Lecture 5. Ideal and Almost-Ideal SG .

Definition*.* SG is called *ideal (perfect or unconditionally undetectable ISG*) ,if its detection is equivalently to random guessing of this fact even with the use of the best statistical methods .

Definition. SG is called almost-ideal (*σ-undetectable AISG*), if $min\{P_m,P_{fa}\} \geq \sigma$, where P_m – is the probability of SG missing, P_{fa} – is the probability of false alarm (SG false detection) in the case of the use the best statistical methods of SG detection by an attacker.

The following question arises – is it possible generally speaking to design ideal ISG or even almost ideal AISG?

Answer to this question:

1. If CO can be chosen arbitrary and it is possible a participation of individuals in embedding and extraction procedures then ISG can be realized as SG-L with the use of hash functions (see Lecture 4) .

2. If it is allowed to embed only a few number of bits then ISG can be design for any types of CO (not necessary for text messages) with use of automatically chosen CO and then their hashing (such method is called *"rejection-sampling" – see Lecture 4*).

3. If there exists natural noise in the channel of SG detection then a design of ISG or AISG even resistant to removal attack occurs possible for small date embedding rate (see Lecture 6 "SG in noisy channels").
4. If the exact statistical model of CO is known for SG designer then ISG (which are in addition resistant to removal attack) can be presented (see next Sections of this Lecture).

5. If statistical model of CO is known only partially then AISG can be design but with small date embedding rate as a rule (see next Sections of this Lecture).

Specification of SG security criterion:
Let us P_c –is statistical distribution of CO *C(n),*
n =1,2…N and *P_w* – is the probability distribution of stego signal *$C_w(n)$* given chosen embedding method.

Definition Relative entropy or Kullback–Leibler divergence with respect to SG is called [6]

$$D(P_w \| P_c) = \begin{cases} \int\limits_{x\in X} P_w(x)\log(\frac{P_w(x)}{P_c(x)})dx, & \text{(if X – is a continues set of SG observations)} \\ \sum\limits_{x\in X} P_w(x)\log(\frac{P_w(x)}{P_c(x)}), & \text{(if X – is a discrete set of SGS observations)} \end{cases} \quad (1)$$

For any SGS detecting methods the following relation will be true [7]:

$$P_{fa}\log(\frac{P_{fa}}{1-P_m}) + (1-P_{fa})\log(\frac{1-P_{fa}}{P_m}) \le D(P_w \| P_c), \quad (2)$$

$$P_m\log(\frac{P_m}{1-P_{fa}}) + (1-P_m)\log(\frac{1-P_m}{P_{fa}}) \le D(P_c \| P_w), \quad (3)$$

$P_e > \pi_0\pi_1\exp(-J/2),$ where $J = D(P_w \| P_c) + D(P_c \| P_w),$ (4)

$P_e = \pi_0 P_{fa} + \pi_1 P_m, \pi_0, \pi_1 -$ prior probabilities for absence and presence of SG, If $P_{fa} = 0$, then it follows from (2) that

$$P_m \geq 2^{-D(P_w \| P_c)}. \tag{5}$$

SG is ISG if and only if

$$D(P_w \,\|\, P_c) = D(P_c \,\|\, P_w) = 0 \Rightarrow P_{fa} = P_m = {}^1\!/_2. \tag{6}$$

SG is AISG (or ε-ISG), if either

$$D(P_w \,\|\, P_c) \leq \varepsilon \text{ or } D(P_c \,\|\, P_w) \leq \varepsilon. \tag{7}$$

Example . Assume that $D(P_w||P_c)= 0.1$, then if $P_{fa} = 0$, then $P_m \geq 2^{-D} \approx 0.933$.

Definition. *Bhattacharyya distance* between two distributions P_w and P_c is called[8,9]

$$D_B(P_c, P_w) = -\ln(\rho_B(P_c, P_w)), \quad \text{where} \tag{8}$$

$$\rho_B(P_c, P_w) = \int_{x \in X} (P_c(x) P_w(x))^{1/2} dx = \sum_{x \in X} (P_c(x) P_w(x))^{1/2}.$$

For any methods of SG detecting the following inequalities will be true:

(9)

$$0.25\rho_B^2(P_c,P_w) \le P_e \le 0.5\rho_B(P_c,P_w),$$

where $P_e = \pi_0 P_{fa} + \pi_1 P_m = \frac{1}{2}(P_{fa}+P_m),$ if $\pi_0 = \pi_1 = \frac{1}{2}.$

(10)

$$P_e \ge 0.25e^{-2D_B(P_c,P_w)}.$$

SG is ISG if and only if

$$D_B(P_c,P_w) = 0 \Rightarrow \rho_B(P_c,P_w) = 1. \quad (11)$$

SG is AISG (or ε-ISG), if

$$D_B(P_c,P_w) \le \varepsilon. \quad (12)$$

Remark. Bhattacharyya distance (BD) is symmetrical function $D_B(P_c,P_w) = D_B(P_w,P_c),$ that is in distinction to relative entropy (RE) (that is asymmetric one)$(D(P_c \| P_w) \ne D(P_w \| P_c)).$ BD does not satisfy to *<u>triangle inequality</u>*$(D_B(P_1,P_2) < D_B(P_2,P_3) + D_B(P_1,P_3)),$ however its modification$(\sqrt{1-\rho_B^2(P_c,P_w)})$ does.

CO with known statistics [10].

In this case it is assumed that before design of SG statistical properties of CO should be known completely .

1.*C(n)* є *N* $(0,\sigma_c^2), E\{C(n)C(n')\}=0,$ if *n ≠ n`.*

Then we can design ISG using the following embedding procedure:

$C_w(n)=\beta C(n)+\alpha(-1)^b\pi(n),$ where (13)

$\beta=\sqrt{1-(\alpha^2/\sigma_c^2)}, \pi(n)\in N(0,1), E\left\{\pi(n)\pi(n')\right\}=0, n\neq n'.$

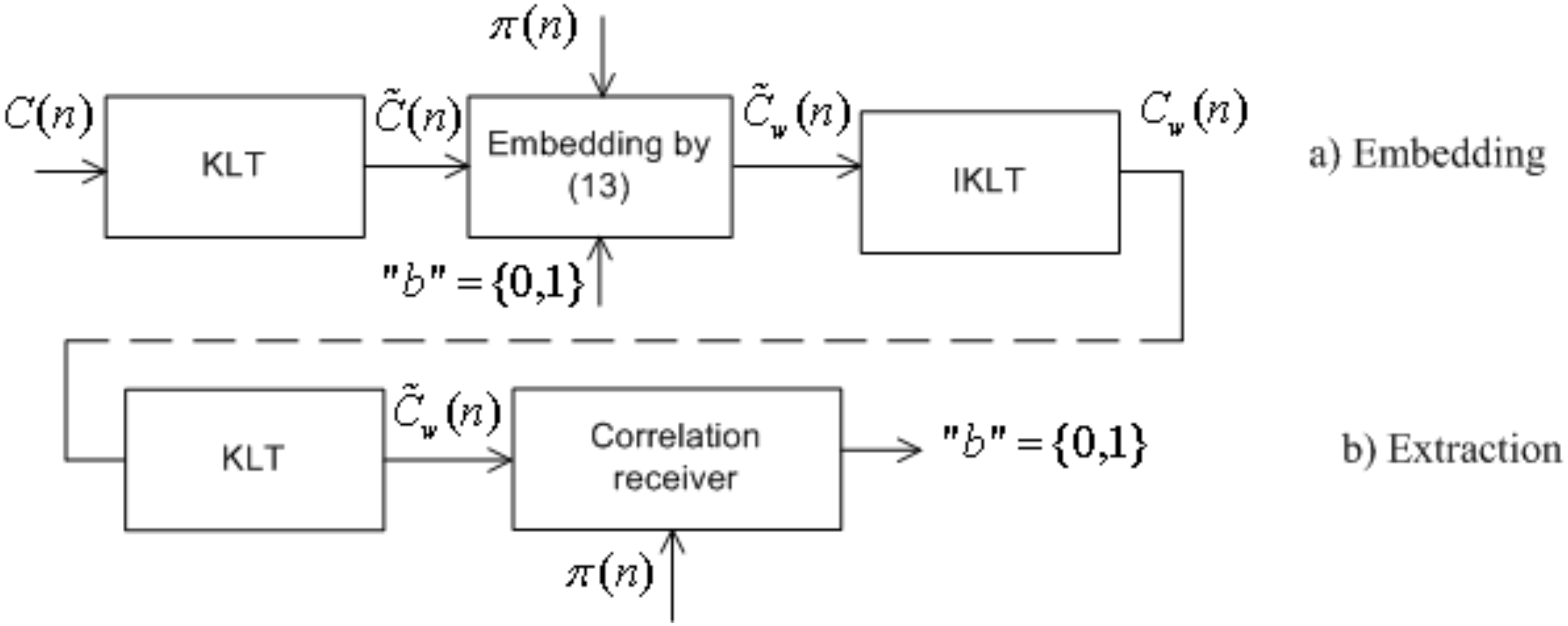
In fact, *C_w(n)* є *N* $(0,\sigma_w^2), E\{C_w(n)C_w(n')\}=0,$ if *n ≠ n` and*

$\sigma_w^2=\beta^2\sigma_c^2+\alpha^2=\sigma_c^2-\alpha^2+\alpha^2=\sigma_c^2,$ that gives $P_w = P_c$.

2. CO is colored Gaussian noise .

C(n) є *N* $(0,\sigma_w^2), E\{C(n)C(n')\}\neq 0,$ if *n ≠ n`* and it is given the correlation matrix $\mathbf{R_c}$.

Then ISG can be presented by the following methods of embedding and detectionon:



Notations above:

KLT – Karunen-Love Transform that transforms colored Gaussian noise to white noise (with independent samples) $\tilde{C}(n)$.

IKLT – inverse to KLT.

3. *C(n)* has arbitrary (non-Gaussian) distribution P_c with independent samples . Then ISG can be presented by the following embedding and detection procedures:

$$C_w(n) = F^{-1}(\beta F(C(n)) + \alpha(-1)^b \pi(n)), \qquad (14)$$

$$b = \begin{cases} 0, \text{ if} & \sum_{n=1}^{N} F(C_w(n)\pi(n)) \geq 0, \\ 1, \text{ if} & \sum_{n=1}^{N} F(C_w(n)\pi(n)) < 0, \end{cases} \qquad (15)$$

where *F(.)* – is such transform that provides for any non-Gaussian random variable *C(n)* with $E\{C(n)\} = 0, Var\{C(n)\} = \sigma_c^2$ a mapping to Gaussian random variable *N (0,* σ^2_c*).*

F^{-1}*(.)* – is inverse transform to transform *F(.).*

Remark 1. Any way it is assumed that for embedding and detection procedures should be known exactly σ_c^2, R_c, and for the last model also P_c.

