Lecture 9. WM embedding and extraction technique.

Preprocessing of CO

Initially it is very commonly to perform a transform of CO (so called *preprocessing*), next embed WM and perform inverse transorm to get stegosignal (SG). These transforms should provide the required quality of CO and allow to extract later WM for SG reliably. In Fig. 1 it is shown such general scheme .

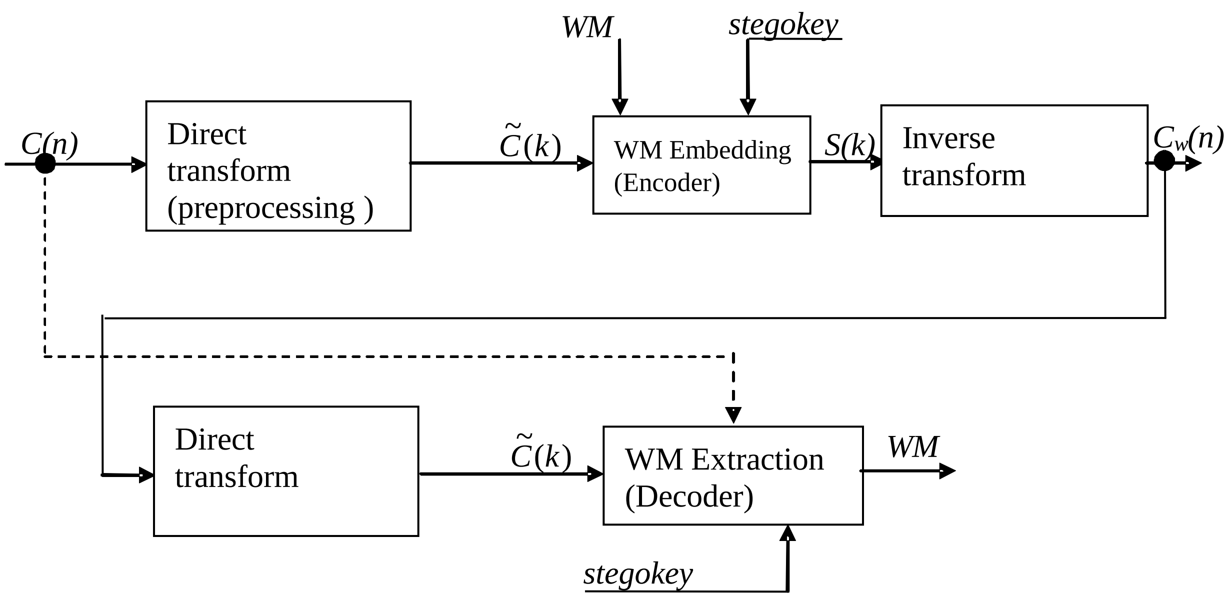


Fig.1. General scheme of embedding and extraction WM with the use of CO preprocessing

Common types of preprocessing

- Discrete Fourier Transform (DFT);
- Discrete Cosine Transform (DCT);
- Walsh Discrete Transform (WDT);
- Expansion in Appropriated Series (EAS);
- Expansion in Matrix Product (EMP);
- and so on.

The reason to be useful preprocessing

- Distortions of CO can be taken into account easier than for direct embedding;
- It is easier to design embedding and extraction methods that are robust to natural and deliberate transforms

Specification of transforms [20]

DFT

$$F(u,v)=\sum_{n=0}^{N-1}\sum_{k=0}^{N-1}C(n,k)\exp\{\frac{-2\pi j(uk+vn)}{N}\} \tag{1}$$

IDFT

$$C(n,k)=\sum_{n=0}^{N-1}\sum_{k=0}^{N-1}C(u,v)\exp\{\frac{2\pi j(un+vk)}{N}\} \tag{2}$$

DCT is more commonly than DFT because DCT is used also in JPEG format

$$\tilde{C}(u,v)=\alpha(u)\alpha(v)\sum_{n=0}^{N-1}\sum_{k=0}^{N-1}C(n,k)\cos(\frac{\pi}{N}u(k+\frac{1}{2}))\cos(\frac{\pi}{N}v(n+\frac{1}{2})) \tag{3}$$

IDCT

$$C(n,k)=\frac{2}{N}\sum_{n=0}^{N-1}\sum_{k=0}^{N-1}\alpha(n)\alpha(k)\tilde{C}(u,v)\cos(\frac{\pi}{N}u(n+\frac{1}{2}))\cos(\frac{\pi}{N}v(k+\frac{1}{2})) \tag{4}$$

$$\begin{cases}\alpha(\omega)=2^{-1/2},\omega=0\\ \alpha(\omega)=1,\omega>0\end{cases}$$

Remark1.

It is commonly to apply DFT and DCT not to complete image but to its consecutive parts like squares consisting of $N_0 x N_0$ pixels

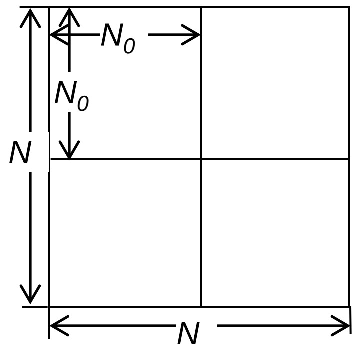


Fig.2.Local transforms DFT and DCT.

Remark 2.

It is commonly to embed WM in the area of middle *spatial frequencies* (see the shaded region in Fig.3) because lower frequencies affect significantly on image quality whereas high frequencies are vulnerable to such attacks as filtering and JPEG compression .

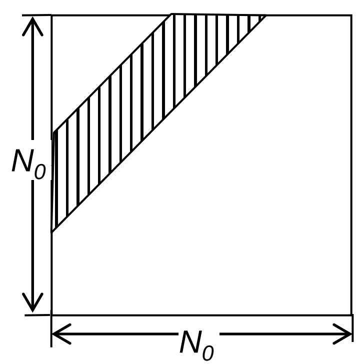


Fig 3. A choice the frequency area for WM embedding .

WDT (audio 1D CO)

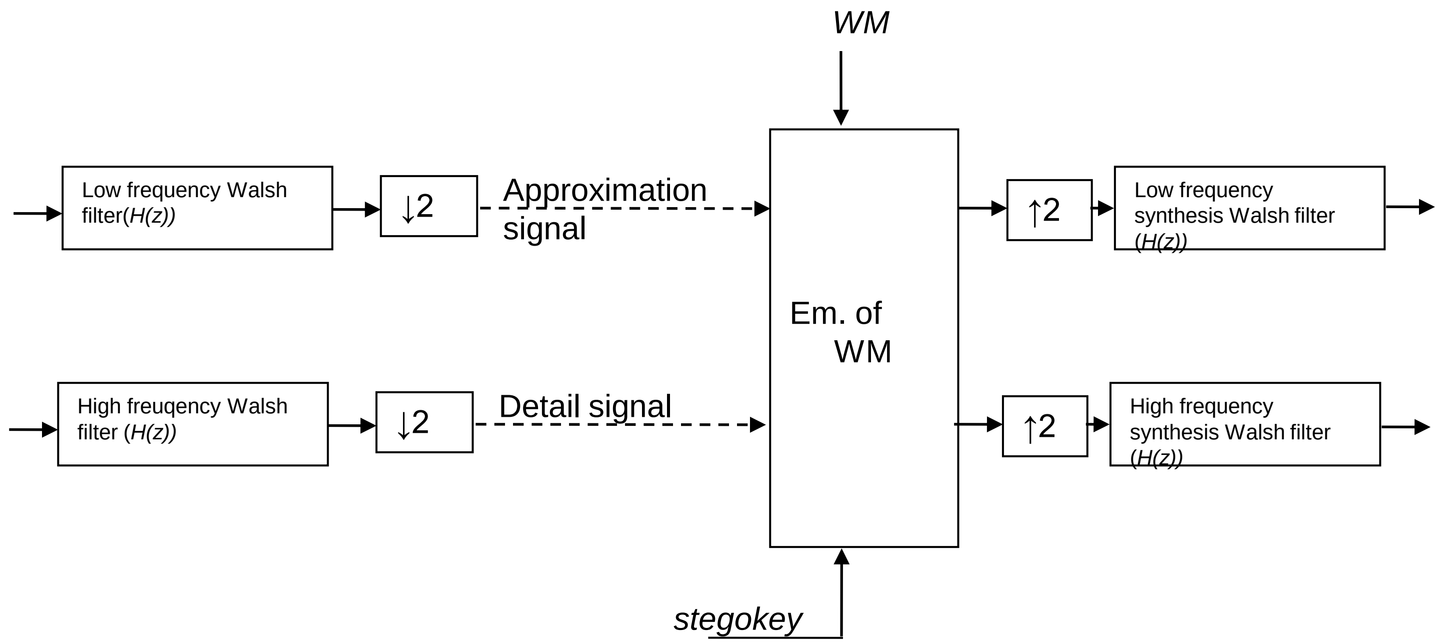


Fig 4.. WDT- based WM

Remark 1. Notations ↓2 and ↑2 mean a frequency changing in two times .

Remark 2. Embedding of WM is possible both in approximation signal (quality of CO decreases) as well as in detail signal (robustness to transforms decreases). However it is more commonly to embed WM only in approximation signal.

