95	1	1
$P=0.01$	P_m	0.17	0.66	0.72	0.81	0.89	0.93	0.93	0.96	1	1

3. Sample pair analysis attack:
(See S.Dumitrescu, et al, “Detection at LSB Steganography via Sample Pair Analysis”, LNCS 2578, pp.355-372,2003. [53])

Notations for 8-bits images:
C_0 – the number of pairs that coincide in the first 7 bits,
C_1 –the number of pairs that differ by value 1 in the first 7 bits ,
D_0 –the number of pairs that coincide in all bits ,
D_2 –the number of pairs that differ by value 2 ,
X –the number of *(2k, 2k-1)*-type pairs, where *k* is integer,
Y – the number of *(2k+1, 2k)*- type pairs, where *k* is integer.

Then an estimation of the probability of *p* can be found as a least real valued root of quadratic equation:

$$(2C_0 - C_1)P^2/4 - \frac{(2D_0 - D_2 + 2Y - 2X)P}{2} + Y - X = 0,$$

under the condition that $2C_0 > C_1$.

Example of histogram-based and sample pair-based steganalysis for typical 8-bits SG-LSB with the use of the image containing 256x256 pixels.

P	Value χ^2	Estimation of *P* by sample pair analysis
“0” (absence of SG)	60000	0
0.0005	59994	0.000426
0.01	58371	0.010237
0.05	53910	0.04949
0.1	48046	0.101321
0.5	15066	0.551201
1.0 (embedding in all pixels)	45	0.995306

LSB-Matching

Embedding:

$$C_w(n) = \begin{cases} C(n) \text{ if } b(n) = LSB(C(n)) \\ \left.\begin{array}{l} C(n)+1 \text{ with Prob.}1/2 \\ C(n)-1 \text{ with Prob.}1/2 \end{array}\right\} \text{if } b(n) \neq LSB(C(n)) \end{cases}$$

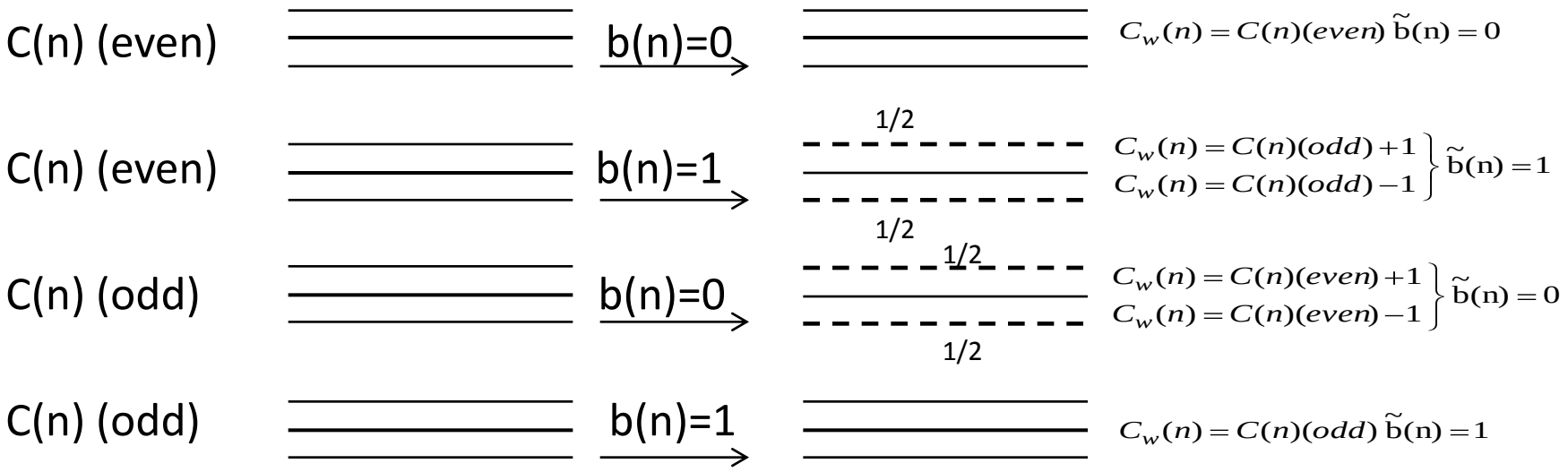
where b(n) is the n-th bit of the embedded message

Extracting:

$$\tilde{b}(k) = 0 \text{ if } C_w(n) \text{ is even } (\text{e.g. } LSB(C_w(n)) = 0)$$

$$\tilde{b}(k) = 1 \text{ if } C_w(n) \text{ is odd } (\text{e.g. } LSB(C_w(n)) = 1)$$

Verification of the extraction procedure:



Example of embedding

Image before embedding (CO)

Image after embedding in 50% randomly chosen (SG)

Steganalysis

Steganalysis methods:

- Histogram method
- Image calibration method
- Second-order functions method

Histogram method

Histogram is distribution of every brightness versus image pixels

$$h_c(n) = \left| \{ (i, j)\, p_c(i, j) = n \} \right|,$$

where $p_c(i, j)$ is brightness of pixel with coordinates (*i*, *j*).