Remark 2. In the all cases considered above SG occurs *robust* that means that it is resistant against removal attack. This property is provided by the use of PRS *π(n)* controlled by the secret key and having the length *N* if of course decoding performs correlation detector by (15). However the more is *N* the less is embedding rate. (There are also more sophisticated removal attacks on SG (see Lectures in the sequel) .

Remark 3. A calculation of the error probabilities for different types of decoders (both blind and informed) can be performed by formulas (13) and (19) (see Lecture 3).

Design of SG for partially known CO distribution [9] .

(This way offers some practical implementation of SG for typical CO like audio and video).

1. Additive embedding into zero mean Gaussian CO with unknown for designer correlation matrices.

Then $$D_B(P_c,P_w)=\frac{1}{2}\ln\frac{\det R}{\sqrt{\det R_w \det R_c}}, \qquad (15)$$

where R_c – is correlation matrix of CO, R_w – is correlation matrix of SG,
$R = (R_s + R_w)/2.$

For embedding by (13) and exponential correlation matrix

$$R_c=\sigma_c^2\begin{bmatrix} 1 & r & r^2 & \dots & r^{N-1} \\ r & 1 & r^2 & \dots & r^{N-2} \\ \dots & \dots & \dots & \dots & \dots \\ r^{N-1} & \dots & \dots & \dots & 1 \end{bmatrix}, \quad R_w=\sigma_w^2\begin{bmatrix} 1 & r\delta^{-1} & r^2\delta^{-1} & \dots & r^{N-1}\delta^{-1} \\ r\delta^{-1} & 1 & r^2\delta^{-1} & \dots & r^{N-2}\delta^{-1} \\ \dots & \dots & \dots & \dots & \dots \\ r^{N-1}\delta^{-1} & \dots & \dots & \dots & 1 \end{bmatrix}.$$

One can prove [9], that

$$\rho_\beta^2(P_c,P_w)\approx\left(\frac{\sqrt{(1-r^2)(1-2r^2\delta^{-1}+r^2)}}{1-2r^2\tau+r^2}\right)^{N-1}, \qquad (16)$$

where $$\delta=\frac{1}{\left(1-\frac{\alpha^2}{2\sigma_c^2}\right)^2};\tau=(1+\delta^{-1})/2.$$

Example.*r = 0.5, δ = 1.01, N = 500,* then by(16) $\rho_\beta^2(P_c, P_w) = 0.997.$

r = 0.9, δ = 1.01, N = 500, then by (14) $\rho_\beta^2(P_c, P_w) = 0.66.$

(Remember that $P_e \geq 0.25\rho_\beta^2(P_c, P_w)$).

We can see that for small correlations this is AISG.

This SG is robust to additive noise :

$$P = Q\left(\sqrt{\frac{N_0}{\eta - 1}}\right)$$ for informed decoder ,

$$P = Q\left(\sqrt{\frac{N_0}{\eta_w}}\right)$$ for “blind” decoder,

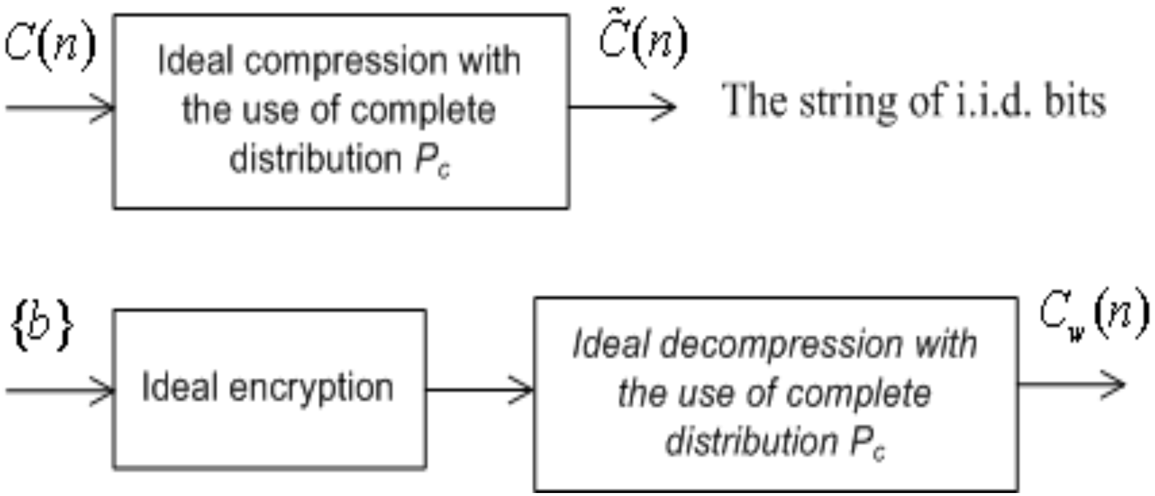
where $\eta_w = \frac{\sigma_c^2}{\alpha^2}; \eta_a = \frac{\sigma_c^2}{\alpha^2 + \sigma_\varepsilon^2}$ (see Lecture 3).

Example.η_w *= 100,* η_a *= 70,* N_0 *= 5, N = 500;* then $P_e \geq 0.16$, $P \leq 3 \cdot 10^{-4}$ and it is possible to embed secure 100 bits in the case of the use informed decoder.

For a large correlation between CO samples SG is not secure even for small embedding rate . (However the conditions above say about a potential opportunity SG to be undetectable while for real attacks it keeps still AISG.)