Remark 3. DWT-based WM have the lack of shift invariance . The way out is to use so called the *Undecimated Discrete Wavelet transform* (UDWT) or *Complex Wavelet Transform* (CWT) which at the price of a moderate redundancy , offers approximately shift invariance [20]

WDT video 2D CO (

Extension to the 2D case is achieved by applying the above 1D analysis to the rows and columns of images .

An example of image 2- level wavelet decomposition is shown in Fig.5

Fig .5. One step of direct DWT (Haar transform).

Expansion to matrix product [21]

Remember that RGB image format is three real-valued NxN matrices: $\mathbf{C}_R$, $\mathbf{C}_G$, $\mathbf{C}_B$.

Singular Value Decomposition (SVD) is :

$$\mathbf{C} = \mathbf{X}\Lambda\mathbf{Y}^T = \sum_{i=o}^{\Gamma} \lambda_i \mathbf{X}_\mathbf{i} \mathbf{Y}^T{}_i \qquad (5)$$

where **X, Y** are orthogonal $(\mathbf{XX}^T=\mathbf{I}, \mathbf{YY}^T=\mathbf{I})$ MxM и NxN –matrices, $\mathbf{X_1}$, $\mathbf{X_2}$,…. $\mathbf{X_n}$, и Y_1, $\mathbf{Y_2}$,…. $\mathbf{Y_n}$, are their columns , respectively, **Λ** is diagonal matrix with nonzero elements, г≤min{M,N} – rank of matrix **C**. Diagonal elements $\lambda_1, \lambda_2, \ldots \lambda_n$ of matrix **Λ** is called the singular values of the matrix **C** and г – is total number of nonzero singular values . Matrix columns **X** и **Y** are termed as left and right singular vectors of the matrix **C ,** respectively.

Remark 1.

Singular values for any matrices can be simply calculated with the use of «Mathematics» package.

Remark 2.

X and Y are responsible for image geometry (image contours), whereas each of singular value λ_i is responsible for luminance (energy) of some SVD levels

WM embedding based on SVD

An embedding is performed in the most SVs of small blocks (actually in low frequencies of CO).

Simulation of such WM systems [21] shows their good robustness to transform bmp into JPEG providing good quality CO after embedding .

The embedding rate is about 0.005 with respect to image size in bmp format.

The main embedding methods of WM (before or after preprocessing)

1. Embedding in LSB.
2. Embedding based on concept of *frequency hopping* (FH) that is very popular in communication systems as anti jamming method .
3. Additive embedding of *spread spectrum signals* (SS).
4. Multiplicative embedding of SS.
5. Additive embedding using CO more effectively (*informed encoder*)

1. Embedding in LSB (It was considered in Part 1 .As we already know this WM can be removed very easily by LSB randomization. Therefore this approach is suitable only for 1 and 2 WM applications (see lecture 8).
2. FH-based WM embedding (see next slide).

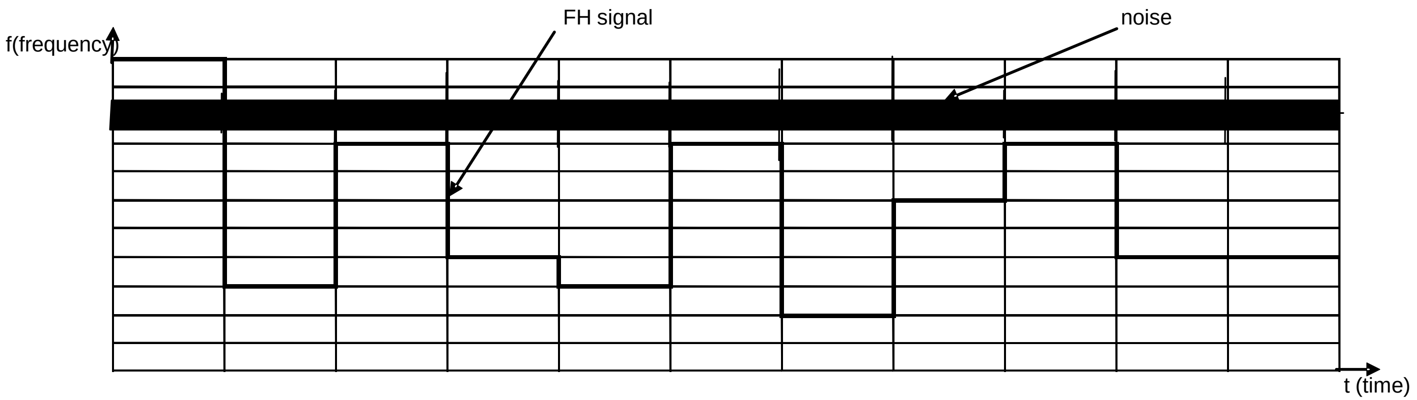


Fig. 6. FH concept in communication systems

In the case of WM the embedding is performed on pseudo random chosen (by stegokey) frequencies (coefficients DFT, DCT, DWT) with large amplitude that does impossible to remove this information , say by adding noise on all frequencies because it results in large distortion of CO.

3. Additive embedding of SS (see Lecture 3 and [22] for details)

$$C_w(n) = C(n) + \alpha(-1)^b \pi(n), n = 1,2...N \qquad (6)$$

Remark. Similar to (6) one can embed WM in «frequency» domain.

Robustness of SS-based WM under the additive noise attack

$$C'_w(n) = C_w(n) + \varepsilon(n), \text{ where } \varepsilon(n) \in i.i.d. \; \mathrm{E}\{\varepsilon(n) = m_c\}, Var\{\varepsilon(n)\} = \sigma_\varepsilon^2 \qquad (7)$$

Blind decoder:

$$\sum_{n=1}^{N} \left(C'_w(n) - m_c\right)\pi(n) = \Lambda, \begin{cases} b = 0, if \;\; \Lambda \geq 0 \\ b = 1, if \;\; \Lambda < 0 \end{cases} \qquad (8)$$

$$p \approx Q(\sqrt{N/\eta_w}), \text{ where } Q(x) = \frac{1}{\sqrt{2\pi}} \int_x^\infty e^{-\frac{t^2}{2}} dt \leq \exp(-\frac{x^2}{2}), \eta_w = \frac{\sigma_c{}^2}{\alpha^2}, \sigma_c{}^2 = Var\{C(n)\} \qquad (9)$$

Informed decoder

$$\sum_{n=1}^{N}\left(C'_w(n)-C_w(n)\right)\pi(n)=\Lambda,\begin{cases} b=0, if\ \ \Lambda\geq 0 \\ b=1, if\ \ \Lambda<0 \end{cases} \tag{10}$$

$$P=Q(\sqrt{\frac{N}{\eta-1}}),\ \text{where}\ \eta=\frac{\eta_w}{\eta_a},\ \eta_a=\frac{\sigma_c^2}{\alpha^2+\sigma_\varepsilon^2} \tag{11}$$

4. Multiplicative SS-based WM

$$C_w(n)=C(n)(1+\alpha(-1)^b\pi(n)) \tag{12}$$

Signal-to-noise ratio

$$\eta_w=\frac{\operatorname{var}\{C(n)\}}{\operatorname{var}\{C_w(n)-C(n)\}}=\frac{\sigma_c^2}{\alpha^2(\sigma_c^2+m_c^2)},\ \text{where}\ m_c=E\{C(n)\} \tag{13}$$

In particular case m_c=0, we get from (13)

$$\eta_w=\frac{1}{\alpha^2} \tag{14}$$

Comparison of multiplicative and additive WM embedding

In the case of multiplicative embedding the proof of formula for the probability of error after decoding is hard problem. Moreover this formula is rough that requires its specification by simulation.

We can conclude after simulation that multiplicative embedding is superior to additive one for small noise power and inferior for opposite condition .

Remark regarding multiplicative embedding.

