Lecture 13. Content authentication

The goal of authentication:
Detect a modification (changing) of the message M (to provide its integrity).

Authentication technique («Applied Cryptography» [29])
-Symmetric ($E_S = f(M,K) \Rightarrow (M,E_S)$), where E_S - authenticator, K - the key of

authentication;

verification : $(\tilde{M},\tilde{E}_S) \Rightarrow \tilde{\tilde{E}}_S = f(\tilde{M},K), \tilde{E}_S \stackrel{?}{=} \tilde{\tilde{E}}_S)$

- Asymmetric ,say based on RSA ($S = h^d \bmod n,\ h = h(M) \Rightarrow (M,S)$, where $h(...)$ - keyless hash function, d - secret key to RSA, n - RSA modulo, S - *digital signature* (DS);

verification: $(\tilde{M},\tilde{S}) \Rightarrow \tilde{h} = h(\tilde{M}), \tilde{S}^e \bmod n = \tilde{\tilde{h}}, \tilde{h} \stackrel{?}{=} \tilde{\tilde{h}})$, where e-public key to RSA.

Peculiarity of authentication application in steganography:
Authenticator E_S or DS S have to be embedded in CO but not appended to CO as attachment as it is commonly in cryptography!

Two types of authentication:
1. Exact (fragile) authentication (changing even one bit should be detected)

2. Selective authentication (some distortions of CO should be detected while other (like addition of small noise ,changing of image format ctr.) not.

Authentication paradox in WM:
On one hand any embedding of extra information results in distortion of CO but on the other hand any distortion of CO results in breaking of its authentication.
The way out is in the use of so called *reversible WM*

Applications of WM-based authentication:
- for medical images,
- police (fingerprinting and pictures of criminals),
- cameras of video observation,
- for verification of individual speech,
- for verification of «paper signatures».

Remark. Although reversible WM can be completely removed from WMed message and hence CO can be recovered exactly it is not allowed sometimes to get large distortions of CO *just after embedding* .

The main technique of WM-based authentication

1. Embedding of authenticators in the fields which do not need to be authenticated (service margins , heads ,pauses in speech ctr.)

2. Modular embedding.

3. Compression of CO:
   3.1. The use of additional compression.
   3.2. The use of natural redundancy of CO.

We consider the techniques 2 and 3 because the first method is trivial.

2. Modular embedding[30]

$$C_W = C(n) + (-1)^b \alpha \cdot \pi(n),\ n = 1,2,\ldots, N,\ \pi(n) \in i.i.d,\ \pi(n) \in \{\pm 1\},\ b \in \{0,1\} = \{E_S \text{ or } S\}.$$

$\tilde{C}(n) = C_w(n) - \alpha(-1)^b \pi(n)$, but if $C_w(n) \le \alpha$ or $C_w(n) \ge L - \alpha$, where

L - the number of quantization levels , then there appear non-reversible distortions of CO

The way out: use for WM embedding and WM extraction modular operations:

$$\left.\begin{array}{l} C_w = C(n) \oplus \alpha(-1)^b \pi(n) \\ \tilde{C}(n) = C_w(n) \Theta \alpha(-1)^{\tilde{b}} \pi(n) \end{array}\right| \begin{array}{l} \oplus - addition \bmod L, \\ \Theta - subtraction \bmod L \end{array} \qquad (1)$$

$\tilde{C}(n) = C(n)$, if $b = \tilde{b}$ (decoding procedure is correct)

3. Extension of modular technique on ISS signals [30].

$$C_w = C(n) \oplus (\alpha(-1)^b \Theta x)\pi(n),\ n = 1,2,\ldots, N, \qquad (2)$$

where $x = \left[\frac{\lambda}{N} \sum_{v=1}^{N} C(v)\pi(v) \right]$, […] – means the choice of the nearest quantization level

The feature of modular embedding:

Decoding after modular embedding by (1) results in increasing of the error probability $p = P\{b \neq \tilde{b}\}$ in comparison with ordinary embedding.

WM decoder with modular embedding [30]

1.Centered correlation decoder

$$\Lambda_{CD} = \sum_{n=1}^{N} (C_w(n) - C_o)\pi(n) \Rightarrow \tilde{b} = \begin{cases} 0, if & \Lambda_{CD} \geq 0 \\ 1, if & \Lambda_{CD} < 0 \end{cases}, \qquad (3)$$

where $C_o = \frac{1}{N} \sum_{n=1}^{N} C_w(n)$

2. Optimal modular decoder

$$\Lambda_{MD} = \sum_{n=1}^{N} ((C_w(n) \Theta \alpha\pi(n)) - C_o)^2 - \sum_{n=1}^{N} ((C_w(n) \oplus \alpha\pi(n)) - C_o)^2 \Rightarrow \tilde{b} = \begin{cases} 0, if & \Lambda_{MD} \geq 0 \\ 1, if & \Lambda_{MD} < 0 \end{cases} \qquad (4)$$

3. Differential decoder:

$$\Lambda_{DD} = \sum_{n=0}^{N-1} (C_w(n+1) - C_w(n))(\pi(n+1) - \pi(n)) \Rightarrow \tilde{b} = \begin{cases} 0, if & \Lambda_{DD} \geq 0 \\ 1, if & \Lambda_{DD} < 0 \end{cases} \qquad (5)$$

4.Wiener filter :

$$\tilde{C}_w = C_w(n) - \tilde{C}(n), \quad \text{где } \tilde{C}(n) = wiener(C_w(n)) \qquad (6)$$

For images $C_w(n) = C_w(n_1, n_2)$ (see Matlab):

$$\tilde{C}(n) = \mu + \frac{\sigma^2 - \nu^2}{\sigma^2}(C_w(n_1, n_2) - \mu),$$

where $\mu = (I)^{-1} \sum_{(n_1,n_2) \in I} C_w(n_1, n_2)$, $\sigma^2 = (I)^{-1} \sum_{(n_1,n_2) \in I} C_w^2(n_1, n_2) - \mu^2$, $\nu^2 = \alpha^2$,

I - is some area in vicinity of every pixel.