2. SG based on compression procedures [11]

2.1. Ideal lossless compression.



$C(n)$

Ideal compression with the use of complete distribution P_c

$\tilde{C}(n)$

The string of i.i.d. bits

$\{b\}$

Ideal encryption

Ideal decompression with the use of complete distribution P_c

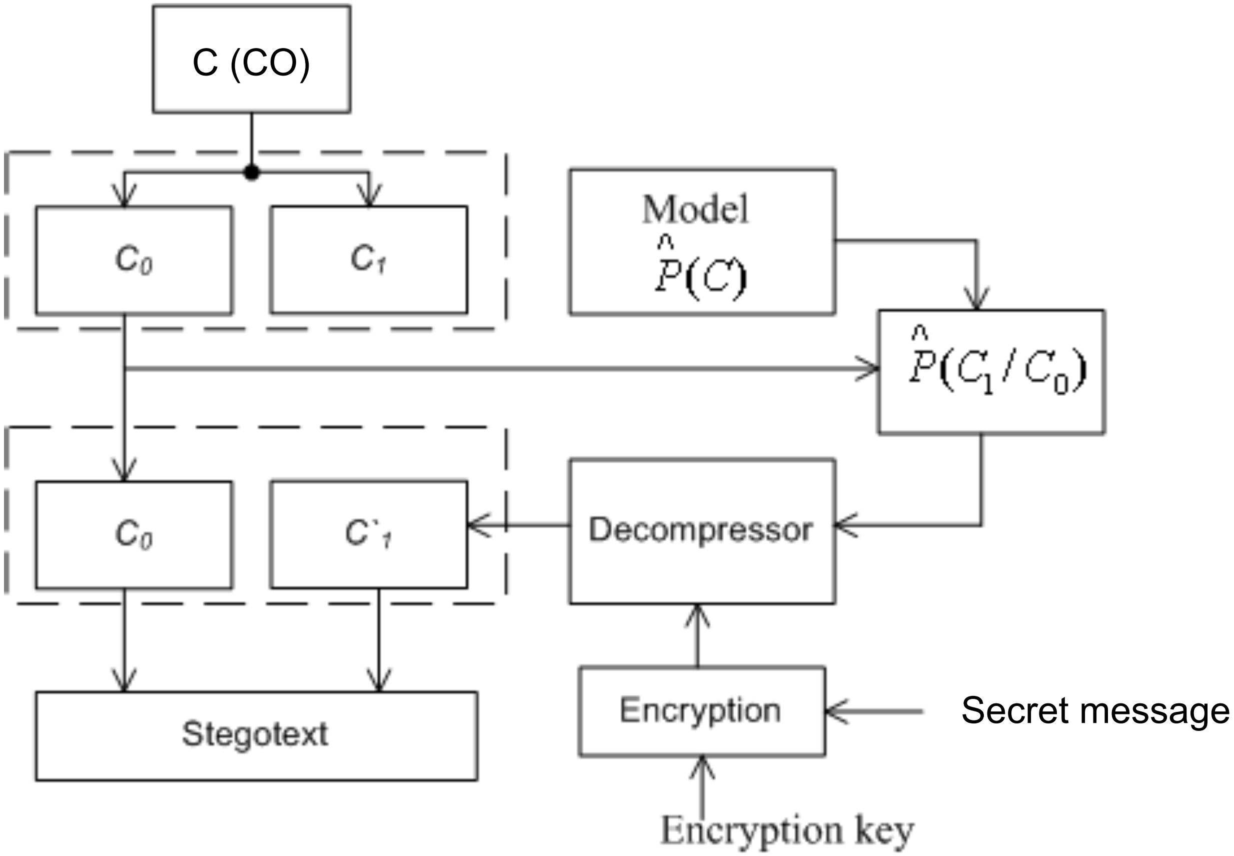
$C_w(n)$

Stegotext coinciding with one of CO

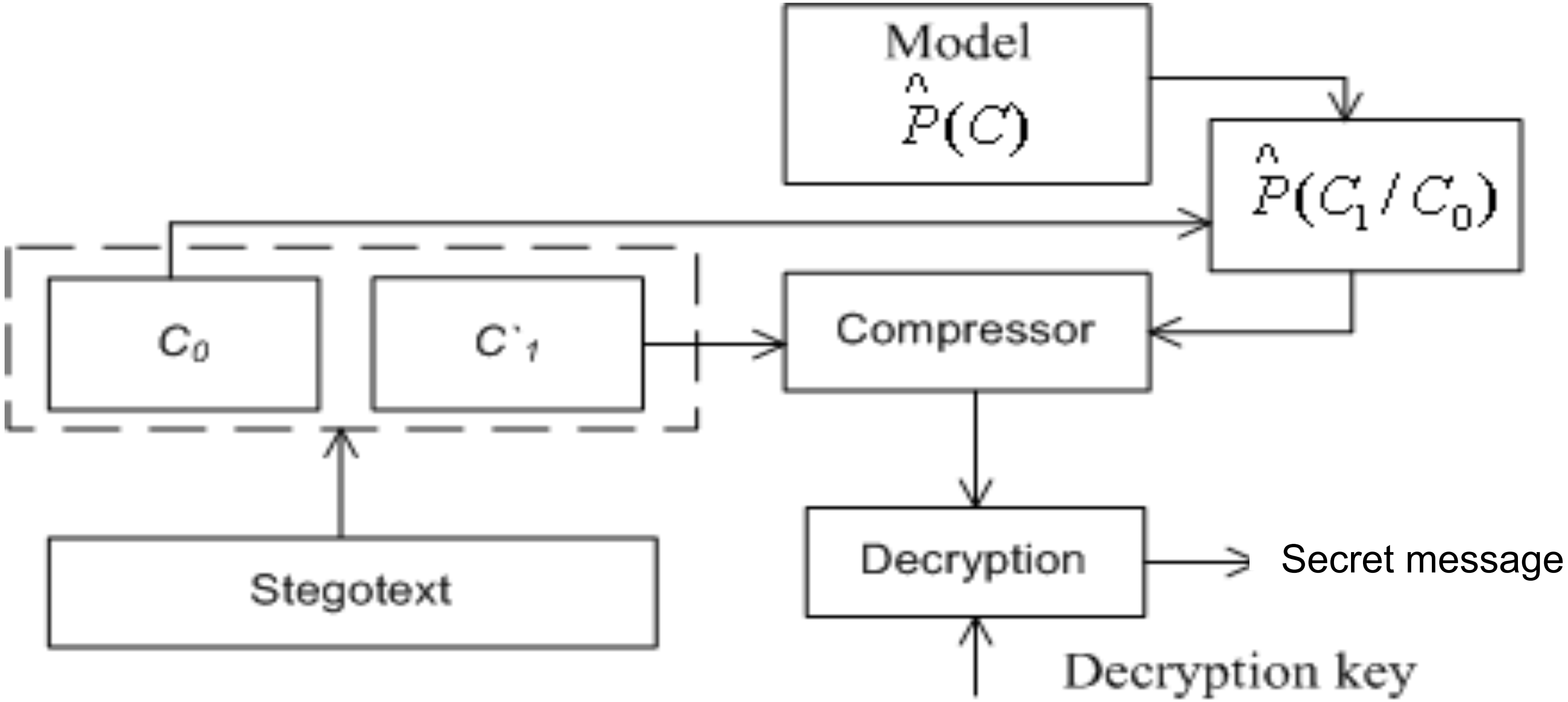
Thus SG is ideal but it is impractical for two reasons:

1. Distribution P_c is never known completely for real CO.
2. Even though P_c would be known it is impossible to arrange an implementation of ideal compression.

2.2. Compression based on partially known statistic of CO (model-based SG)[11]. CO is divided in two parts: C_0 and C_1, where C_0 is kept in SG . The statistic $\hat{P}(C)$ known about CO is used for estimation of conditional probability $\hat{P}(C_1 / C_0)$. Encrypted message comes at input of decompression algorithm that uses conditional distribution $\hat{P}(C_1 / C_0)$ in order to form output that is taken as a second part of SG. A combination of C_0 and C_1 gives SG.



a) Algorithm of embedding

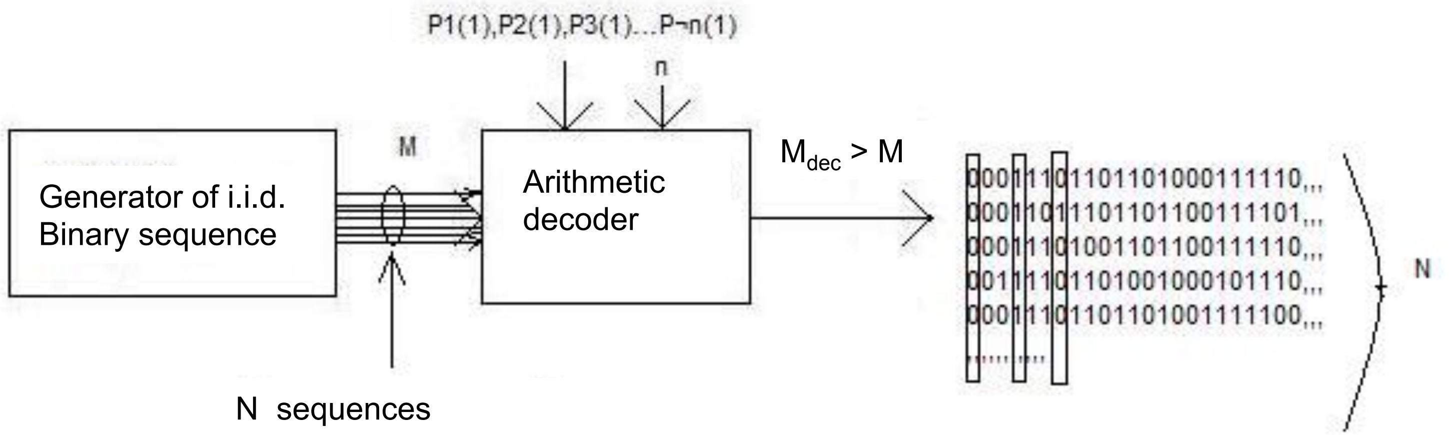


b) Algorithm of extraction

Particular case. Consider the case where C_1 is area of LSB-DCT image coefficients. Simulation of such SG demonstrates [11] high enough data embedding rate and a distribution of DCT coefficients in SG very close to their distribution in CO.

Remark. In essence, this method implies that a distribution of LSB for DCT coefficients is estimated more correctly on real CO than in conventional SG-LSB and such estimation determines embedding procedure .

Decompression by arithmetic decoder [38]



00011101101101000111110,,,
00011011101101100111101,,,
00011101001101100111110,,,
00111101101001000101110,,,
00011101101101001111100,,,

Generator of i.i.d. binary sequence inputs *N* such sequences of the length *M* each.

Arithmetic decoder (AD) is determined by *n* probabilities of ones : $P_1(1),..P_n(1)$.

AD outputs N sequences of the length $M_{dec} > M$.

Experiments shows [38] that the statistical probabilities (calculated *by columns*) are very close to the probabilities at the AD.

This means that if we change i.i.d. generator by strong encrypted secret messages and determine the probabilities at the AD by conditional probabilities

$\hat{P}(C_1/C_0)$

then we are able to embed secrete information into LSB of DCT coefficients keeping their statistic approximately as it was in CO before embedding.

Extraction of secret message can be obtained by implementation of arithmetic coder (AC) determined by the same set of probabilities $P_1(1),..P_n(1)$ and decryption of AC output with the same cipher and secret key.

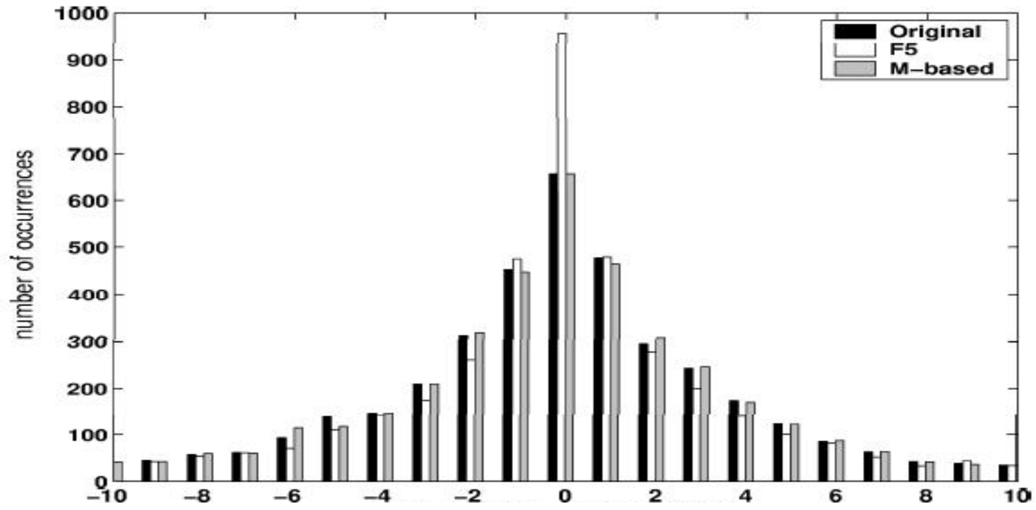
It is proposed a model of the DCT probability distribution (Cauchy) [11]:

$$P(C) = (p-1)(|u/s|+1)^{-p}/2s$$

where s and p are the parameters which can be estimated by the most significant bits of CO. Next can be computed the required probabilities $P_1(1),..P_n(1).$

This is why this SG is called as *model-based one*.

Images	Size of images (bytes)	Size of SG (bytes)	Embedding rate (%)
barb	48459	6573	13.56
boat	41192	5185	12.59
bridge	55698	7022	12.61
goldhill	48169	6607	13.72
lena	37678	4707	12.49
mandrill	78316	10902	13.92



Histogram of DCT (2,2) before and after embedding by SG F5 and MB [11] .

In fact SG-MB can be simply enough detected by blind steganalysis. (See Lecture 7)

2.3. Perturbed Quantization Steganography (SG-PQS) [12])

2.3.1. Conventional quantization-based embedding (SG-CQ).

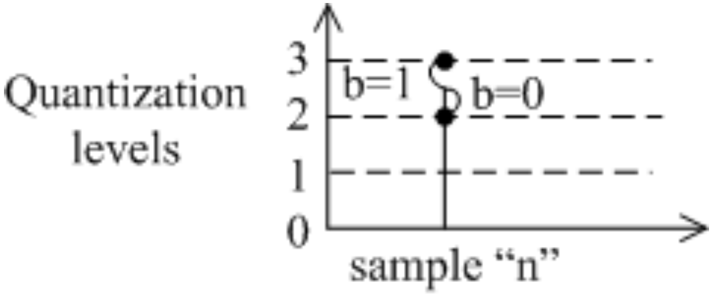
C(n) – amplitude-continuous sequence of samples or amplitude-discrete sequence of samples (for the thing 16-bits samples for medical images under by second quantization).

Embedding algorithm

$$C_w(n) = \begin{cases} C_{qe}(n), b = 0, \\ C_{qo}(n), b = 1, n = 1, 2..., \end{cases} \qquad (17)$$

where $C_{qe}(n)$ - are *C(n)* quantized to the nearest even quantization level,
$C_{qo}(n)$ - are *C(n)* quantized to the nearest odd quantization level.