For embedding modeled as independent additive noise, f_Δ its mass function is

$$\mathrm{h_s} = h_c \times f_\Delta$$

$$\mathrm{H_s(k)} = H_c(k) \cdot F_\Delta(k),$$

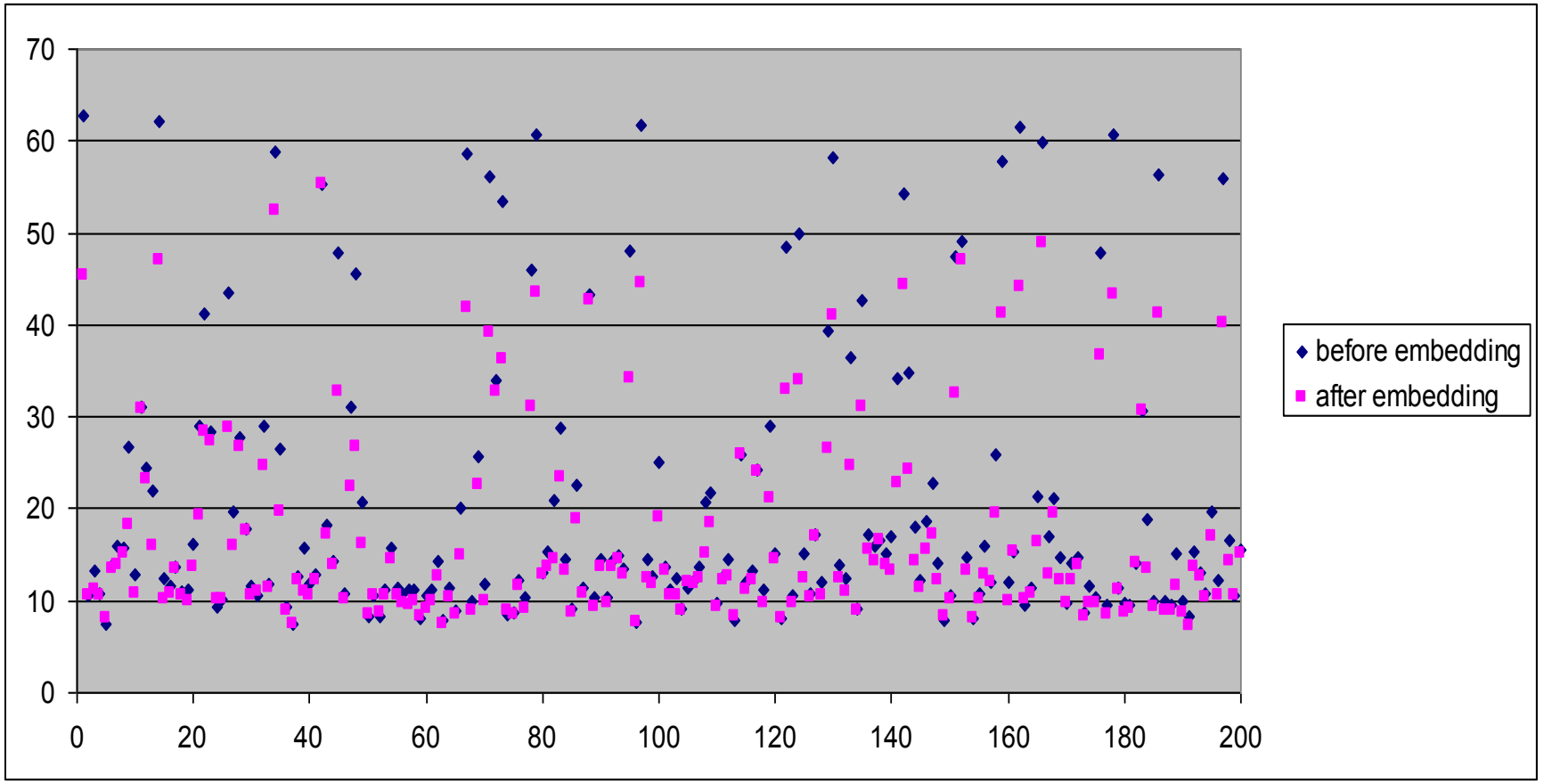
where $\mathrm{H_s}(k), H_c(k), \mathrm{F}_\Delta(k)$ is *N*-element discrete Fourier transform $h_s(n), h_c(n), f_\Delta(n)$
$\mathrm{H_s(k)}$ are HCF SGs

$$\mathrm{F_D}[k] = \cos^2(\rho k / N)$$

For center of mass (COM) of HCF one have $C(\mathrm{H[k]}) = \dfrac{\sum_{i=0}^{n} i\left|H[i]\right|}{\sum_{i=0}^{n} \left|H[i]\right|}$