Calculation of the error probabilities for different methods of WM decoding.
Owing Central Limit Theorem the following relation holds:

$$p = Q(\frac{E(\Lambda)}{\sqrt{Var\Lambda'}}) \qquad (7)$$

However theoretical calculations of $E\{\Lambda\}, Var\{\Lambda\}$ for different Λ (see (1÷4)

occurs very hard and depending on a distribution of CO [30].

α	p	α	p
1	0.45	6	0.487
2	0.24	10	0.439
3	0.053	20	0.352
4	0.122	30	0.301
5	0.328		

Table 1 . The probabilities of errors p for correlation decoder , typical image and $N = 1000$

Remark . For modular embedding the probability of error p is not monotonic decreasing function of “signal amplitude” α !

Calculation of the error probabilities for different embedding and extraction methods followed by Wiener filtering preprocessing [30]

N	Images			
	1		2	
	CD	DD	CD	DD
50	0.0593	0.062	0.0105	0.0077
100	0.02	0.020	0.0044	0.0044
200	0.0035	0.0046	0.0015	0.0019
500	0	0	0.0007	0.0007
1000	0	0	0	0

1- image 1
2 - image 2
CD – correlation decoder
DD – differential decoder
N-the length of PRS

$$\alpha = 3$$

$$I = 3x3 pixels$$

$$L = 256$$

Conclusion. It is possible to embed only 100-300 bits of message in the 256-gray scale image even in the case of the best methods of modular embedding and extraction.

Remark. The images just after modular embedding are still recognizable but there appear distortions known as «salt» and «pepper».

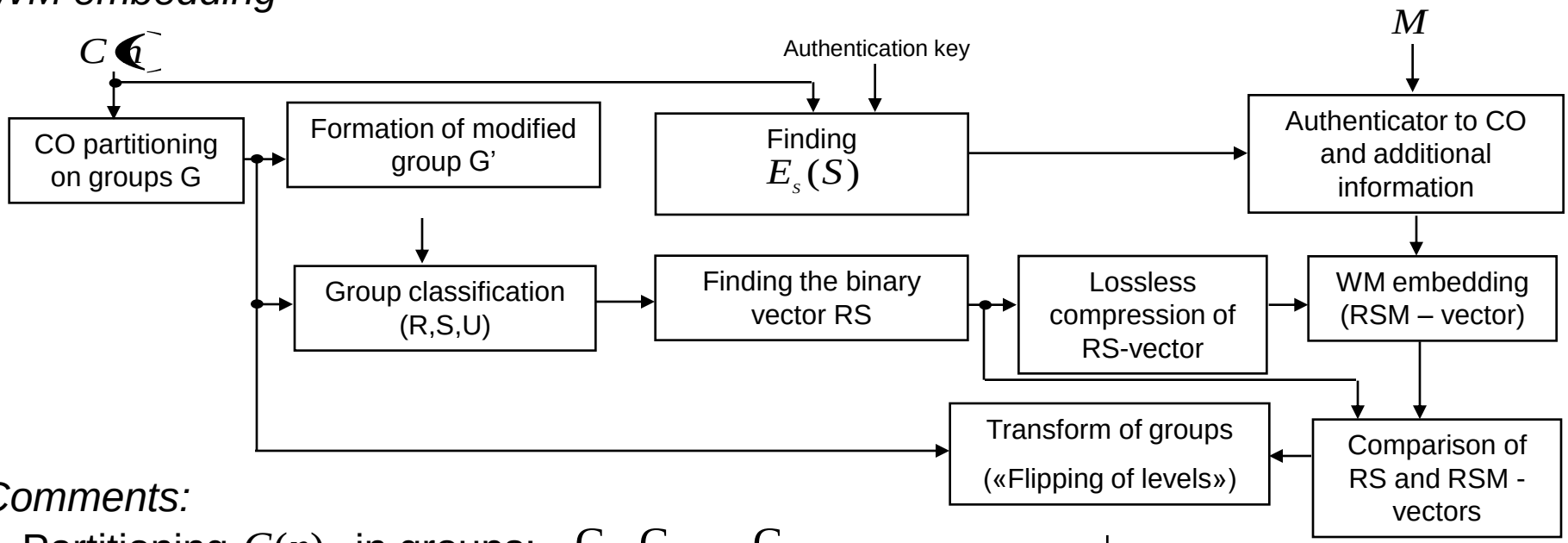
3. Compression-based authentication [31].

3.1. Special compression of the processed image

Fact. It is impossible to perform reversible embedding if CO has no redundancy.

Remark. Direct CO compression (both for video and audio) results in its distortion and in impossibility of comprehension.
This requires to use more sophisticated methods of embedding by lossless compression that does not corrupt image just after embedding of authenticators .

WM embedding



Comments:

1. Partitioning $C(n)$ in groups: $\mathrm{G}_1, \mathrm{G}_2, ..., \mathrm{G}_{N/K}$

2. Formation of modified group $\mathrm{G}' = (C_1', C_2' ... C_K'),$ where $C_i' = F(C_i), \mathrm{G} = (C_1, ..., C_K)$

$F(C)$ -gives a flipping of levels:

Example. $0 \leftrightarrow 1, 2 \leftrightarrow 3, ..., 254 \leftrightarrow 255 (LSB); 0 \leftrightarrow 2, 1 \leftrightarrow 3, 4 \leftrightarrow 6, 5 \leftrightarrow 8, ...$ and so on.