Example



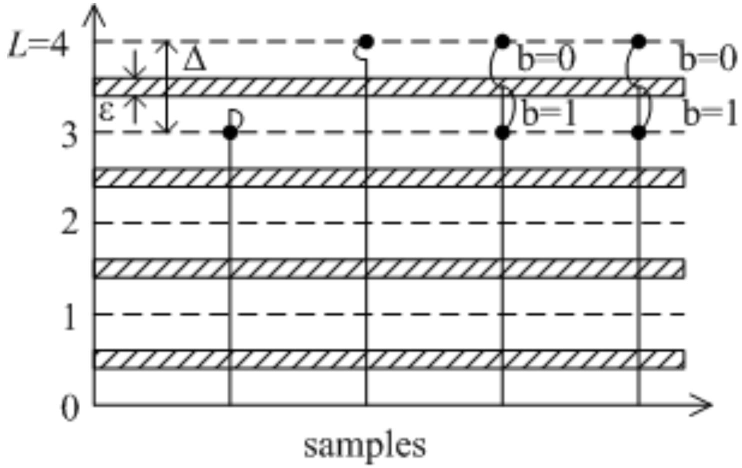
Properties of SG-CQ :

- embedding rate is 1 bit/sample,
- CO is not required for error free decoding,
- suffers from removal attack by randomization of even/odd quantization levels,
- it is easy detectable .

In order to overcome the last defect has been proposed PQS .

The main idea: to use the fact that attacker never knows samples of CO before quantization (embedding).

Embedding algorithm is illustrated in the Figure*:*



Embedding is performed only in such samples that have amplitude belonging to intervals wide around the middles of quantization levels. In this case samples are quantized into the nearest even levels if *b = 0* and into odd levels if *b = 1*.

An attacker is unable to detect deviation from conventional quantization because he (or she) never knows the amplitude of samples before quantization procedure. Besides of them the amplitude distribution within *ε*–intervals is very close to uniform distribution and therefore the statistic of SG be very close to statistic of CO.

The following problem arises. How to find in the extraction procedure samples which have the embedded information?

This problem can be solved by the use of so called "*wet paper codes (WPC)*":
$\boldsymbol{b} = (b_1, b_2, \ldots b_k)^T$, $b_i = \{0,1\}^k$, "T" – symbol of transposition, n_0 – is the number of samples in which it is necessary to embed these k bits.
H – kxn_0 binary matrix that is determined by stegokey distributed in advance between authorized users.
$S_p(n) = C_q(n) mod2, n = 1, 2\ldots$, where $C_q(n)$ – is the value of $C(n)$, quantized to the nearest level for given quantization interval Δ if the number of quantization levels is L. (We can see that $C_q(n)mod2$ takes binary values 0 и 1,corresponding to even and odd quantization levels .)
$E_\varepsilon \subseteq \{1, 2 \ldots n_0\}$- set of samples where it is allowed to embed information due to PS method .

Algorithm of embedding:

$$\mathbf{S_p} \rightarrow \mathbf{S}'_p = [S'_p(n)]_{n=1}^{n_0} : \mathbf{HS'_p} = \mathbf{b}, S'_p(n) \neq S_p(n), n \in E_\varepsilon. \qquad (18)$$

The necessary condition to be solved matrix equation (18) is

$$rank \tilde{\mathbf{H}} = k, \qquad (19)$$

where $\tilde{\mathbf{H}}$ - binary (kxm) submatrix of $\boldsymbol{H}$, that is obtained by removal from H all columns which do not belong to E_ε, m – is the number of samples among n_0, where it is allowed to embed messages in line with PS algorithm.

It has been proved in [12], that $m \approx k$, as $n_0 \to \infty$. That means that on average and for large enough values of block lengths n_0 in every of them can be embedded about $k = m$ information bits.

Decoding:

$$\mathbf{b} = \mathbf{H}\mathbf{S}'_{\mathbf{p}}. \tag{20}$$

We can see that in distinction to conventional error correction codes WPC have more complex *encoding procedure* (it is necessary to solve liner system of equations), than *decoding procedure* (it is necessary only to multiply matrix by vector).

Remark 1. Because the block length n_0 can be very large (hundreds and thousands bits), it is rather necessary to use special methods [41] in order to solve equations like (18) .

Remark 2*.* PQS has to contain an additional information about the number of bit k that have been embedded in this block (this information can be inserted into the head of the length α bits).

It has been proved [13] that the probability $P_e(k, d, n_0, P_w)$ of such event that in the block containing n_0 samples cannot be embedded k bits given the head length is d and the probability of embeddable sample is P_w , holds the following bound :

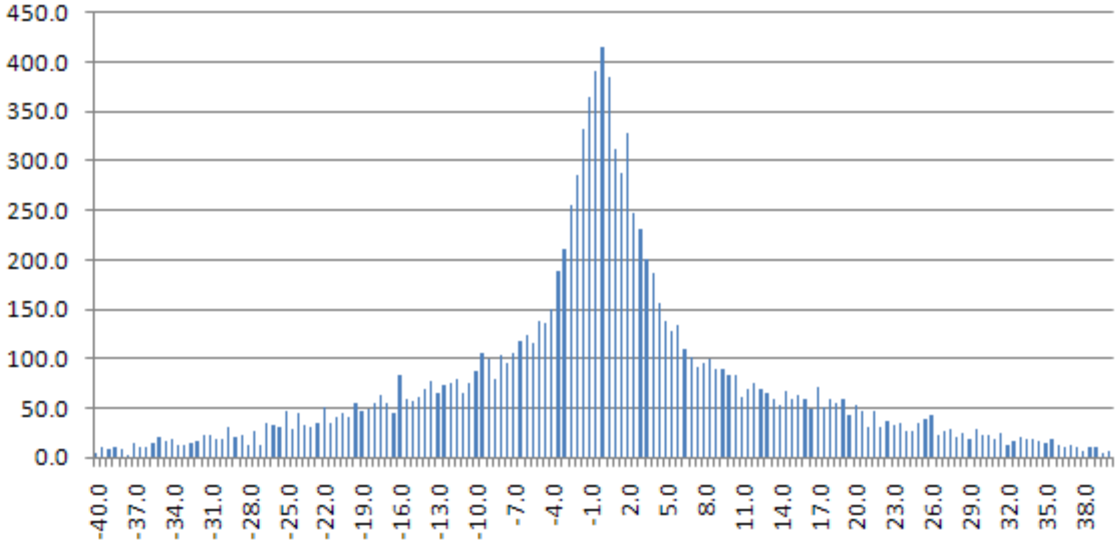
$$P_e(k,d,n_0,P_w) \le \left[\left(\frac{P_w}{\mu}\right)^{\mu}\left(\frac{1-P_w}{1-\mu}\right)^{1-\mu}\right], \tag{21}$$

where $\mu = \dfrac{k+d-1}{n_0}.$

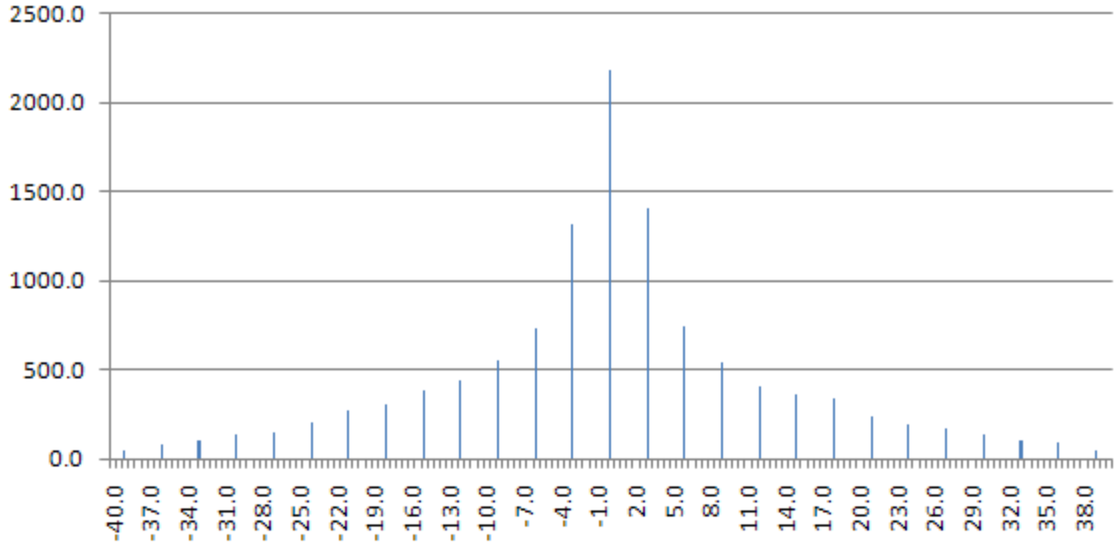
2.4 PQS after double compression[12].

PQS is applied to information-reducing process of repeated JPEG compression.

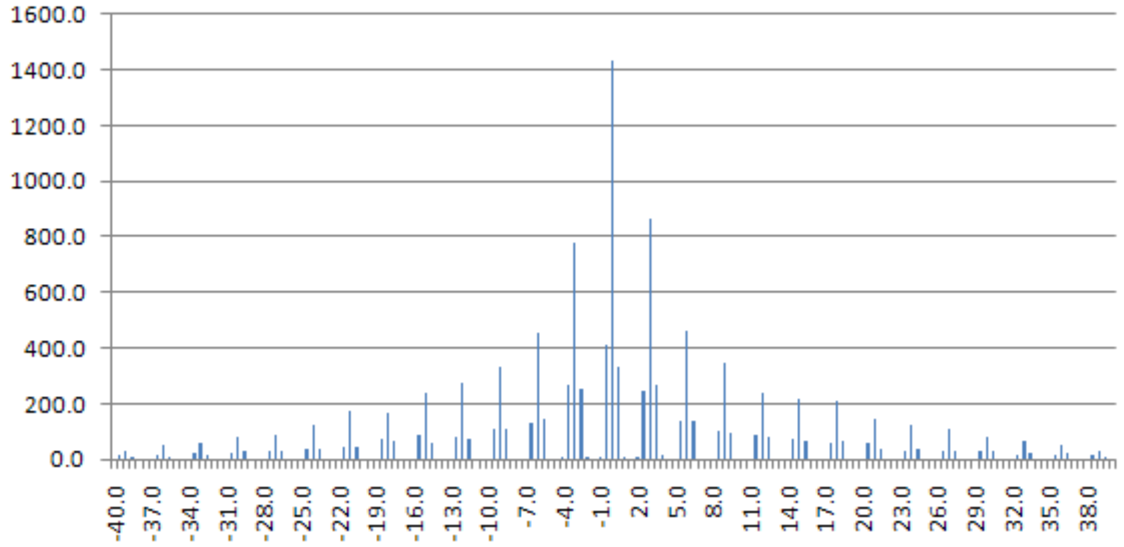
The method takes a single compressed JPEG (very natural for storing images inside of digital cameras) and produces a double compressed and embedded JPEG file as SG.