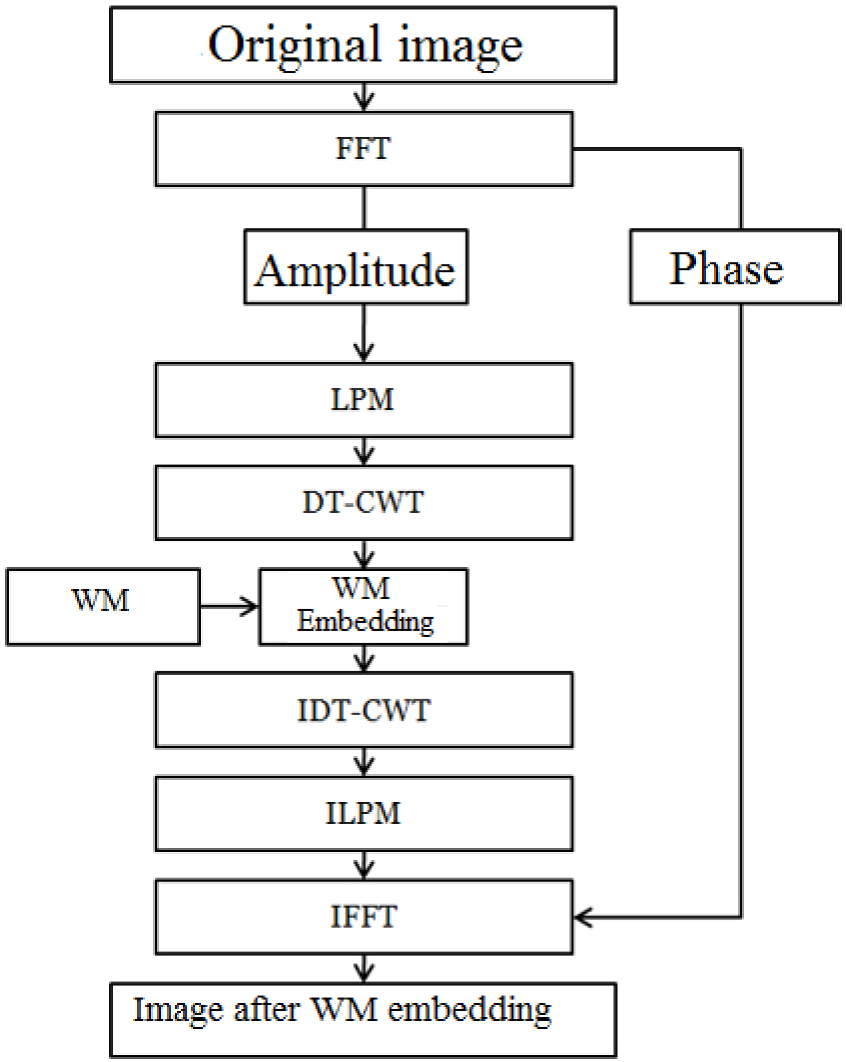
We can see from (12) that multiplicative embedding is *CO- driven* and therefore if the embedding is performed in frequency domain the distortion of CO reduces because energy of the embedded WM is proportional to CO energy on frequency of embedding.

This type of embedding is less vulnerable to attack by estimation and subsequent subtraction of WM (see Lecture in the sequel).

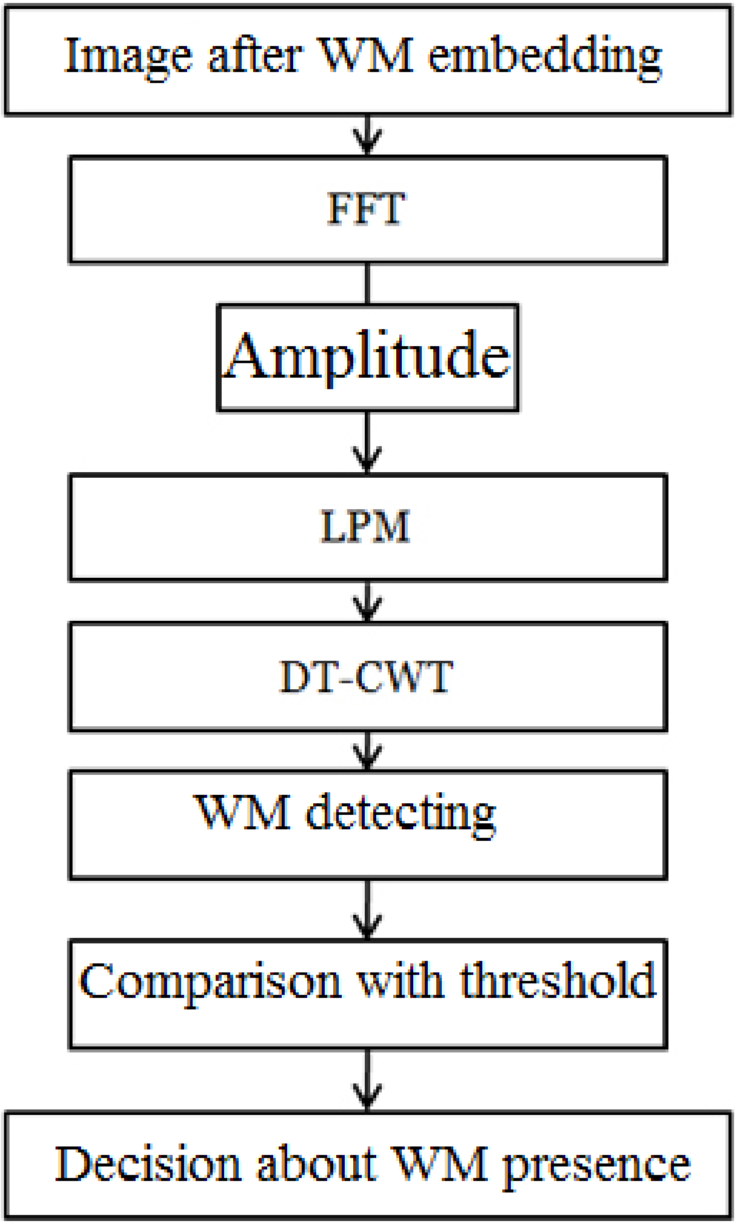
Signal-to-noise ratio (see eq.(14)) does not depend on σ_c^2, that is very useful property if this value varies in time.

5. Examples of robust WM.

*5.1. Embedding into the area wich is tolerant to some transforms(Fourier-Mellin Transforms)***.**