$A = \frac{1}{L} \sum_{C \in I} |C - F(C)|$, where I -the set of quantization levels, A - amplitude of flipping. Property of $F(C): F(F(C)) = C$

3. Group classification:

$$\mathrm{G} \in R, \text{if } f(F(\mathrm{G})) > f(\mathrm{G}) \text{ (regular groups)}$$

$$\mathrm{G} \in S, \text{if } f(F(\mathrm{G})) < f(\mathrm{G}) \text{ (singular groups)}$$

$$\mathrm{G} \in U, \text{if } f(F(\mathrm{G})) = f(\mathrm{G}) \text{ (unused groups)}$$

$$\text{where } f(C) = f(C_1 ... C_K) = \sum_{i=1}^{K-1} |C_{i+1} - C_i| \text{ (discriminant function)} \qquad (8)$$

4. Formation of RS-vector: $R \to 1, S \to 0, U \to \varnothing.$

5. Lossless compression of RS-vector: $RS^{'} = \Phi(RS), |RS| = L_{RS}, |RS^{'}| = L_{RS^{'}}, L_{RS^{'}} < L_{RS},$
$\exists \Phi^{-1}(..): \Phi^{-1}(RS^{'}) = RS$

6.WM embedding: $RSM = (RS^{'}, C), |C| = L_{RS} - L_{RS^{'}}$, where $C = (M, E_S(M))$

7. Comparison of vectors RSM and RS:

$x_i \neq x_i^{'} \Rightarrow \pi_i = 1, x_i = x_i^{'} \Rightarrow \pi_i = 0,$ where

x_i *is* i - th symbol of the vector RS, $x_i^{'}$ *is* i - th symbol of the vector RSM.

8. Transform of groups:

$G_i^{'} = F(G_i), i = 1,2,..., N/k,$ if $\pi_i = 1, G_i^{'} = G_i,$ if $\pi_i = 0$ or $G_i = U$

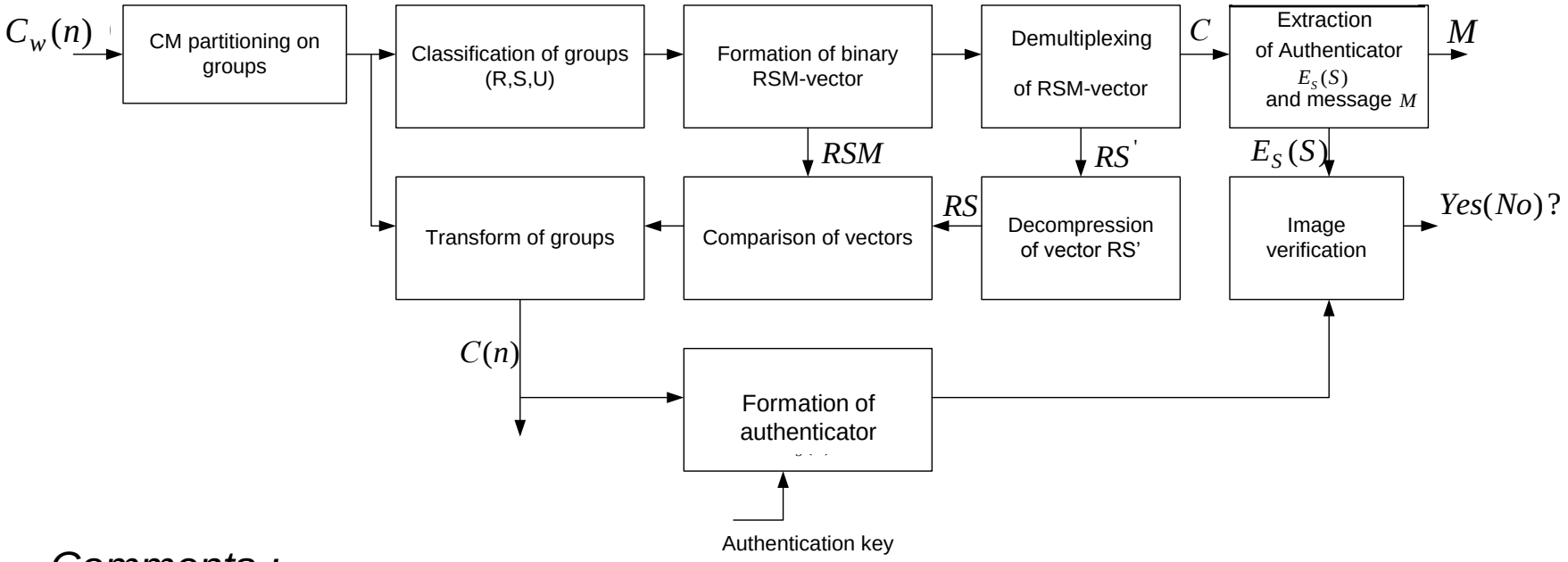
Property of flipping level function:

$F(R) = S,\ F(S) = R,\ F(U) = U$

Remark.

One can select any lossless compression algorithm but the most preferential seems to be the use *of adaptive arithmetic codes* [31].

Algorithm of WM extraction and CO authentication



Comments :

1. Decompression of RSM-vector

$RSM \Rightarrow (RS', C)$, where RS' – compressed image, C – message.

2. Extraction of authenticator and additional message

$C = (M, E_S(S))$, where M – message, $E_S(S)$ – authenticator.

3. Decompression of RS'-vector: $RS = \Phi^{-1}(RS')$

4. Comparison of vectors RSM and RS:

$x_i \neq x'_i \Rightarrow \pi_i = 1, x_i = x'_i \Rightarrow \pi_i = 0,$ где x_i is i - th symbol of the vector RS,

x'_i *is* i - th symbol of the vector RSM

5. Transform of groups:

$G_i' = F(G_i), if \ \pi_i = 1, \ G_i = G_i', if \ \pi_i = 0$ or $G_i = U$

6. Verification (see Sl. 1)

Conclusions:

1.The method considered above allows to perform exact authentication of the images if

$$L_{RS} - L_{RS'} \geq |E_S(S)|$$

2. The number of additional embeddable bits are $L_{RS} - L_{RS'} - |E_S(S)|$

3. Efficiency of the method(the embedding rate) $R_{WM} = \frac{L_{RS} - L_{RS'}}{N}$ depends on «compressability» R,S-groups, e.g. the more differ the probabilities of their occurrence P(R), P(S)=1-P(R), the more additional information can be embedded. Embedding capacity is determined by entropy function– $(P(R)\log_2 P(R) + P(S)\log_2 P(S))$, that depends in turn on particular image.