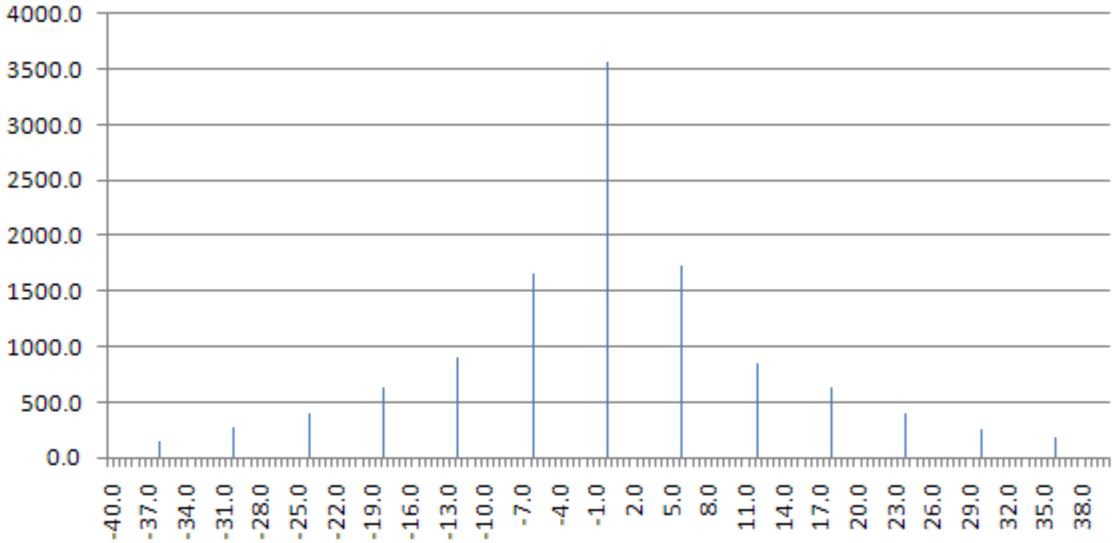
Histogram of DCT C21 before the first quantization



Histogram of DCT C21 , Q = 88%, q21 = 3 (after quantization).



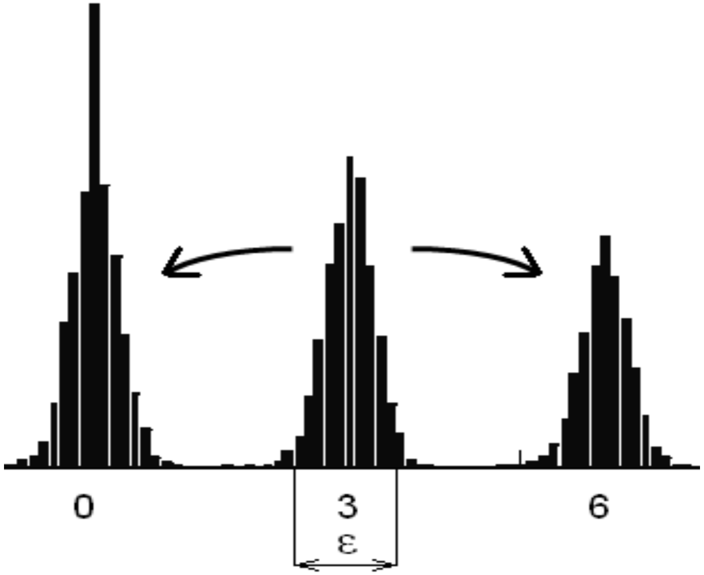
Histogram of non-quantized C_{21} after BMP-Jpeg-BMP-transforms



Histogram of quantized coefficient C_{21} after BMP-Jpeg-BMP-transforms with Q = 76%, q21 = 6

We can see that peaks around the even multiples $2kx3 \quad ,k = ... -1.0,1,..$ are quantized to $6k$, while the peaks around the odd multiples $(2k+1)x3, k = 0,1..$ are split in half , the left half being quantized to $6k+2$ and the right half to $6k+4$.

PQS feature : *Include all odd multiples to the set of changeable coefficients.*



PQS embedding procedure .

Coefficient selection rule: $kq_{ij}^{(1)} = lq_{ij}^{(2)} + q_{ij}^{(2)} / 2$,
where k and l are integers and $q_{ij}^{(1,2)}$ are quantization steps.
All *contributing multiples k* of $q_{ij}^{(1)}$ are expressed by the formula:

$$k = (2m+1)\frac{\mathrm{q}_{\mathrm{ij}}^{(2)}}{2g}, \; m = \ldots -2, -1, 0, 1, 2, \ldots$$

where $g = \mathrm{gcd}(q_{ij}^{(1)}, q_{ij}^{(2)})$
The total number of changeable coefficients is [12] :

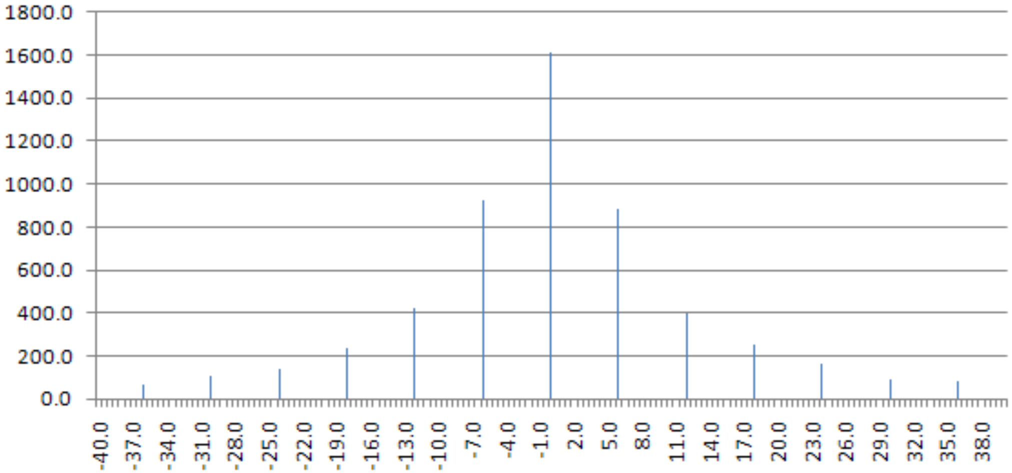
$$\left|S\right| = \sum_{i,j=0}^{7} \sum_{m} z_{ij} h_{ij}((2m+1)\frac{\mathrm{q}_{\mathrm{ij}}^{(2)}}{2g})$$

where $z_{ij} = 1$, if $(q_{ij}^{(1)}, q_{ij}^{(2)})$ is “contributing pairs” and $z_{ij} = 0$, otherwise.

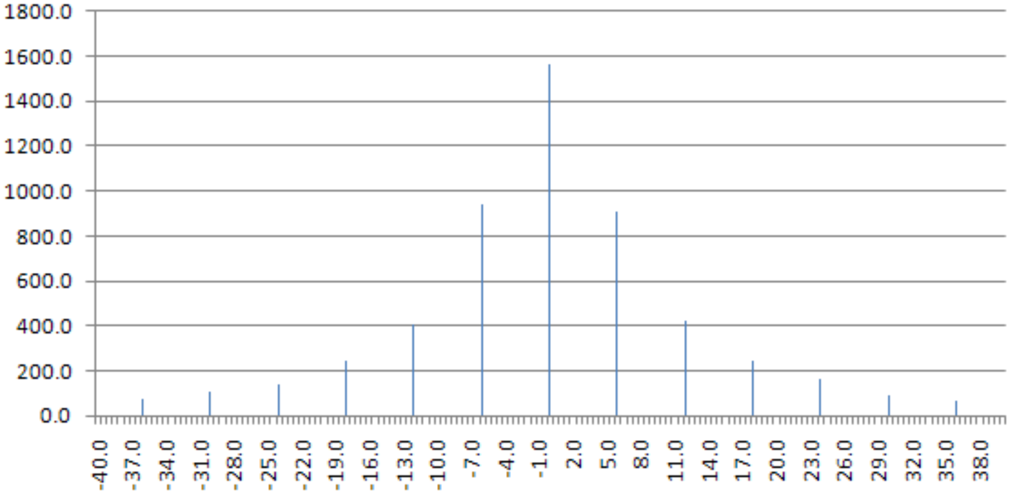
Original BMP cover image

Image after double compression, $Q_1 = 88\%$, $Q_2 = 76\%$

Image after double compression and PQS embedding of 65622 bits,
Q_1 = 88%, Q_2 = 76%



Histogram of DCT C_{21} image after double compression Q_1 = 88%, Q_2 = 76%



Histogram of DCT C_{21} image after double compression and PQS embedding of 65622 bits, Q_1 = 88%, Q_2 = 76%

We can conclude that both histograms practically coincide .
But it is necessary to investigate also other attacks on PQS.

PQS security [13].

We will use relative entropy criterion as first order statistic :

$$D(\mathbf{P}_c \,\|\, \mathbf{P}_w) = N\sum_{\ell=1}^{L} P_\ell \log\frac{P_\ell}{\tilde{P}_\ell} = ND_1(P_c \,\|\, P_w), \qquad (22)$$

where $P_c = (P_{\mathrm{l}})_{\mathrm{l}=1}^{L}$ - is one- dimensional distribution of quantized CM

$P_w^{'} = (\tilde{P}_\ell)_{\ell=1}^{L}$ - is one dimensional distribution of SG by QS method,

N - is the general number of samples,

L - is the number of quantization levels.