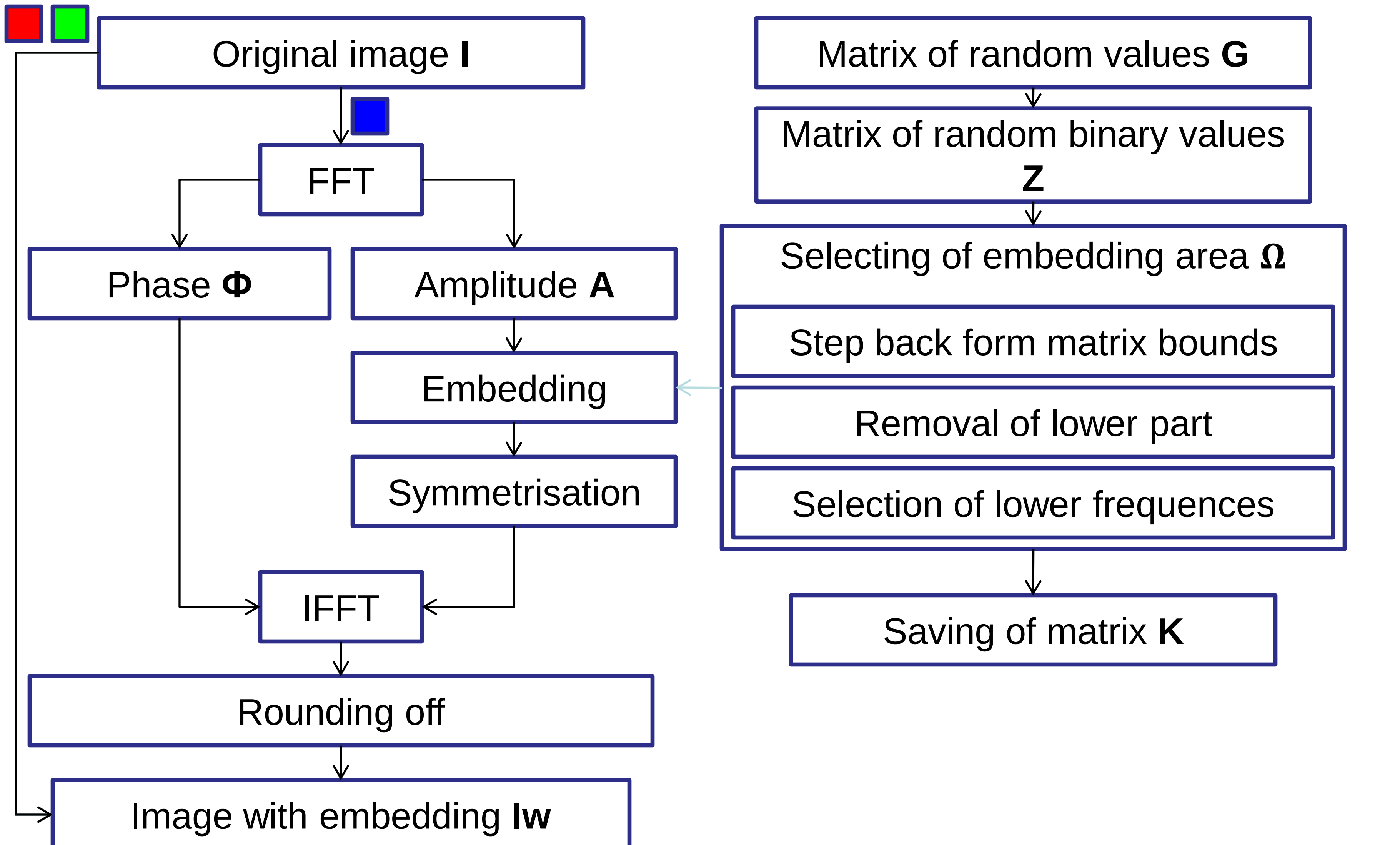
a) Embedding procedure

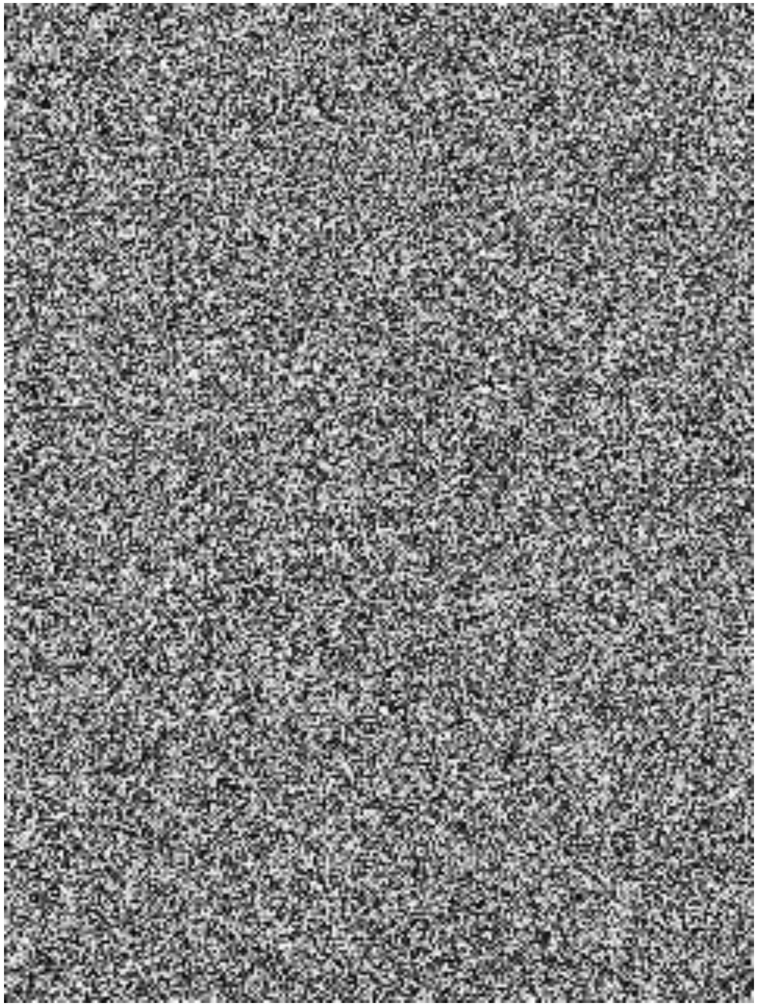


b) Extracting procedure

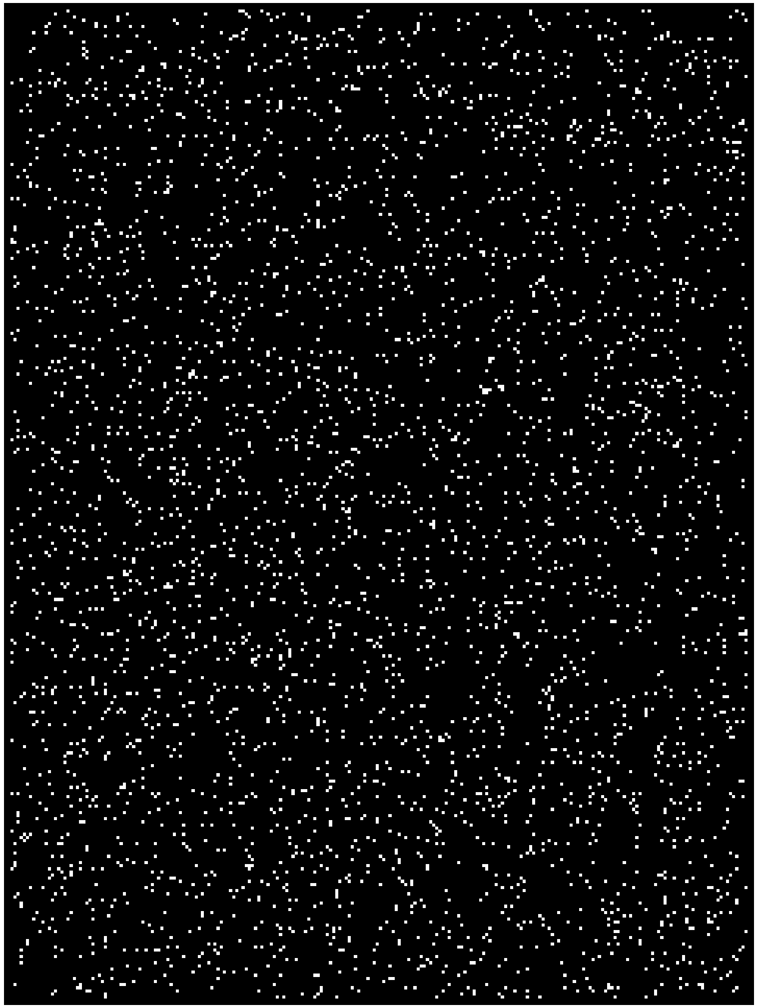
5.2. Embedding of 0 bit WM based on locations of maxima [59]

Scheme of embedding

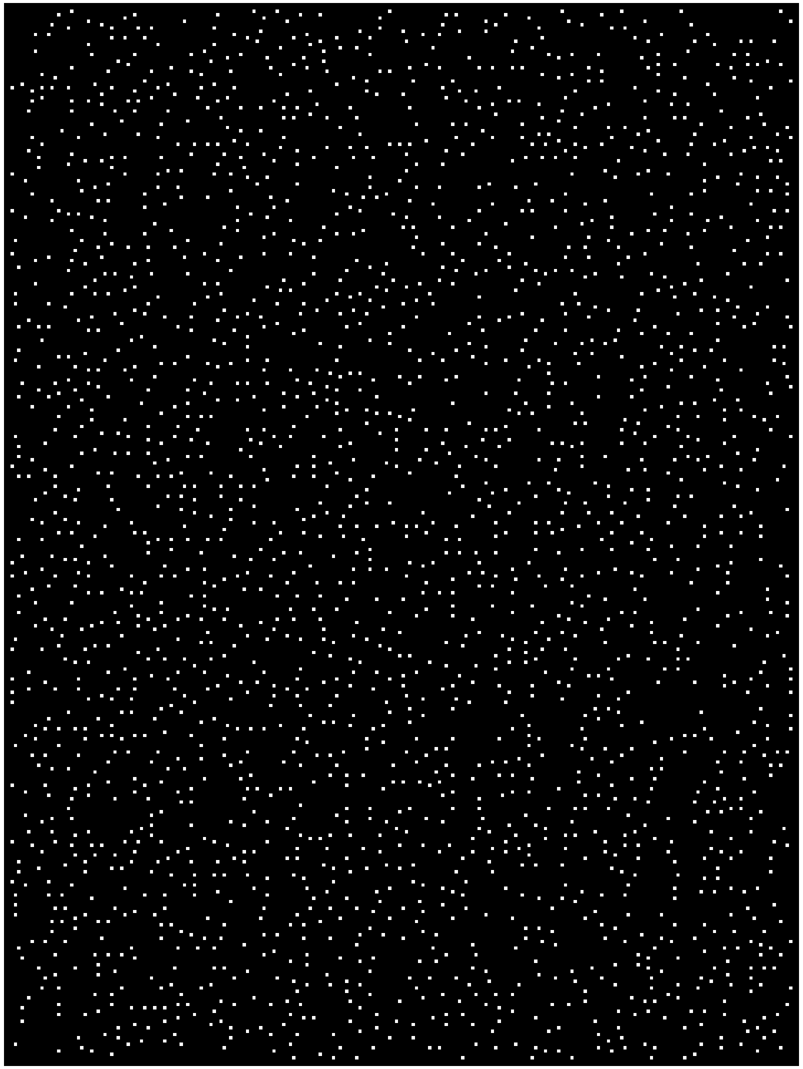




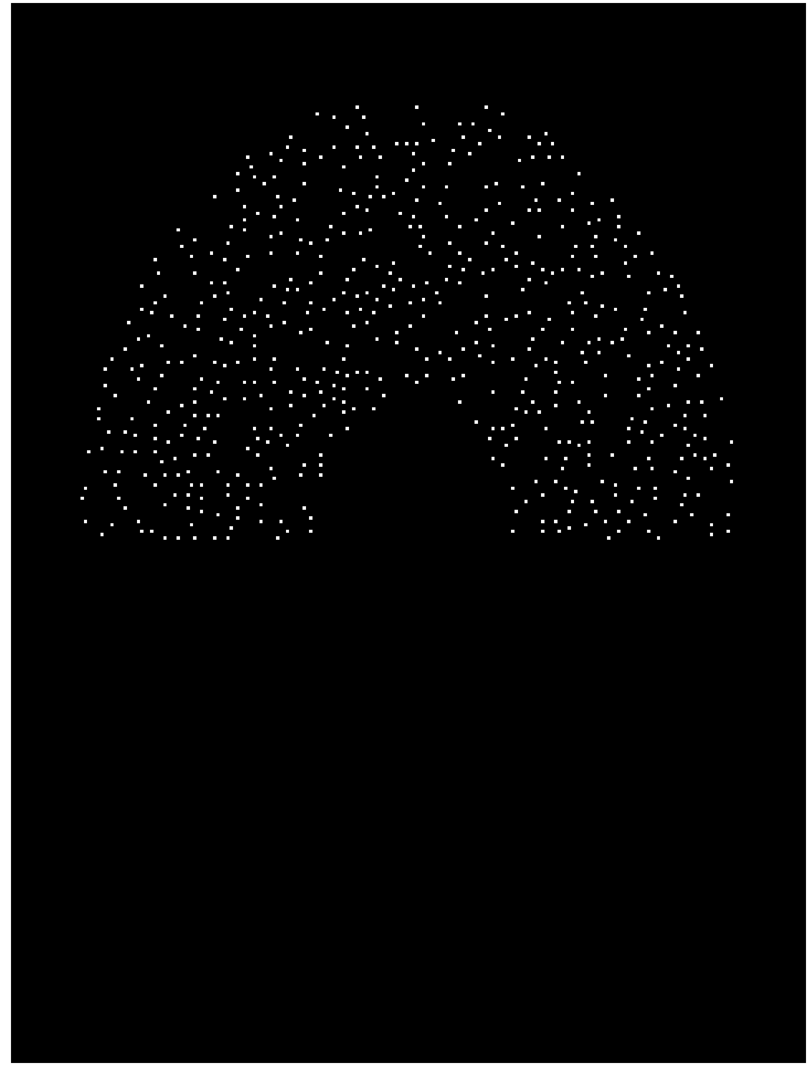
Matrix G of mutual independent uniformly distributed random values



Matrix Z –result of matrix G comparison with threshold that determines the amount of ones.