Typically P(R)>P(S), because application of transform F(G) is equivalentey to addition of small noise to the image that results in increasing of discriminant function f(G) (see (8))

Example.

$$G = (0,1,2,3) \Rightarrow f(G) = 3, G' = F(G) = (1,0,3,2), if\ \mathrm{F}(...) = LSB. \text{ Then } \mathrm{f}(\mathrm{G}') = 5 \text{ and } \mathrm{f}(\mathrm{G}') > \mathrm{f}(\mathrm{G}).$$

$$\text{Typically}: \mathrm{P_r}_{(0,1,2,3)} > \mathrm{P_r}_{(1,0,2,3)}$$

4. The more is «magnitude» A, the more is the embedding rate R_{WM}, but the more is image distortion just after embedding :

$$\eta_w = \frac{\sigma_C^2}{A^2}, where\ \sigma_C^2 = Var\{\mathrm{C(n)}\}$$

Remember that after WM extraction the image is recovered exactly however the quality of the image is also important before WM extraction .

Simulation results [32]

Image NxM pixels	The number of embeddable bits with magnitude A=1,2…6, L=256					
	1	2	3	4	5	6
Lenna (128x128) Face	170	512	1045	1390	1865	1996
Palms (400x268)	916	2274	4020	4621	5778	6643
Monkey (512x512)	186	702	1810	2905	4398	5664
Girl (1024x1024)	25506	65577	109805	131994	166806	176587
$\eta_w(dB)$	53	47	43	39	38	36
Average R_{WM} (%)	1,9	4	7	8	9	10

Conclusion: It is possible to embed authenticators in all test images and provide good quality just after embedding . It is possible to embed authenticator + additional information and provide satisfactory quality of the image just after embedding.

a) Original image

b) Image after embedding of 1212 bits (magnitude A=1)

в) Image after embedding of 3324 bits (magnitude A=4)

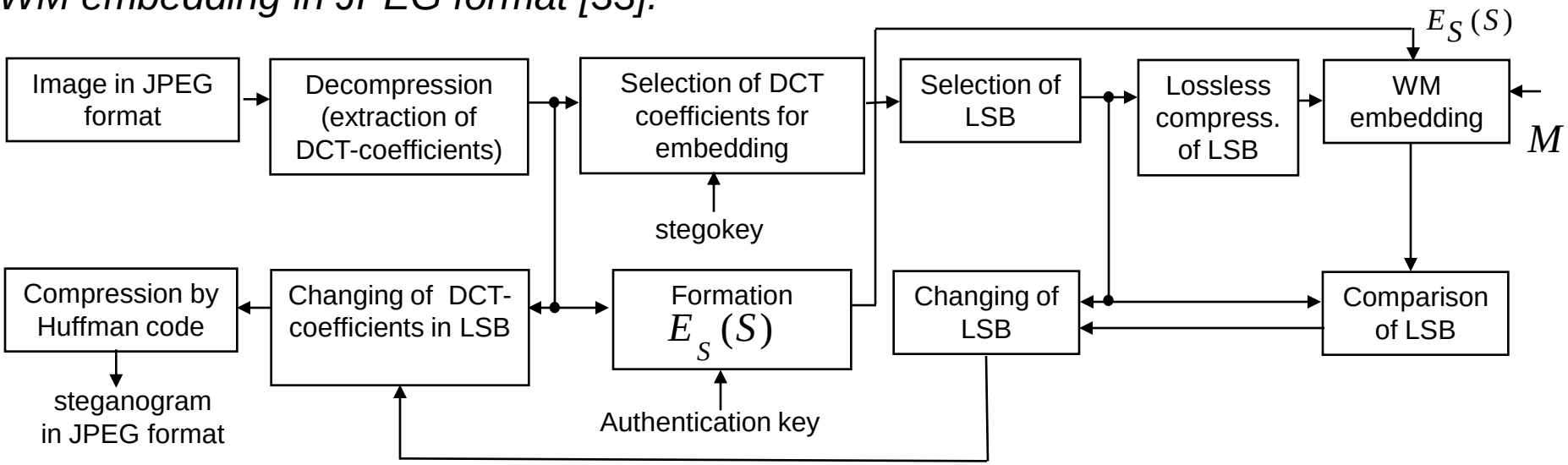
WM-based authentication of images in JPEG format.

Fact. It is impossible to provide exact authentication of the images under embedding in *bmp* format if after that the image be saved in *JPEG* format. Therefore it is necessary to embed and extract WM directly in *JPEG* format (before the image be transformed back to *bmp format*).

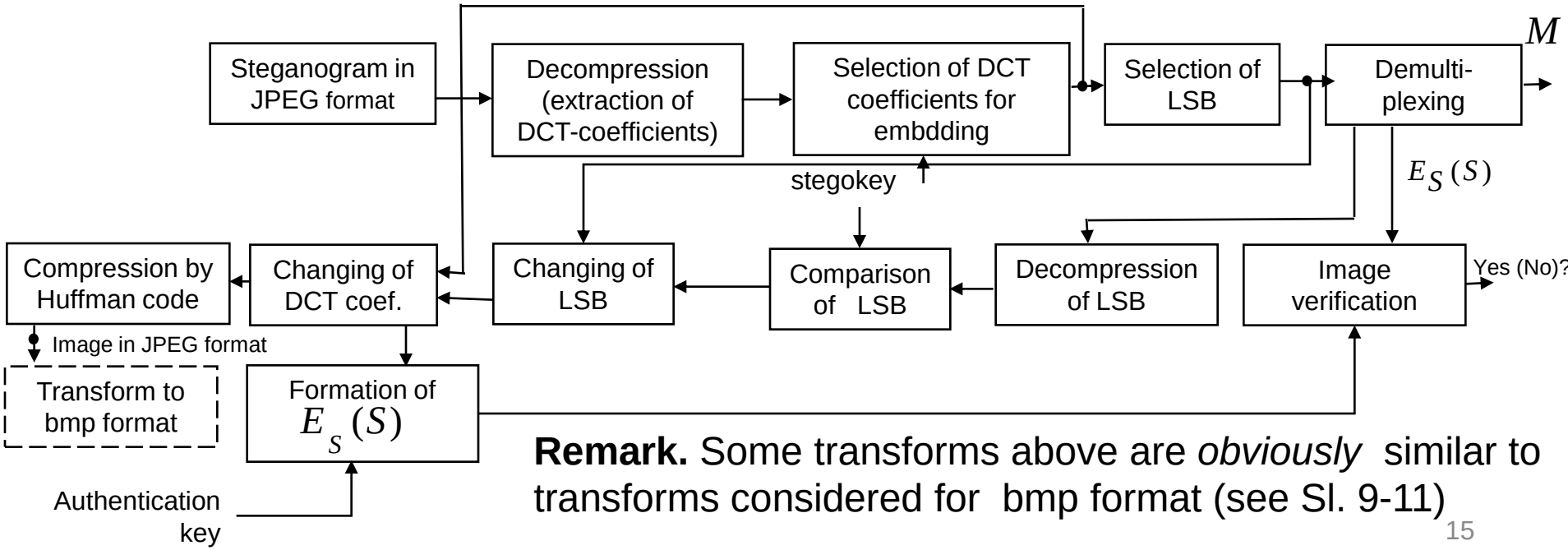
Reversible embedding with the use of lossless compression.