It is easy to see that

$$P_{\mathrm{l}} = \int_{J_{\mathrm{l}}} P_c(x)dx,$$ where $J_{\mathrm{l}} = [\Delta(\mathrm{l}-1/2), \Delta(\mathrm{l}+1/2)], \Delta -$ quantization interval.

$$\tilde{P}_\ell = \frac{1}{2}\int_{I_{\ell,\varepsilon}} P_c(x)\,dx + \int_{M_{\ell,\varepsilon}} P_c(x)\,dx + \frac{1}{2}\int_{K_{\ell,\varepsilon}} P_c(x)\,dx,$$

where

$$I_{\mathrm{l},\varepsilon} = [\Delta(\mathrm{l}-1/2) - \varepsilon/2, \Delta(\mathrm{l}-1/2) + \varepsilon/2], K_{\mathrm{l},\varepsilon} = [\Delta(\mathrm{l}+1/2) - \varepsilon/2, \Delta(\mathrm{l}+1/2) + \varepsilon/2],$$

$$M_{\mathrm{l},\varepsilon} = [\Delta(\mathrm{l}-1/2) + \varepsilon/2, \Delta(\mathrm{l}+1/2) - \varepsilon/2].$$

$$P_w = \sum_{\mathrm{l}=1}^{L} \int_{H_{\mathrm{l},\varepsilon}} P_c(x)dx,$$ where $H_{\mathrm{l},\varepsilon} = [\Delta(\mathrm{l}+1/2) - \varepsilon/2, \Delta(\mathrm{l}+1/2) + \varepsilon/2].$

Simulation results for Gaussian CO.

$$\sigma_c^2 = 1, L\Delta = 6\sigma_c^2 = 6, L = 256.$$

v = ε/Δ	D_1	P_w	*m*
0.005	$6.588 \cdot 10^{-11}$	0.00498	$7.56 \cdot 10^6$
0.01	$2.6 \cdot 10^{-11}$	0.00973	$3.78 \cdot 10^6$
0.025	$1.647 \cdot 10^{-9}$	0.025	$2.5 \cdot 10^6$
0.05	$6.58 \cdot 10^{-9}$	0.05	$7.5 \cdot 10^5$
0.1	$2.6 \cdot 10^{-8}$	0.1	$3.8 \cdot 10^5$
0.25	$1.6 \cdot 10^{-7}$	0.249	$1.5 \cdot 10^5$
0.3	$2.372 \cdot 10^{-7}$	0.299	$1.26 \cdot 10^5$
0.5	$6.592 \cdot 10^{-7}$	0.499	$7.56 \cdot 10^4$
1.0	$2.641 \cdot 10^6$	0.997	$3.77 \cdot 10^4$

We can see that the number of secure embedded bits increases as the parameter *v = ε/Δ* (that is the more narrow than the area of embedding) decreases.
For real CO the relation above will be untrue in general.
First order statistic is not sufficient for effective detecting of PSGS. It is still open problem how to detect PS effectively.

If we let that on average the number of the embeddable bits is $N P_w$, then the number of secure embedded bits *m* (for $D(P_c||P_w) = 0.1$) is

$$m = N P_w = 0.1 \frac{P_w}{D_1(P_c \| P_w)}.$$

More effective method is to use blind steganalysis *(see in the sequel).*

2.5. Maintaining of CO statistics after embedding of the message[39]- (SG-R).

The main model:
CM is binary (a,b) i.i.d. (but not necessary uniformly distributed) sequence.

Secret message is binary (0,1) i.i.d. uniformly distributed sequence (say, after strong encryption).

Embedding algorithm:

1.Divide the CO sequence on pairs .
2.Define a mapping: $aa \to u, bb \to u, ab \to v_0, ba \to v_1$

3.Maintain the all u-pairs (“unused”) without changing.
4.Change (if necessary) the pairs v_k(e.g. v_0 or v_1) to the pairs v_{y_k} where y_k is $k-th$ secret bit.
5.Change the pairs v_{y_k} to corresponding binary symbols.

Extraction algorithm:

1.Divide the SG- sequence on pairs.
2.Find the pair ab and ba and extract the embedded secret message following the rule: $ab \to 0, ba \to 1$

Example.

$y = 0110$

$CO = aababaaabbaaaaabb$

$Map. = u v_1 v_1 u v_0 v_1 uuu$

Emb.= $u v_0 v_1 u v_1 v_0 uuu$

SG= aaabbaaabaabaaaabb

Extr.= 0 1 1 0

Positive properties of SG-R :

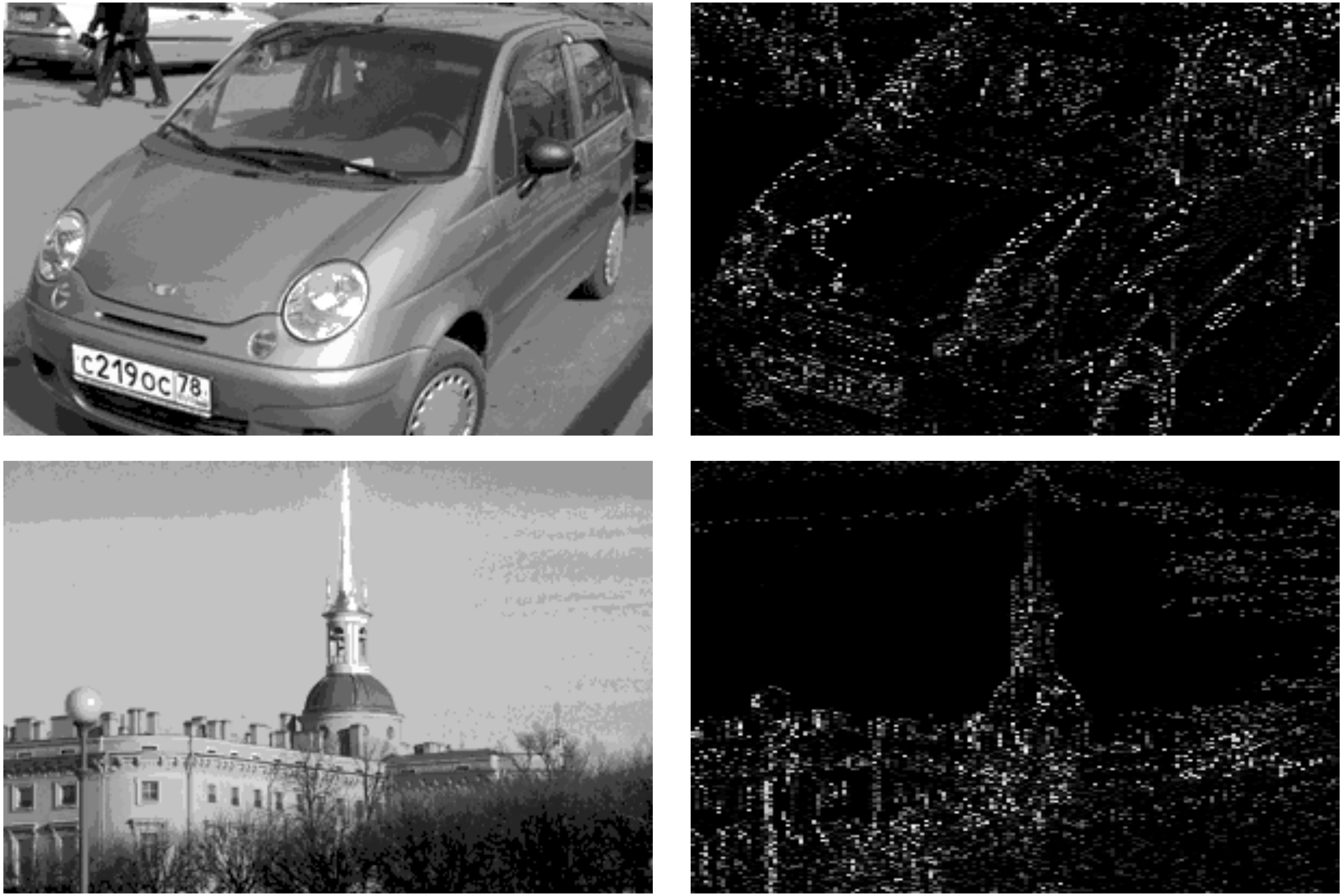
1.The length of SG equal to the length of CO.
2.Correct extraction of message.
3.Maintaining of statistics after embedding : $P_{SG}(a) = P_{CO}(a)$

Defects of SG-R :

1.SG is corrupted significantly against CO.
2.CO cannot be correctly recovered even after extraction of secret message.
(In fact if CO = $aaabba$... , then after embedding of the same sequence 0110 we would obtain the same stego message although the CO was different.
3.SG-R works only for i.i.d. CO although it possibly can be extended in the future to other models.

Proposal: Apply SG-R to LSB of CO only [56].

Example of information embedding by means of SG-R method



Embedding into the least significant bits (LSB)

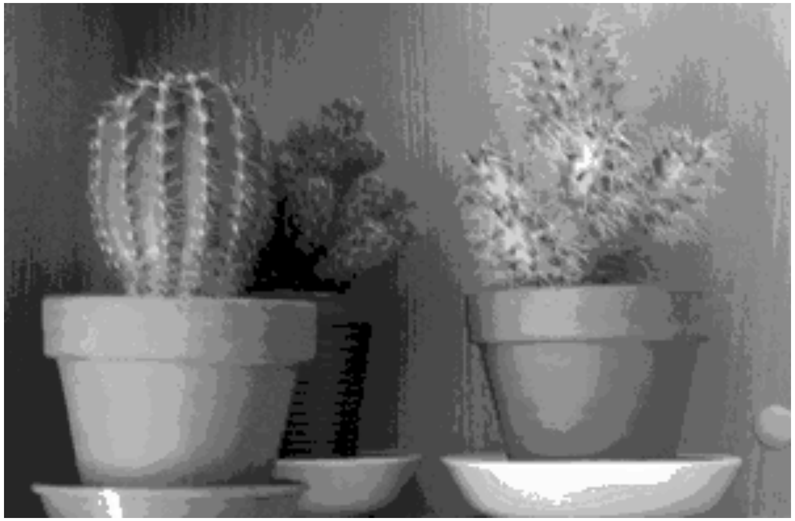
Due to strong spatial correlation of the image samples the embedding of information will be fulfilled into the least significant bits, which do not essentially change the content of image.