After embedding $\mathrm{C(H_s[k]) < C(H_c[k])}$

Values of C(H[k]) before and after embedding for 200 images



Spread of C(Hc[k]) values is essential. Sometimes it can be greater than difference between C(Hc[k]) and C(Hs[k]).

Therefore we don’t see CO while detect the embedding and sequently we don’t know C(Hc[k]). This is a disadvantage of this method.

Image calibration

Now we turn to image calibration method taking into account the disadvantages of the histogram method.

In this method image size decrease of a kind $p_c^{/}(i,j)=\left|\sum_{u=0}^{1}\sum_{v=0}^{1}\frac{p_c(2i+u,2j+v)}{4}\right|$ is image calibration.

$p_c^{/}(i,j)$ is brightness of decreased image pixel with coordinates (*i*, *j*).

For images without embedding $C(H_c^{/}[k])\approx C(H_c[k])$

$$C(H_c[k])-C(H_s[k])>C(H_c^{/}[k])-C(H_s^{/}[k])$$

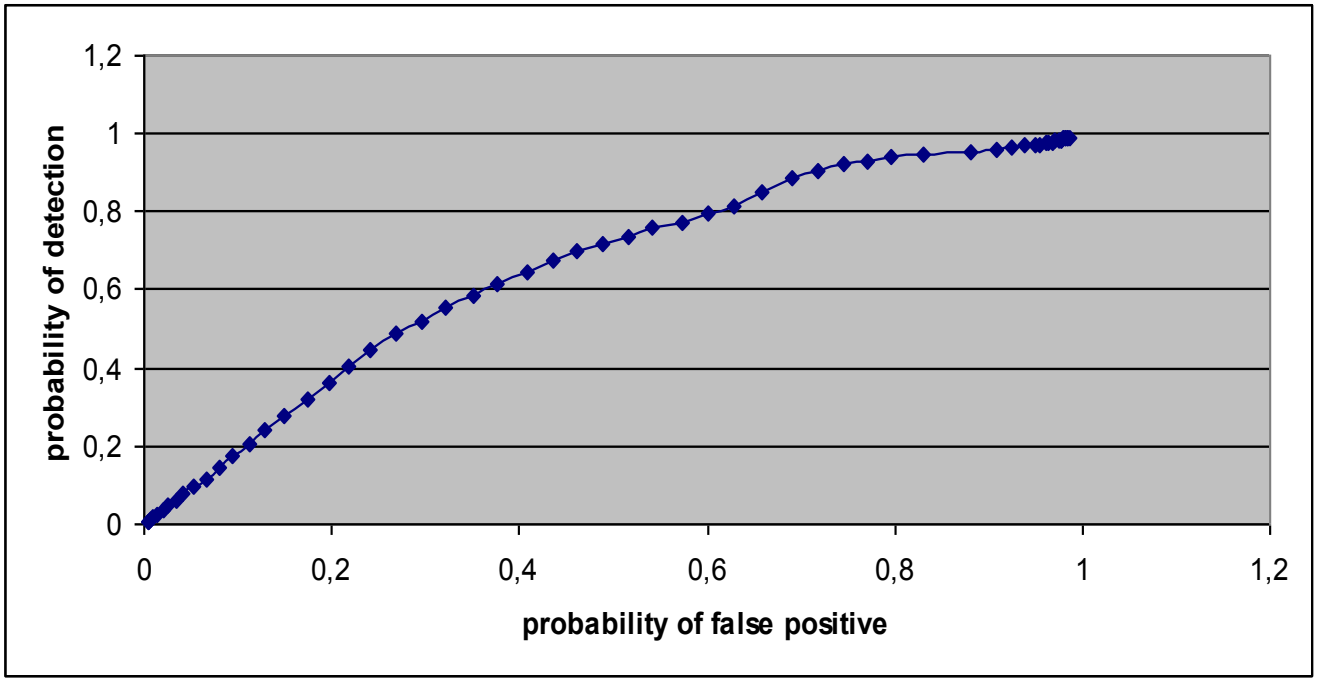
We shall carry out the statistical analysis combining two above formulas