Remark. Since the image is subjected by compression already in JPEG format there exists a opportunity in increasing of the size JPEG file after embedding based on additional compression.

WM embedding in JPEG format [33].

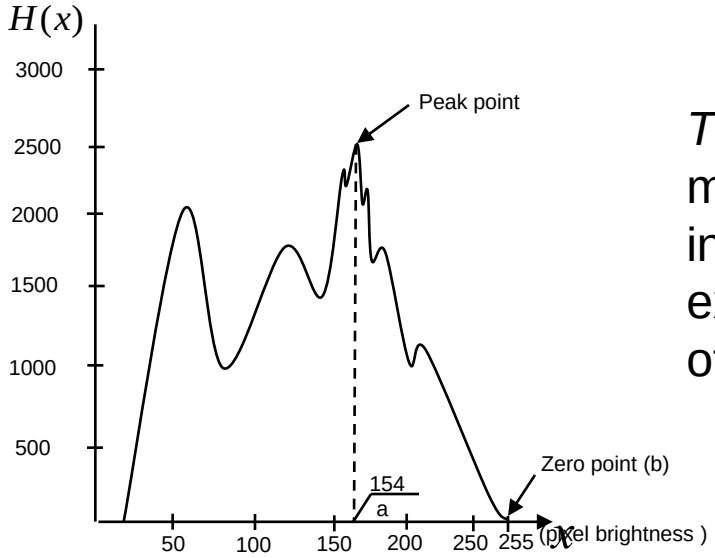


WM extraction in JPEG format.



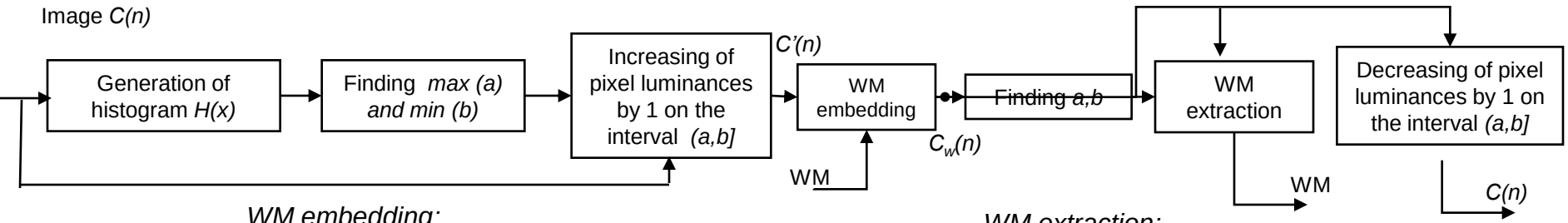
Remark. Some transforms above are *obviously* similar to transforms considered for bmp format (see Sl. 9-11)

3.2. Reversible WM embedding with the use of natural redundancy of the image in bmp format [34].



Histogram of image(Lena)

The main idea: Shift a part of histogram (from maximum to minimum), to the right and to embed information in the liberated space. After WM extraction recover the original image shifting a part of histogram to the left.



WM embedding:

N is the number of the pixel with the luminance «a»	1	2	3	4…
N of WM-ed pixels	1	2	3	4…
Bits of WM	0	1	1	0…
Вложение	a'=a	a'=a+1	a'=a+1	a'=a…

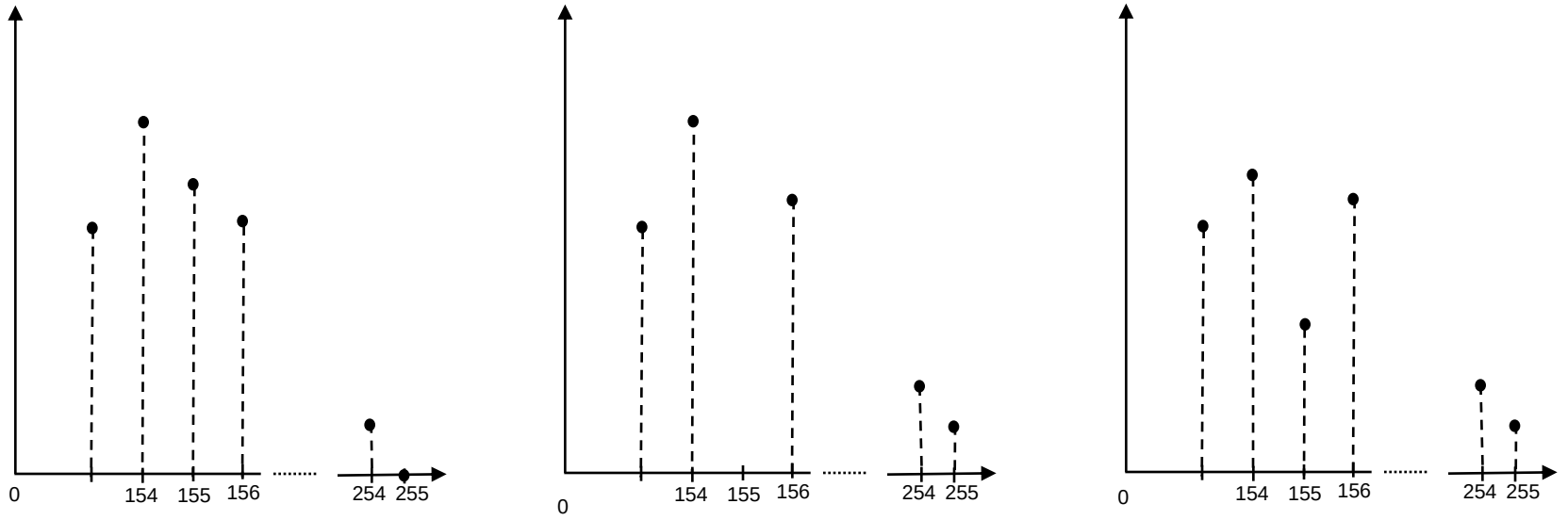
a) Algorithm of WM embedding

WM extraction:

N of pixels with the luminance a , a+1	1	2	3	4…
Pixel luminances	a	a+1	a+1	a…
Extracted WM	0	1	1	0…

b) Algorithm of WM extraction

Histogram transform after embedding (for particular case a=154, b=255)



a) *H(x)* Original image

b) *H(x)* after shiftinfat 1 right

c) *H(x)* just after embedding

The main properties of the method:

1. There are no errors after extraction and the image is recovered exactly.
2. The volume of embedding information bits is equal to the number of pixels with maximum luminance.
3. Embedding and extraction algorithms are very simple.
4. Just after embedding only some of pixels increase their luminance at 1 and therefore signal-to –noise ratio has the following bound:

$$\eta_w = \frac{\sigma_c^2}{1} = \sigma_c^2, \text{where } Var\{C(n)\}.(If\ \sigma_c^2 = 256,^2 \text{ then } \eta_w \approx 48.2dB)$$

Remarks:

1. It is known [34] a generalization of the considered method to the case of zero absence in histogram but if histogram has a minimum in some point «b». Then in order to recover the image correctly it is necessary to embed additional information about positions of pixels having the luminance «b».

2. It is known [34] a generalization of the considered method to the case when several minimum and maximum pairs of histogram (a_i,b_i) are used. This approach increases the volume of embedding information but makes the embedding algorithm more complex. The volume of embedded information for typical images lies in interval 5-80kb, whereas the time of embedding in the image of size 512x512x8 pixels on PC "Intel Celeron 1.4GHz" is of about 100ms.

3. The embedding by the all considered above algorithms is impossible for images having "flat" histogram.

4. This method cannot be extended directly to JPEG format however there exist other methods of reversible WM embedding for JPEG format.

4. Selective authentication.

Definition. Authentication is called *selective* if CO is assumed to be valid for some *acceptable distortion* and invalid for *not allowed CO distortions*. The choice of allowed and not allowed distortions depends on application of authentication and the conditions in which it works.

Typical legitimate distortions:

- Addition of small noise,
- Filtering,
- Transform to JPEG format
- Transform from JPEG to bmp and vice versa, or from wav to mpeg and vice versa,
- Printing and next scanning
- Changing of contrast and resizing
- Transmission of audio signal through aqustic transformers (for example - loud speaker and microphone-see Sl.11 in Lecture 11)
- and so on.

Typical non-legitimate distortions :

- All distortions mentioned above if they result in significant CO distortions
- Deliberate distortions of both video and audio signals which change significantly the content of them (contours of images ,individual signs of the voice ctr.).

Selective image authentication resistant to JPEG compression

Authentication is process of proving that image is legal

Fragile image authentication can detect all
possible modifications of the pixel luminance values

Semi-fragile image authentication can distinguish a
content-preserving operations from malicious manipulations

There are two possible types of the image tampering

Non-malicious

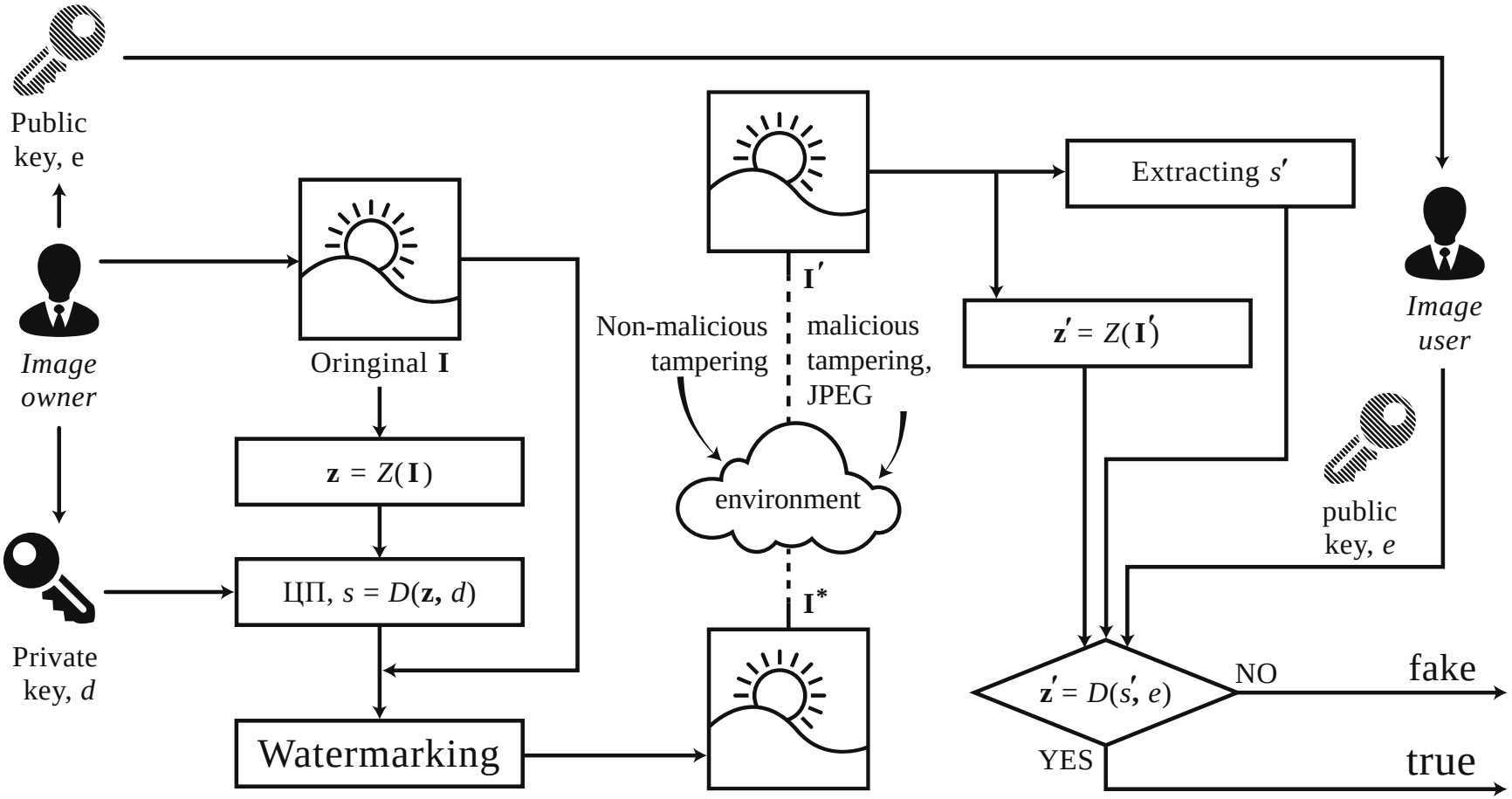
- a noisy channels
- JPEG compression/decompression
- filtering
- print / scan
- image resizing