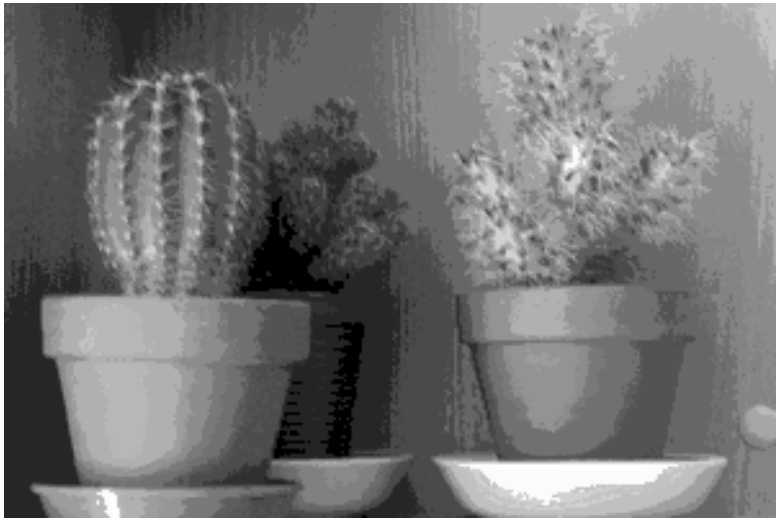
The right-hand side picture shows the image with 3,000 bits embedding by means of SG-LSB-R method, while cover object (CO) capacity is 4,740 bits.

Example of 100% information embedding by means of SG-R method

As the images have different luminance distributions the capacity of possible IH will vary as CO changes. Let consider several images and obtain the possible volume of additional information could be embedded in them.

1. The size of given image is 200x300px. N_{max} = 6,330 bits.



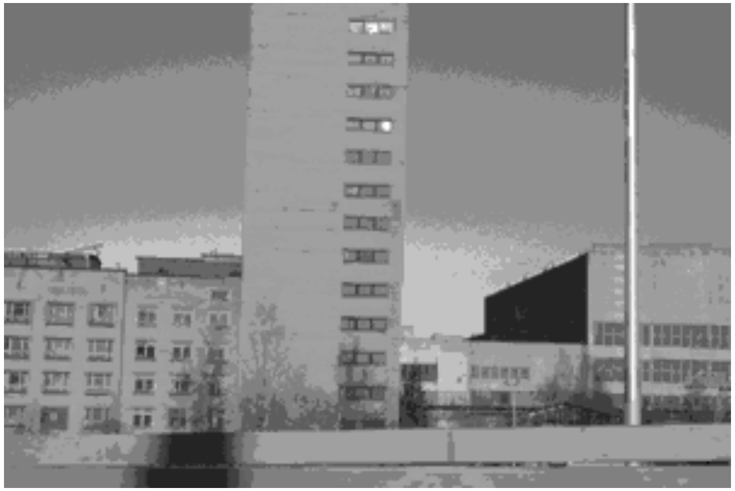


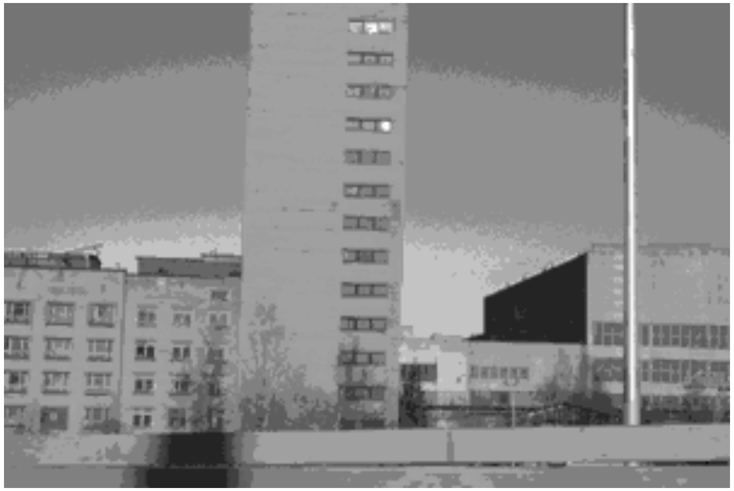
The left-hand side picture shows the original and the right hand picture presents image after embedding.

2. The size of given image is 200x300px. Nmax = 12,057 bits.

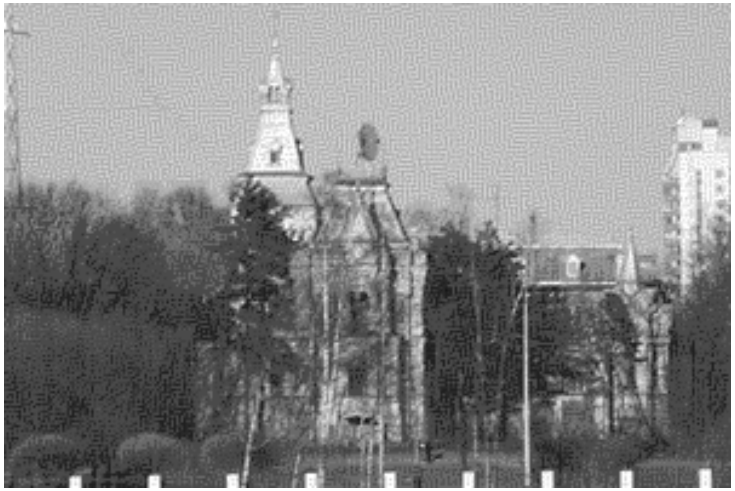
3. The size of given image is 199x300px. Nmax = 11,443 bits.

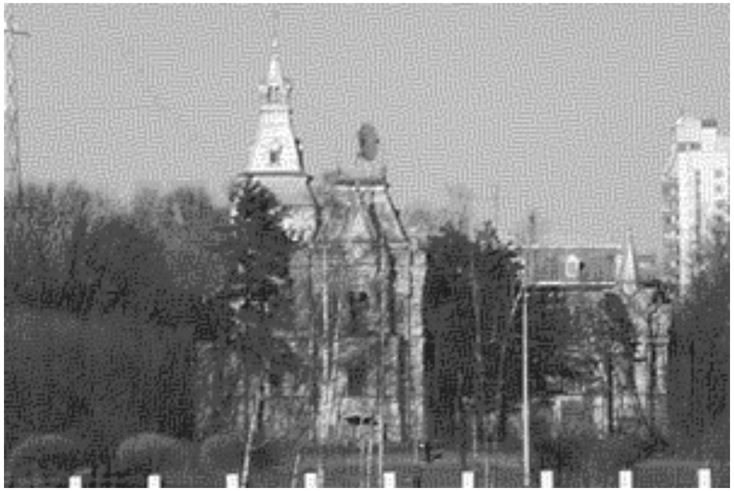
4. The size of given image is 200x300px. Nmax = 4,051 bits.





5. The size of given image is 200x300px. Nmax = 13,747 bits.





The obtained results are presented in the table below

№	car	1	2	3	4	5
N_{max}	4,740	6,330	12,057	11,443	4,051	13,747

The presented data allow to conclude that in average 5,000-10,000 bits of additional information can be embedded into 8-bits gray-scaled image containing 200x300px.

In this method the possible embedding capacity depends on the size and luminance distribution of image which varies while image color depth changes.

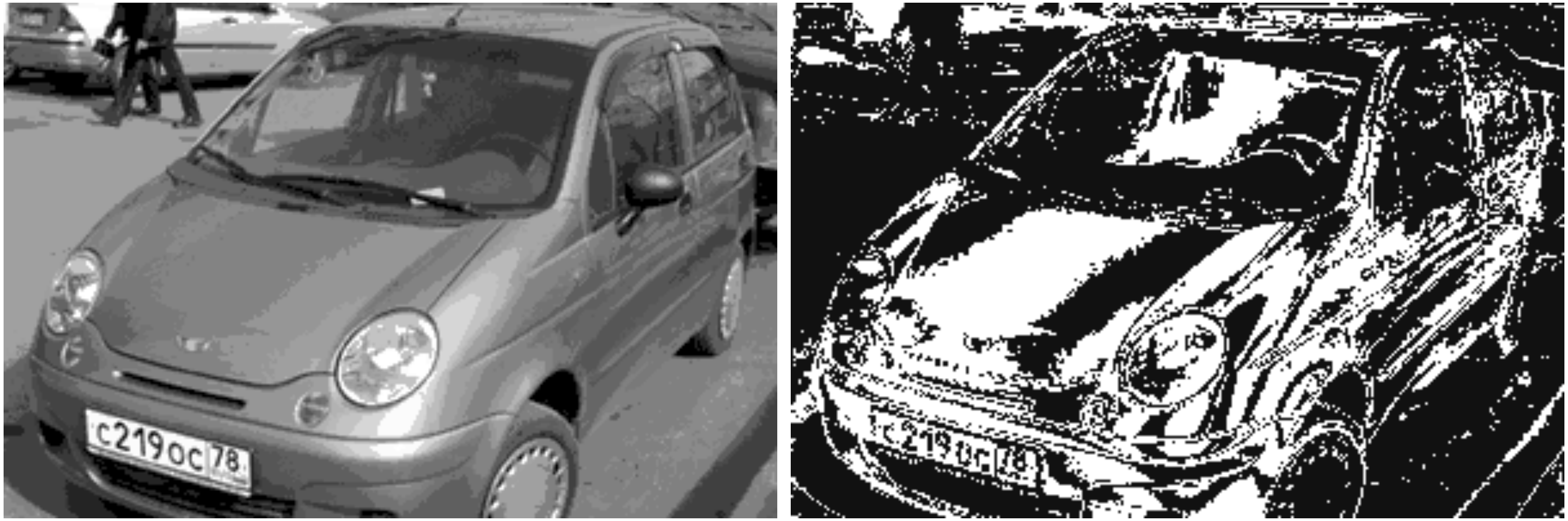
Steganalysis of SG-LSB-R method:

comparison of regular SG-LSB and SG-LSB-R methods

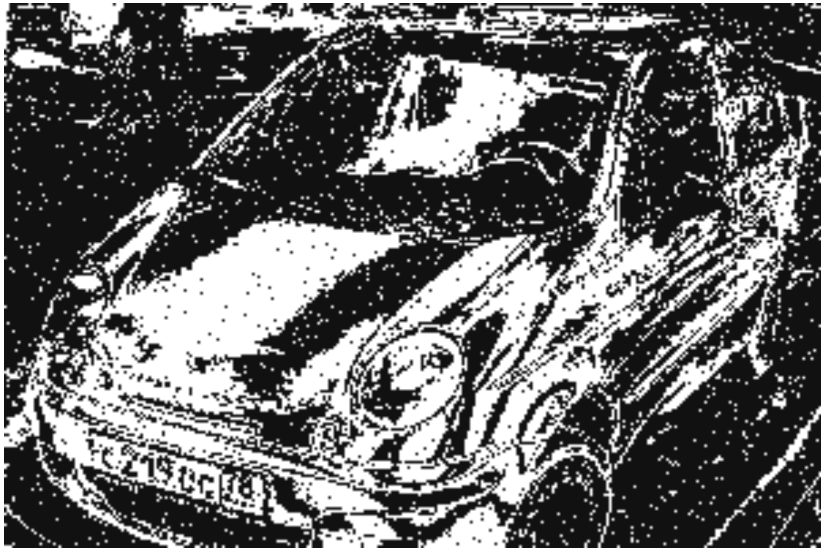
Visual attack

Visual attack means extraction of LSB from the image. The clear contour of image content means absence of embedding otherwise we will see noises which will depend on the size of embedding.