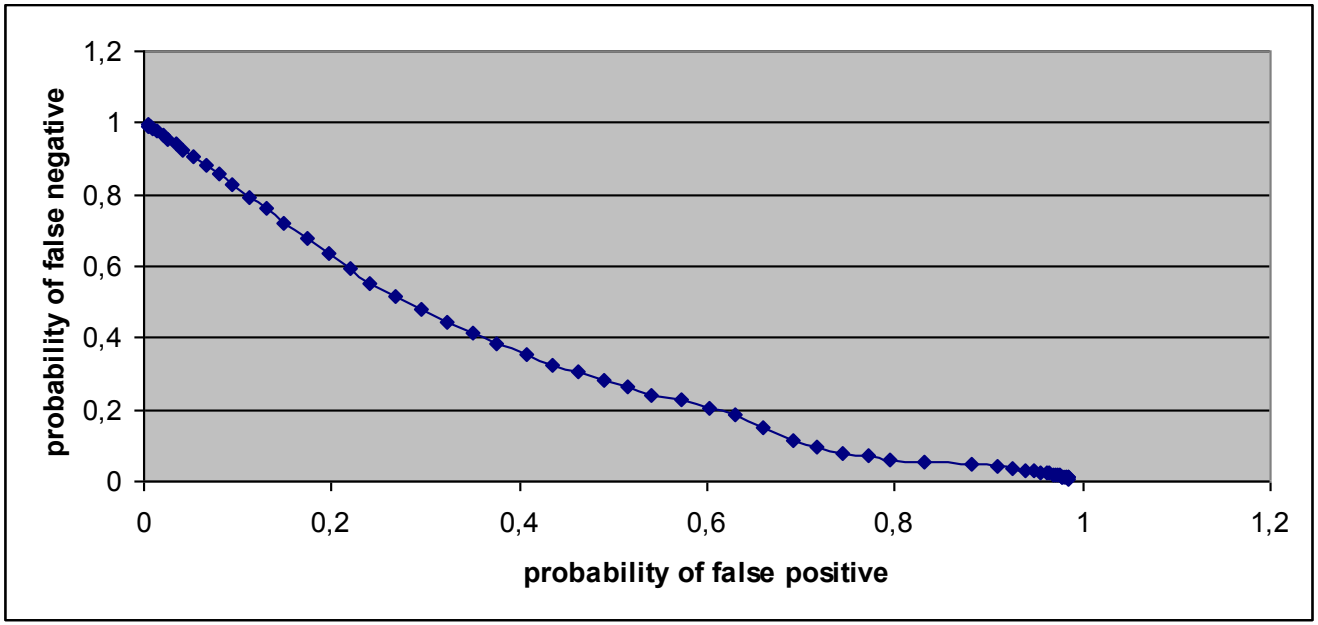
and calculating the discriminator $\frac{C(H[k])}{C(H^{/}[k])}$

Statistics based on 10 thousand images

Threshold	Detection probability	false positive probability	false negative probability
1.2	0.9916	0.9856	0.0084
1.1	0.9814	0.9712	0.0186
1.0	0.9473	0.8314	0.0527
0.9	0.7578	0.5411	0.2422
0.85	**0.6571**	**0.4075**	**0.3429**
0.8	0.4856	0.2675	0.5144
0.7	0.1167	0.0661	0.8833
0.6	0.0059	0.0037	0.9941

If the value of the discriminator $\frac{C(H[k])}{C(H'[k])}$ is greater than the threshold then given image is considered to be a CO otherwise it is considered to be a SG.


probability of detection
1,2
1
0,8
0,6
0,4
0,2
0
0
0,2
0,4
0,6
0,8
1
1,2
probability of false positive


probability of false negative
1,2
1
0,8
0,6
0,4
0,2
0
0
0,2
0,4
0,6
0,8
1
1,2
probability of false positive

Second-order functions method

In order to obtain the detecting results better than in the calibration method we need to provide the histogram to be less spread in its values.

In this method we form a histogram of brightness of horizontally neighboring pixels.

$$h_c^2(m,n) = \left| \{(i,j) \middle| p_c(i,j) = m, p_c(i,j+1) = n \} \right|$$

Due to the adjacent pixels often have close in value brightness we obtain near to diagonal histogram.

Then we form HCF $H^2[k,l]$ using 2D discrete Fourier transform.

At last we obtain 2D COM $C^2(H^2[k,l]) = \dfrac{\sum_{i,j=0}^{n} (i+j)\left|H^2[i,j]\right|}{\sum_{i,j=0}^{n} \left|H^2[i,j]\right|}$