Malicious

i.e. any possible change of the image content, for example: scene, textures, or objects

The aim of selective image authentication is that only malicious tampering would be detected whereas non-malicious tampering won’t.

Method based on image Zernike moments (ZM) magnitudes



Complex Zernike moments [72]

$$V_{pq}(x, y) = V_{pq}(\rho, \theta) = R_{pq}(\rho) e^{jm\theta}$$

where p is a non-negative integer and q is an integer such that $p-|q|$ is non-negative and even;
ρ and θ are polar coordinates within the unit circle and R_{pq} are polynomials of ρ (Zernike polynomials) given by relations:

$$R_{pq}(\rho) = \sum_{s=0}^{p-|q|} \frac{(-1)^s (p-s)! \rho^{p-2s}}{s! \left(\left(p + \frac{1}{2}|q|\right) - s\right)! \left(\left(p - \frac{1}{2}|q|\right) - s\right)!}$$

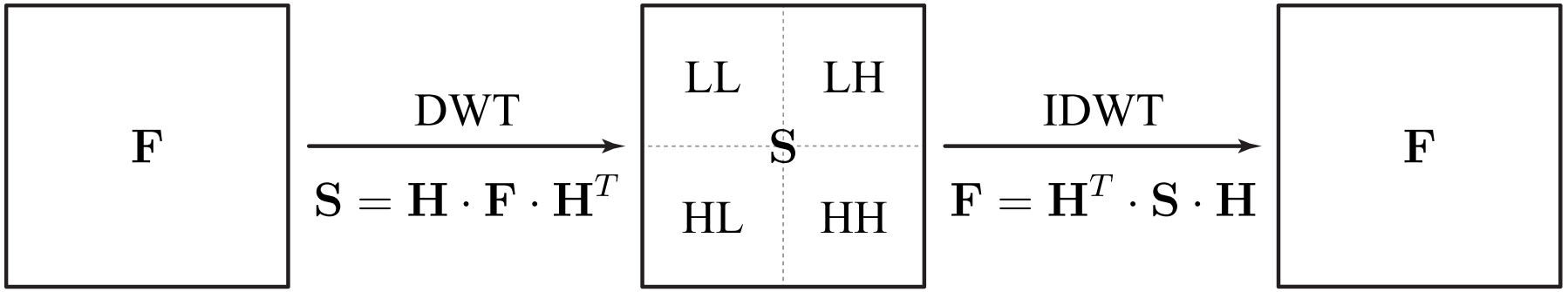
$$A_{pq}(\rho) = \frac{p+1}{\pi} \int_0^{2\pi} \int_0^1 f(\rho, \theta) V_{pq}^*(\rho, \theta) \mathbf{d}\rho \, \mathbf{d}\theta$$

Multi-level 2D Haar discrete wavelet transform [73], [74]

The Haar matrix of one-level DWT of order *n* represented by **H**(*n*) is given by

$$H(n) = \frac{1}{\sqrt{2}} \begin{pmatrix} I\left(\frac{n}{2}\right) & \otimes & (1 & 1) \\ I\left(\frac{n}{2}\right) & \otimes & (1 & -1) \end{pmatrix}, \quad n > 1, \qquad H(1) = \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix},$$

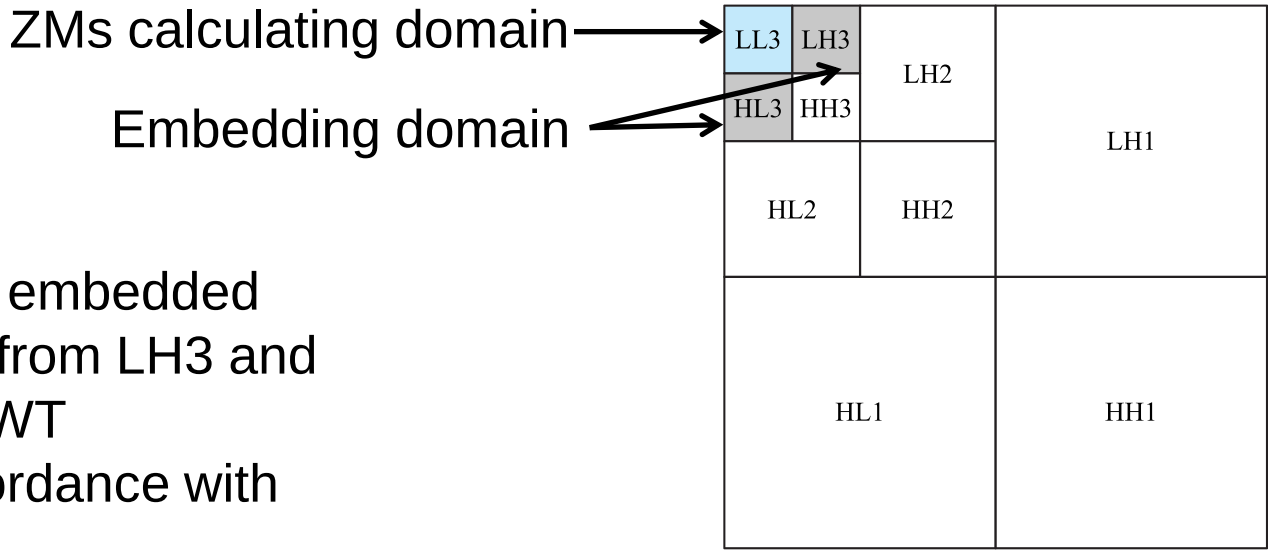
where **I**(*s*) is the identity matrix of order *s* and $\otimes$ stands for the Kronecker matrix product.