Matrix L after removal of close located ones in matrix Z.



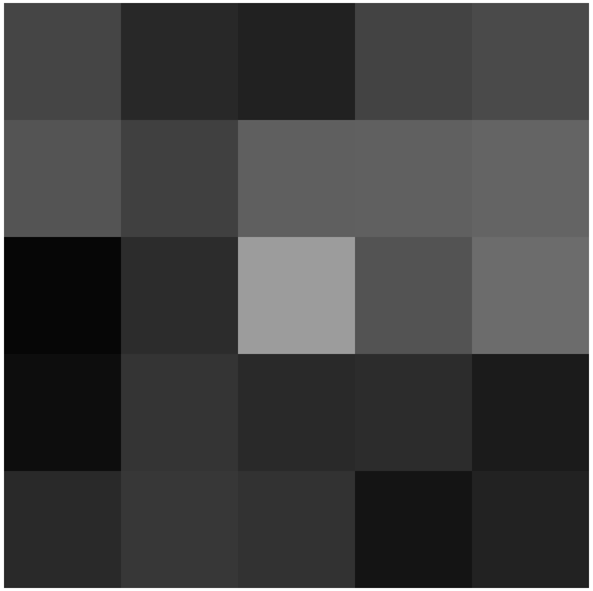
Matrix K after a selection of embedding area **Ω**

WM embedding

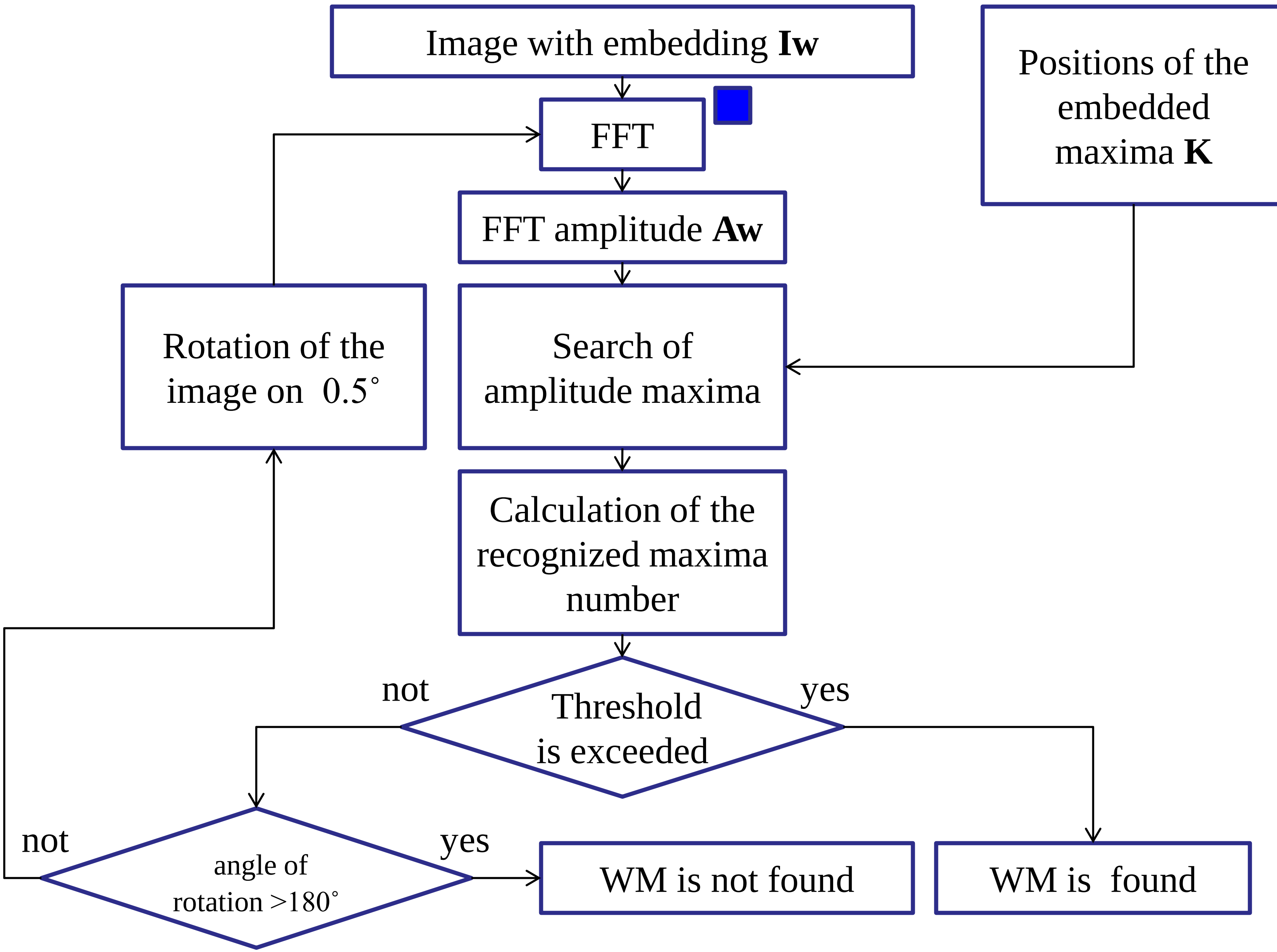
$$A_w[i,j] = \max A\,[i-a..i+a, j-a..j+a] * \beta\ если\ K[i,j] = 1$$

$$A_w[i,j] = A[i,j]\ если\ K[i,j] = 0,$$

where A is an amplitude of two dimensional FT , coefficient **a** determines the size of area for searching of maximum, **β** is depth of embedding.



Scheme of extraction



WM detecting procedure

$S[i,j] = 1$, if $K[i,j] = 1$ u $x_0 = i, y_0 = j$,

$S[i,j] = 0$,for another points.

where x0, y0 are coordinates of maxima in the area δ, **Aw** in vinisity of the point i , j.

$$\Delta = \frac{\sum_{i=0}^{M-1}\sum_{j=0}^{N-1} S[i,j]}{\sum_{i=0}^{M-1}\sum_{j=0}^{N-1} K[i,j]}$$

whe: **Δ** - is a ratio of recognized maxima amounts to total amount of maxima.

WM is resistant to cyclic shifts

Original image

Δ =0.92808

Cyclic shift on 10%

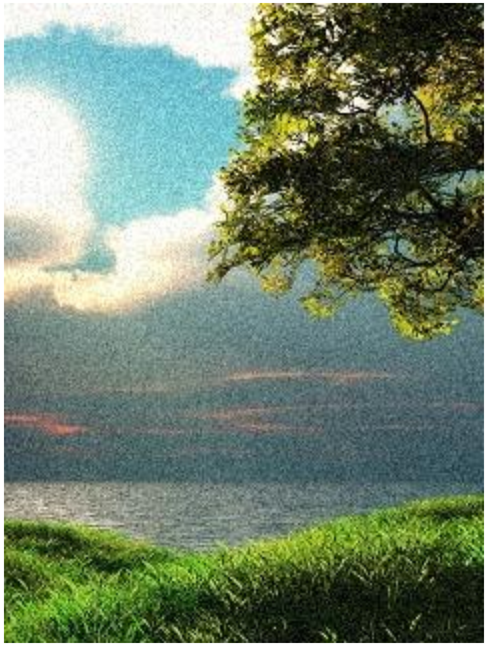
Δ =0.92743

Cyclic shift on 50%

WM is found in 100 cases after 100 tested images.

.

WM is found successfully after noising



Δ =0.7343

SNR is 100

Δ =0.28575

SNR is 20

Δ =0.14997

SNR is 10

The Probability that WM is found

99% 95% 89%

Removal of rows

Δ =0.83326

Removal of 1% rows

Δ =0.55875

Removal of 10% rows

Δ =0.23189

Removal of 50% rows

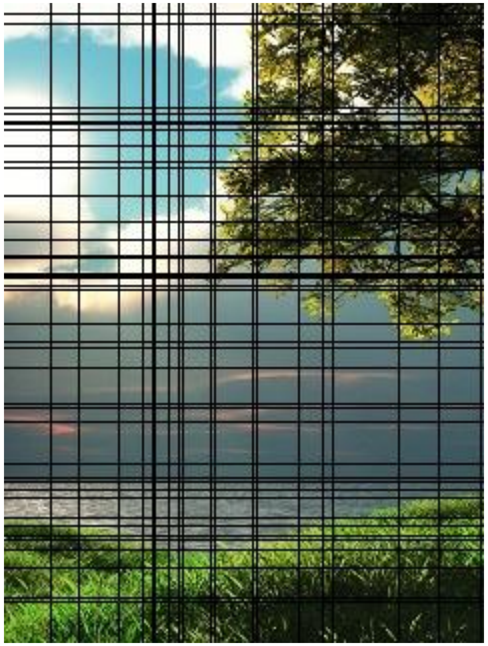
The probability of successfully recognition of WM is 100%

.