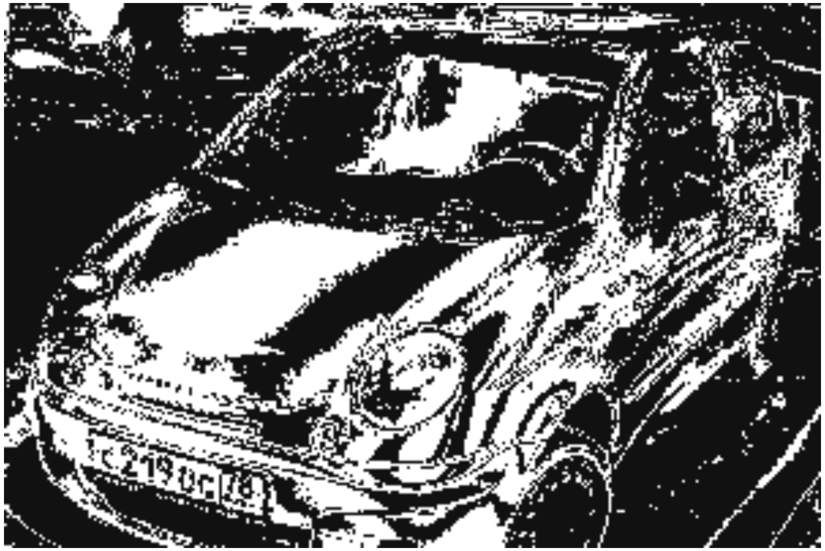
Visual attack on the original image is presented



Let compare the results of visual attacks on SG-LSB and SG-LSB-R methods.



SG-LSB



SG-LSB-R

3,000 bits of information have been embedded. In the case of regular SG-LSB embedding we obtain hardly noised picture. While in the case of SG-LSB-R method the fact of embedding cannot be detected rather simply and comparison with the original image is necessary. At decrease of embedded information (for example to 1,000 bits and lower) the fact of embedding becomes not eyes-obvious.

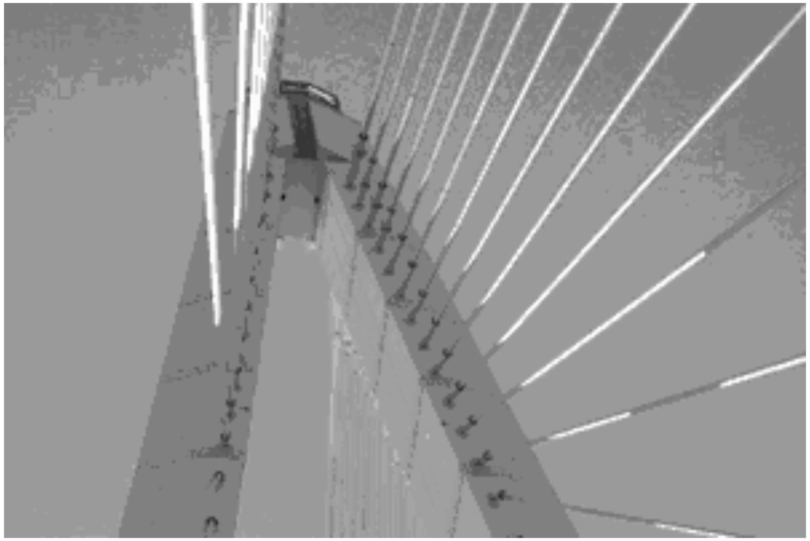
Other methods of SG-LSB-R steganalysis

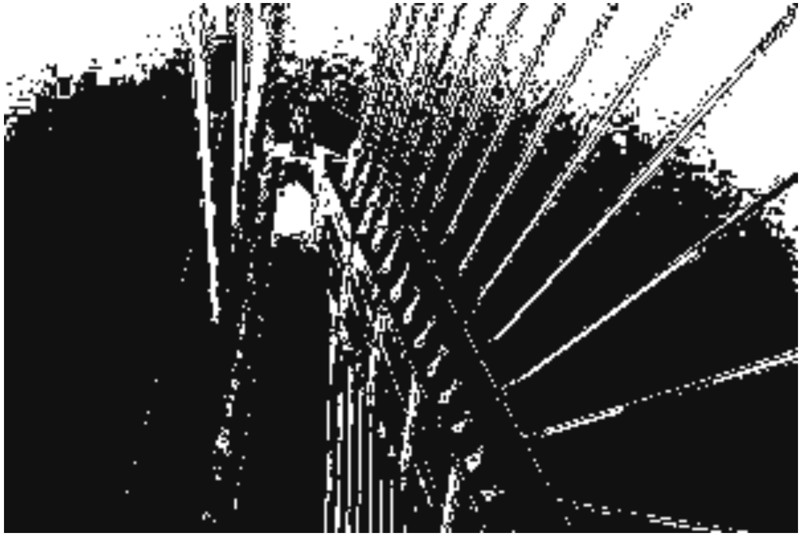
By means of «test» and «Gerl-3» software developed by PhD student of ISTS department K. Gerling the statistics of great number of images has been obtained.

The following attack were applied:

- First-order statistical attack (FOSA)
- Second-order statistical attack (SOSA)
- «Zeros of histogram» attack (ZHA)
- «Neighboring values» attack (NVA)

Examples of results of attacks

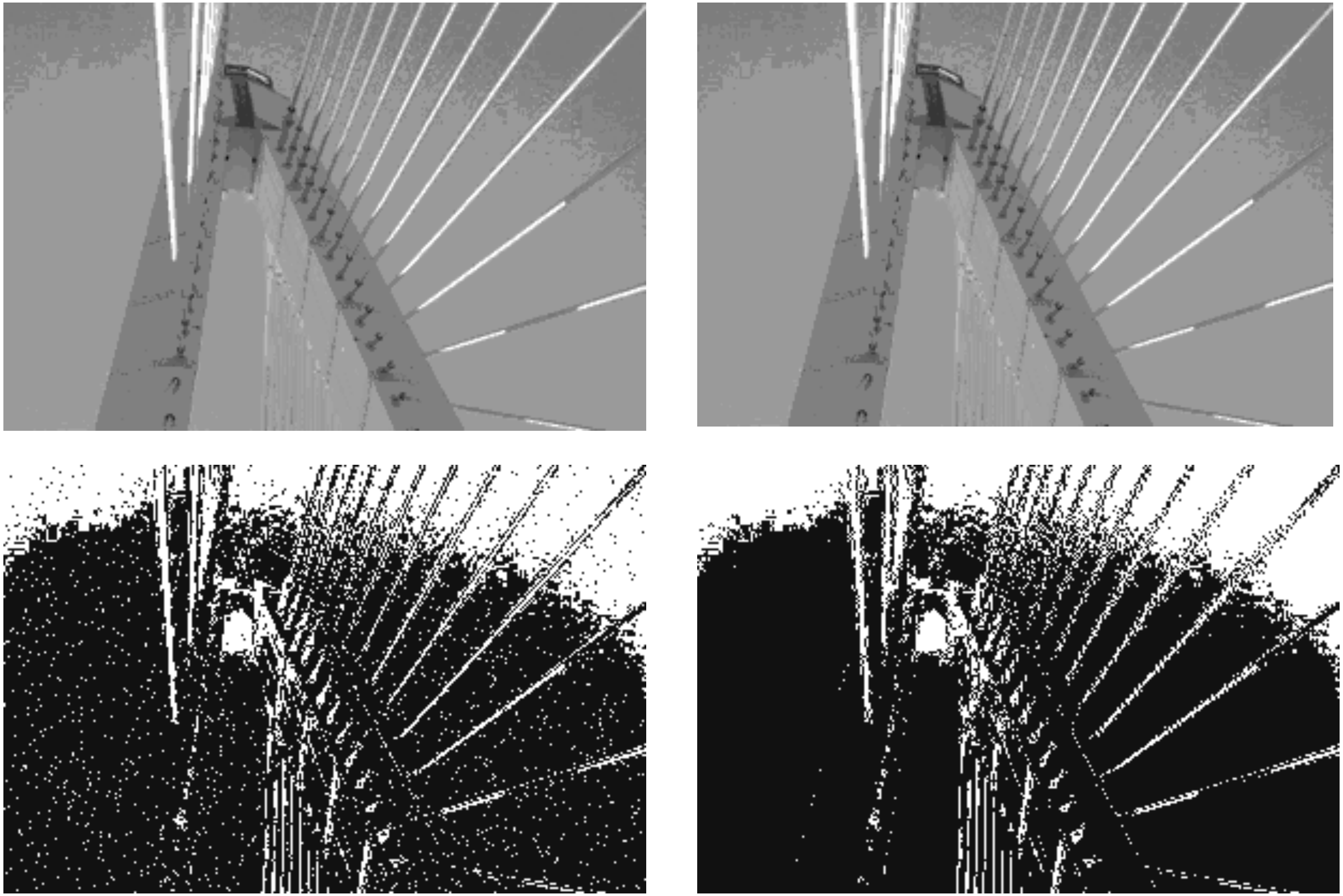




method	FOSA	SOSA	ZHA	NVA
SG-LSB-R	detected	not detected	not detected	not detected
SG-LSB	detected	detected	not detected	not detected

3,000 bits have been embedded nevertheless the SOSA did not detected the fact.

The results of visual attacks for methods SG-LSB (left-hand side picture) and SG-LSB-R (right-hand side picture) at 3,000 bits of additional information embedding are presented.



Conclusion

1. The SG-LSB method has been investigated. By means of this method embedding into and extraction from gray-scaled images were simulated.
2. It was showed that the direct usage of SG-LSB-R method leads to unacceptable CO distortion.
3. This method was proposed to use in practical applications deal with LSB of image.
4. Embedding by means of the SG-LSB-R method has been simulated. The correct extraction of information was showed.
5. Steganalysis of SG-LSB-R method and its comparison with SG-LSB method were carried out.

Remark

This method can be considered as improved SG-LSB one. In practice SG-LSB should be changed to SG-LSB-R method.