(image) (DWT coefficients) (image)

To calculate *k*-level 2D Haar discrete wavelet transform one-level transform over LL domain is need to be repeated *k* times.

ZMs are calculated over LL3 domain and then digital signature is computed by means of any method say RSA.

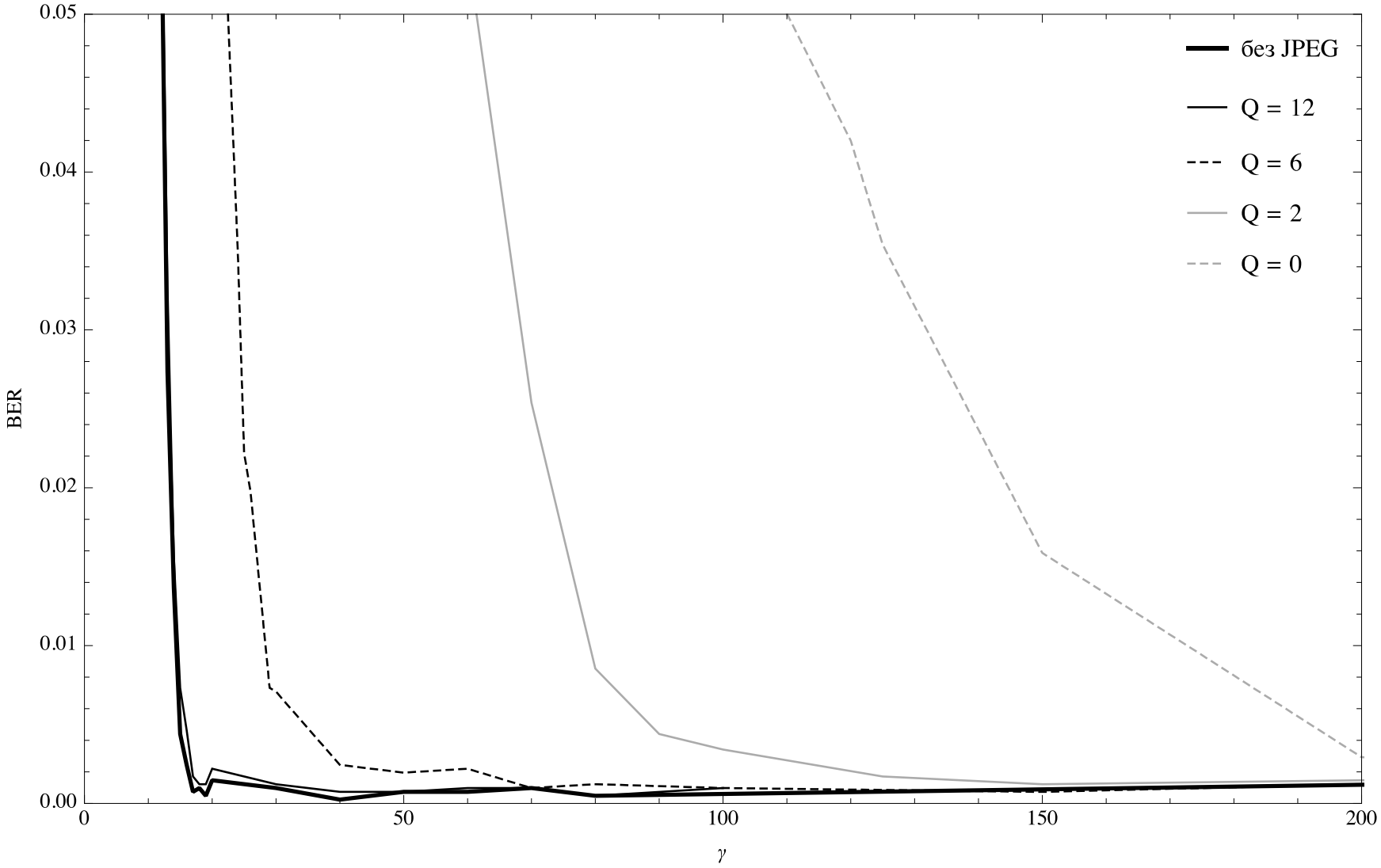


Digital signature is embedded into and extracted from LH3 and HL3 domains of DWT coefficients in accordance with

$$S'_k = \begin{cases} \gamma\left[\gamma^{-1}S_k\right] + 1/4, & b_k = 1, \\ \gamma\left[\gamma^{-1}S_k\right] - 1/4 & b_k = 0, \end{cases} \qquad b_k = \begin{cases} 1, & S'_k - \gamma\left[\gamma^{-1}S'_k\right] \geq 0, \\ 0, & S'_k - \gamma\left[\gamma^{-1}S'_k\right] < 0, \end{cases}$$

S_k and S_k' are the DWT coefficients before and after embedding of bit b_k, respectively; γ is the embedding depth and $[x]$ means the largest integer not greater than x.

Dependence of BER for the method resistant to JPEG compression with different JPEG *Q*-parameter against embedding depth γ



Original
«car.bmp»

After embedding WM
PSNR is 36 dB

After 70%-JPEG

Authentication succeeded

Fake car plate number

Authentication failed