Removal of columns

$\mathbf{\Delta}$ =0.28235

Removal of 50% columns



$\mathbf{\Delta}$ =0.24798

Removal of 10% columns and rows .

The probabiliyu of successfully recognition of WM is 100%

.

WM cropping

$\boldsymbol{\Delta}$ =0.22337

Removal of 50%

$\boldsymbol{\Delta}$ =0.1531

Changing of 50%

The probabilities of successfully WM recognition are:

98% 89%

Image scaling

Original image

Δ =0.76563

Scaling on 20%

Δ =0.30711

Scaling on 50%

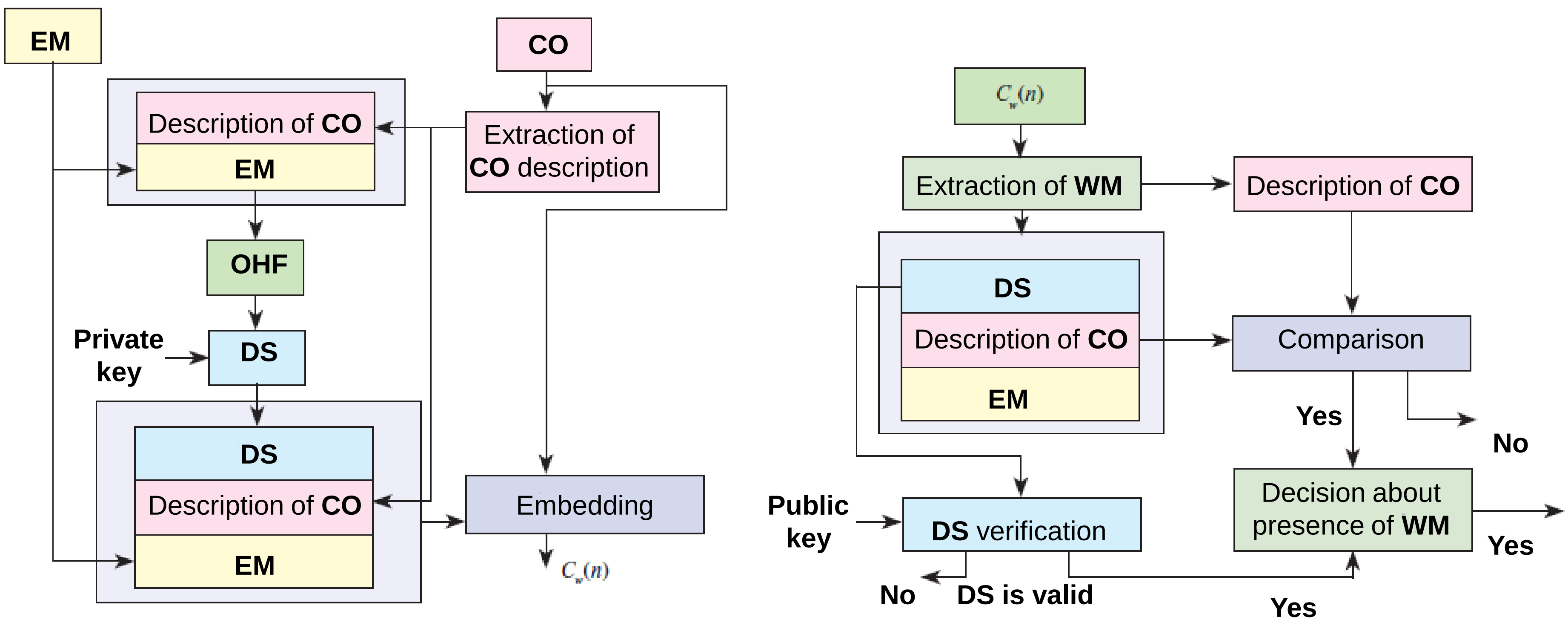
Δ =0.14674

Scaling on 70%

The probabilities of successfully WM recognition :

100% 100% 97%

Copyright verification Scheme using Digital Watermark and Digital Signature



Ambiguity attack against 0-bit WM with the use of local maxima

Ambiguity attack allows to prove for an attacker that his (her) WM is also presented in CO.

The conditions for an attacker (E) before its implementation (activity):

1. E knows WM embedding and extraction algorithm completely (including the size of local area and "density" of local maxima) but does not know secret stegokey and as a consequence the exact positions of local maxima.
2. After attack cover object (image) cannot be significantly corrupted.

What E does?

E generates truly random key and embeds WM according to legal (known for her) algorithm.

After such attack E is able to prove a presence of her WM and corresponding key independently on presence in this CO legal WM.

Fidelity of CO slightly degrades but not very much, that can be provided by selection of appropriated parameters for E’s WM.

The main idea to compromise E is to prove that her WM was embedded after later embedding of legal WM.

Let us consider how this condition can be provided.

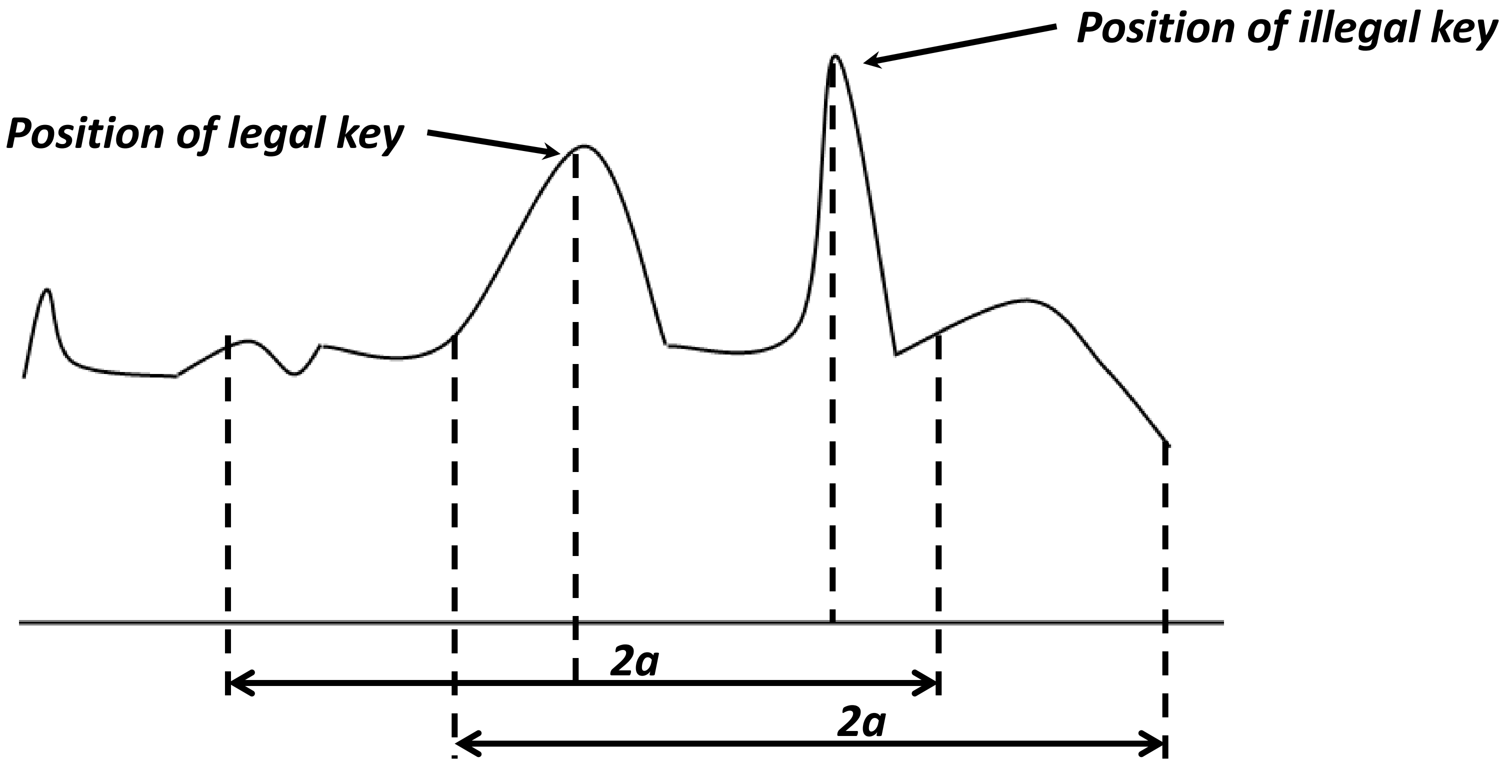
Algorithm for legal user that can realize the main idea is:

1. Legal user (say B) finds the local areas where he selects maxima in line with his stegokey.
2. B counts the number λ of such areas but only if maxima are not coincide with his stegokey and compares it with given threshold λ_0.

If $\lambda \geq \lambda_0$ then B is real owner of WMed image.

Otherwise this conclusion cannot be done.

This scenario is presented in Fig. below (for simplicity two-dimensional $2a$x$2a$ areas are replaced by one dimensional areas)



It is easy to see that if CO was not transformed (corrupted) after WM embedding it is sufficiently to find at least one such area to prove that the greater maximum was created later and hence it was created by attacker.

Under the condition of possible image corruption after WM embedding some threshold $\lambda_0>1$ should be selected.

The algorithm to find "a later embedding" fails in the case when distance between all positions of a legal and illegal key is greater than *a.* Thus the parameters of legal 0-bit WM system should be selected in such a way that the probability of such event be negligible small.

Results of simulation for different n×n images and different number of ones in the key are shown in the table below.

Size of image	100×100	100×100	100×100	1000×1000	1000×1000	1000×1000
Number of legal local areas	96	247	79	480	27064	154
Number of failed maxima	7	149	26	120	14910	91

We can consider from this table that "later embedding" can be easily detected.

There is more sophisticated attack to break the algorithm mentioned above.

In this setting an attacker selects randomly disjoint local areas and puts ones at her stegokey in maxima of selected areas. However such attack can be easily compromised because the attacker is unable to prove in a court that such key was generated according to her digital signature and identification date.

More detail prove of ambiguity attack breaking is still an open problem.

.

Conclusion

1. This WM system is resistant to the following attacks:
   - Cyclic shift
   - Additive noise
   - Removal of rows and columns
   - Cropping and changing of the image partly
   - Image rotation
   - Scaling
   - Ambiguity attack

2. Image saves a good quality after WM embedding.
3. Original image is not required in extraction procedure.
4. Open problems: lower quality JPEG and copy/scanning .

5.3. Embedding of multiple-bit WM based on “holographic” transform [45].

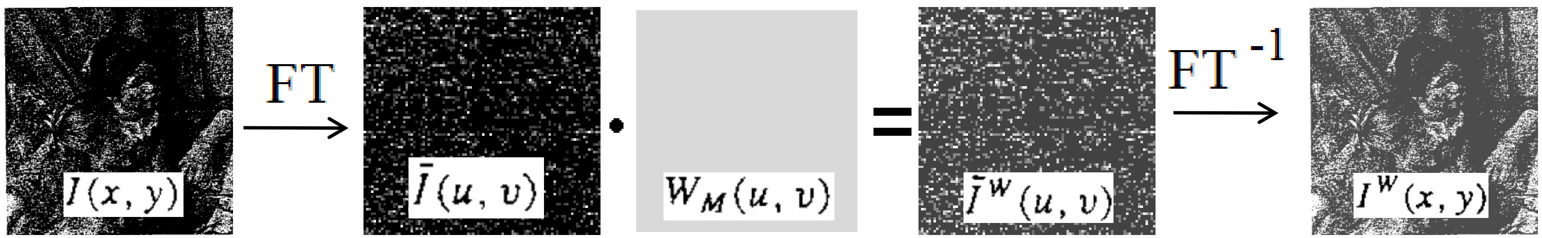
Embedding of WM into amplitudes of FT :

$$M^{W_M}(u, v) = W_M(u, v) \cdot M(u, v)$$

$$M^{W_A}(u, v) = W_A(u, v) + M(u, v) \, ,$$

where $M(u, v)$ – amplitude spectrum;

$W_M(u, v)$ – watermark mask.



$$W_M(u,v) = 1 \pm \varepsilon(u,v),$$

ε- depth of embedding.

$$M(-u,-v) = M(u,v);$$

$$P(u,v) = 2\pi - P(-u;-v).$$

WM extraction for error free case.

- $$\frac{\tilde{I}^W(u,v)}{\tilde{I}(u,v)} = \frac{M^W(u,v)}{M(u,v)} = W_M(u,v),$$

$W_M(u,v)$ – WM mask ;

$\tilde{I}^W(u,v)$ – FT of WMed image ;

$\tilde{I}(u,v)$ – FT of original image;

$M^W(u,v)$ – FT amplitude of WM-ed image;

$M(u,v)$ – FT amplitude of original image.

- It is necessary to know original image.

Extraction of WM after noising

Model:

$$q_i = \alpha \cdot s_i + n_i \ ,$$

$\{q_i\}_{i=1,2,...,k}$ - FT samples of stegosignal ;

$\{s_i\}_{i=1,2,...,k}$ - FT samples of original image;

n_i - FT noise samples ;

α - real value that contains information about WM.

It is necessary to determine the values α by optimal manner.

If n_i has Gaussian distribution with parameters ($0, 2\sigma^2$), then we get the following optimal estimation for α:

$$\hat{\alpha}_{opt} = \frac{\sum_i Re\{q_i^* \, s_i\}}{\sum_i s_i^* \, s_i} = \frac{\sum_i Re\{q_i^* \, s_i\}}{\sum_i |s_i|^2} \underset{\alpha_-}{\overset{\alpha_+}{\gtrless}} \frac{\alpha_+ + \alpha_-}{2}$$

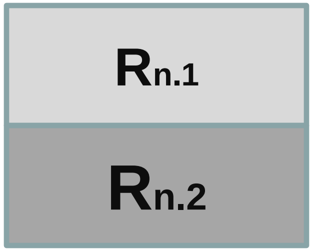
If $\alpha_- = 1 - \varepsilon, \alpha_+ = 1 + \varepsilon$,then:

$$\hat{\alpha}_{opt} \underset{1-\varepsilon}{\overset{1+\varepsilon}{\gtrless}} 1$$

Let us define embedding of WM by differential manner:

$$b_n = 0 \qquad \begin{cases} W(u,v) = 1+\varepsilon & (u,v) \in R_{n,1} \\ W(u,v) = 1-\varepsilon & (u,v) \in R_{n,2} \end{cases}$$

$$b_n = 1 \qquad \begin{cases} W(u,v) = 1-\varepsilon & (u,v) \in R_{n,1} \\ W(u,v) = 1+\varepsilon & (u,v) \in R_{n,2} \end{cases}$$



,

This allows to be resistant to a filtering effect.

.

Decision rule:

$$\frac{\sum_{i \in N_1} Re\{q_i^* \; s_i\}}{\sum_{i \in N_1} |s_i|^2} \underset{b_n=0}{\overset{b_n=1}{\gtrless}} \frac{\sum_{i \in N_2} Re\{q_i^* \; s_i\}}{\sum_{i \in N_2} |s_i|^2}$$

N_1 – set of samples in area $R_{n.1}$;

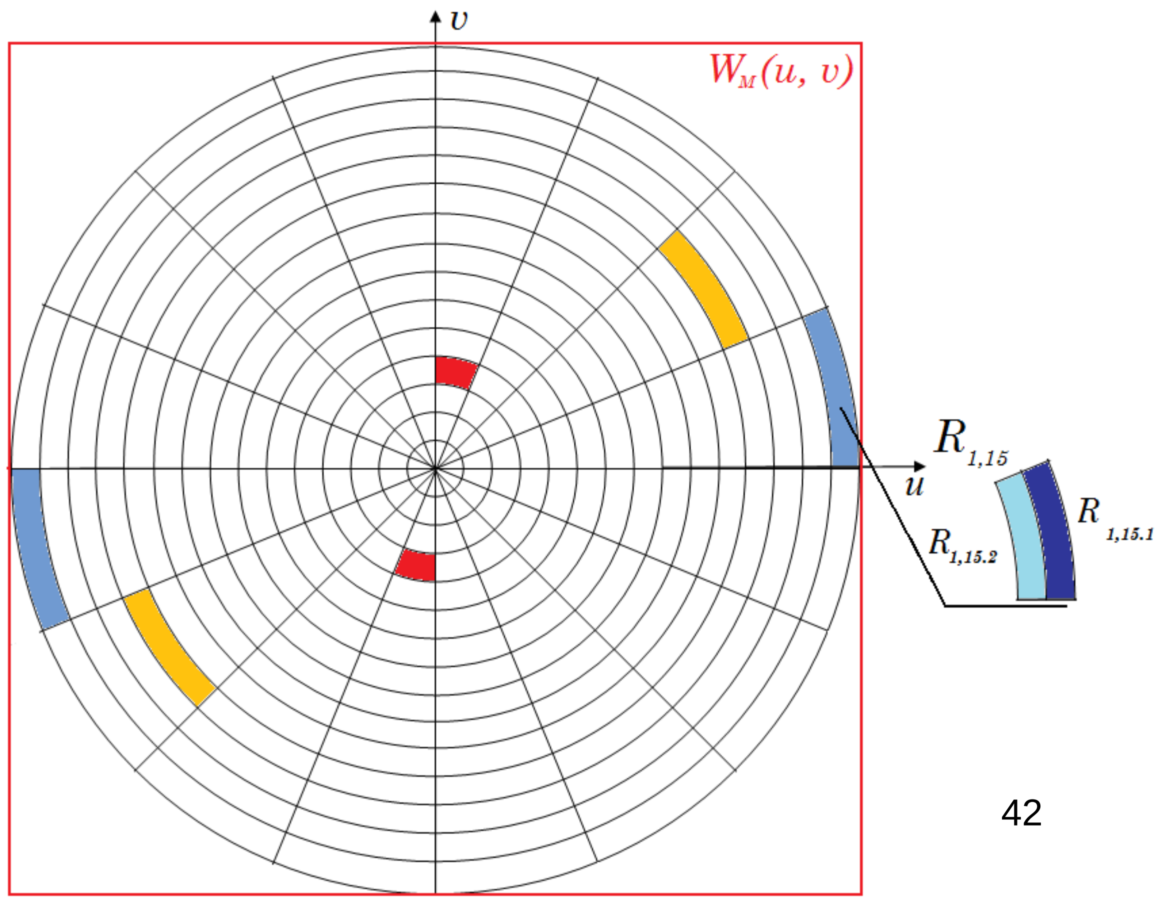
N_2 – set of samples in area $R_{n.2}$.

Example of mask design

$$\mathcal{R}_{m,n} = \left\{ (r,\theta) : r \in [(m-1)\frac{1}{15}, m\frac{1}{15}),\ \theta \in [(n-1)\frac{\pi}{8}, n\frac{\pi}{8}) \right\}.$$

r – radius of sector;

θ – angle $[0;\pi]$.



Condition of symmetry:

$$M^W(-u,-v) = M^W(u,v);$$

Totally is embedded:

$$15 \cdot 8 = 120.$$

Simulation results for images of the size 512x512 pixels.

№	Transforms of WM.	The amount of correctly extracted bits out off 120 embedded bits.
1	Cropping of frame (256 x 256).	80
2	Re-saving in JPEG with quality loss.	90 (55 in LF - area)
3	Changing of contrast.	120
4	Printing and scanning of the whole image.	105
	Printing and scanning of frame (256 x 256) pixels.	95

Concatenated Watermarking [60]

The watermarking technique based on the holographic transform domain (see the section before) is resistant to a bunch of attacks (cropping, removal of row and columns) but it is not resistant to *geometric attacks* (including a *rotation* on small angles).

An image $\tilde{I}(x,y)$ is said to be subjected by *affine distortion* of the original image $I(x,y)$ of the size *M×N* if there is a matrix

$\boldsymbol{A} = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix}$ and vector $\boldsymbol{d}=(d_1,d_2)$ such that $\tilde{I}(x,y) = I(x',y')$,

where $\begin{pmatrix} x' \\ y' \end{pmatrix} = \boldsymbol{A} \cdot \begin{pmatrix} x \\ y \end{pmatrix} - \boldsymbol{d}$

(In particular case if $\boldsymbol{d}=0$ and $\boldsymbol{A} = \begin{pmatrix} \cos\varphi & \sin\varphi \\ -\sin\varphi & cos\varphi \end{pmatrix}$ it is a rotation by angle φ).

The normalization image transform is [61]:

$$\begin{pmatrix} x' \\ y' \end{pmatrix} = \boldsymbol{A}_s \cdot \boldsymbol{A}_x \cdot \boldsymbol{A}_y \cdot \begin{pmatrix} x \\ y \end{pmatrix} - \begin{pmatrix} d_x \\ d_y \end{pmatrix},$$

where: $\boldsymbol{A}_x = \begin{pmatrix} 1 & \beta \\ 0 & 1 \end{pmatrix}, \boldsymbol{A}_y = \begin{pmatrix} 1 & 0 \\ \gamma & 1 \end{pmatrix}, \boldsymbol{A}_s = \begin{pmatrix} \alpha & 0 \\ 0 & \delta \end{pmatrix},$

$d_x = \frac{m_{10}}{m_{00}}, d_y = \frac{m_{10}}{m_{00}}, m_{pq} = \sum_{x=0}^{M-1} \sum_{y=0}^{N-1} x^p y^q I(x, y),$

β - is a solution to the following cubic equation:

$\mu_{30} + 3\beta\mu_{21} + 3\beta^2\mu_{12}\mu + \beta^3\mu_{03} = 0,$

$\mu_{pq} = \sum_{x=0}^{M-1} \sum_{y=0}^{N-1} (x - d_x)^p \left(y - d_y\right)^q I(x, y),$

$\gamma = \frac{\mu'_{11}}{\mu'_{20}}$, where μ'_{11},μ'_{20} are the parameters calculated by relation above but for $I'(x, y) = \boldsymbol{A}_x \cdot I(x, y)$.

$\alpha = \frac{\widetilde{M}}{\widetilde{M}'}$,$\beta = \frac{\widetilde{N}}{\widetilde{N}'}$, where $\widetilde{M}, \widetilde{N}$ are width and height of the normalized image, respectively, $\widetilde{M}', \widetilde{N}'$ are width and height of the of the normalized image $I''(x, y) = \boldsymbol{A}_y \cdot I'(x, y)$.

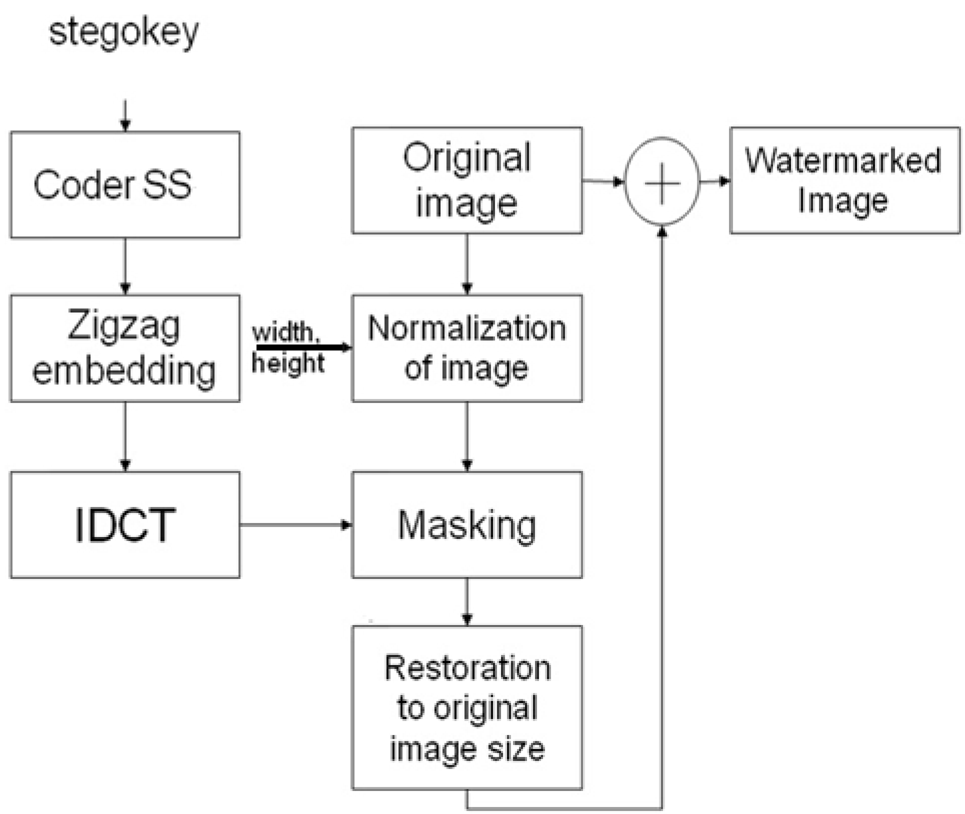
In Fig. below an original image and the same image after affine distortion and normalized image both for original image and after its affine distortion are presented.

(a) (b) (c)

(a)Original image. (b)Image after affine distortion. (c)Normalized image from both (a) and (b).

We can see that an image and its affine transforms have the same normalized images.

Scheme of normalized-based embedding is presented below:



Thus we can conclude that normalized-based method is resistant to affine attacks but it was very sensitive to removal of columns and rows and cropping attack.

The following idea arises: let us combine both methods (holographic-based and normalized-based) in one WM method (called by *concatenated-based WM*) to extend robustness of such system:

a)HE→ NE

b)NE→ HE

After many experiments [60] has been taken a solution HE→ NE against NE→ HE.

The original image (a), holographic-based watermarked image (b), normalization-based watermarked image (c) and concatenated-based watermarked image (d) are shown below:


(a)


(b)


(c)


(d)

The results of investigations after a set of attacks are shown in table below:

Attacks	The probabilities of bit errors, %	
	Holographic decoder	Normalization decoder
Geometric attack (rotation 1 grad)	40.0	3.5
Geometric attack (scaling 1,05)	42.0	3.5
Cropping attack (of window 510 × 510 pixels)	0	47.0
5 rows and 5 columns removal	0	43.3
Saving in JPEG format with Q=60 %	0	1.2
Saving in JPEG format with Q=40 %	2.1	2.8
Addition of Gaussian noise with d = 5	2.0	5.5

We can see that the embedded bits can be successfully extracted by holographic decoder after cropping attack and by normalization decoder after geometric attack.

In order to select which of decoders should be used for bit extraction can be applied encoding by BCH code (63, 10).

In fact, it is sufficiently to select such decoder that gives less Hamming distance between the received vector word and the nearest to it code word. Concatenated WM can be extended to other components and to more than two stages of concatenations.