Computer Science and Information Systems 11(4):1581–1594 DOI: 10.2298/CSIS131218072K

Concatenated Digital Watermarking System Robust to Different Removal Attacks

Valery Korzhik[1], Guilermo Morales-Luna[2], Alexander Kochkarev[1], and Dmitriy Flaxman[1]

[1] State University of Telecommunications
Saint-Petersburg, Russia
val-korzhik@yandex.ru, kochkareff@mail.ru, flxdima4951@gmail.com
[2] Computer Science
CINVESTAV-IPN, Mexico City, Mexico
gmorales@cs.cinvestav.mx

Abstract. A new concatenated digital watermarking system that combines in a serial manner both "holographic" transform domain and image-normalized method has been proposed and developed. Since the first procedure is resistant to watermarks removal attacks as cropping of windows, removal of rows and columns and JPEG compression, and the second procedure is especially robust against geometric transforms, we get a watermarking system embracing a resistance to the above mentioned attacks. The image corrupting after concatenated watermark usage and error correcting codes applying in order to improve a reliability of fingerprinting application of watermark have been also investigated.

Keywords: Error correction codes, image processing, tracing traitors, watermarking.

1. Introduction

Digital watermarking (WM) is widely used for copyright protection of still images and, in particular, it is used as fingerprinting. In such situation the owner of some image sales it legally to a set of users but without authorizing to distribute this product outside of the buyer set. Unfortunately it may not be the case if some members of the buyer set (becoming thus "pirates") illegally redistribute the product. The owner of the image would want to recognize the illegal distributors. That can be done if the owner embeds an unique bit string in every copy of the image known as *digital fingerprinting*. However, the pirates may try to remove the fingerprints (FP) by performing different (sometimes very sophisticated) transforms over the watermarked product. The seller should be sure that it is impossible to extract the FP without damaging the product. There are a lot of WM which are declared to be resistant to different attacks [2, 5, 6, 11]. A good robustness to practically all possible transforms has been proposed in [1] but unfortunately it works only for 0-bit watermarks. In [10], an approach for watermarking embedding that is invariant to such attacks as rotation, scale and translation has been proposed but the use of log-polar transforms results (confirmed by our experiments) to significant distortion of the cover images after WM embedding. Only a very restricted number of possible attacks are considered in [12]. Hence, the design of WM resistant to a "bunch" of attacks is

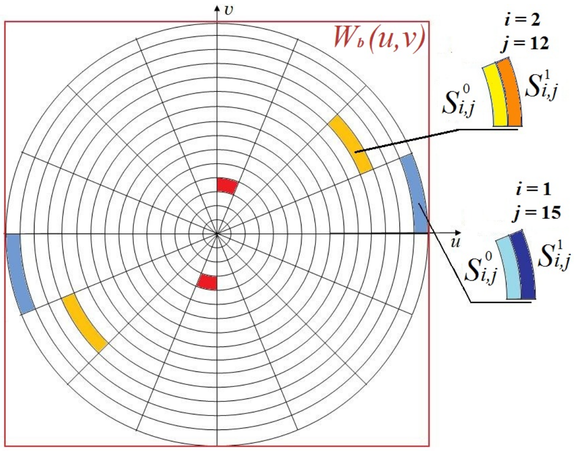


Fig. 1. Equally radius geometry embedding mask.

still urgent. Therefore we consider in the next section some approaches to solve this open problem.

2. Watermarking based on holographic transform domain

We investigated the *Holographic Transform Domain–Based* WM in [8], proposed early by A Bruckstein and T. Richardson [4]. The embedding procedure is performed as:

$$I^W = \mathcal{F}^{-1}\left(W_b \cdot \mathcal{F}\left(I\right)\right)$$

where $I = (I(x,y))_{(x,y)}$ is a grey-level (8 bit) image in an (x,y)-pixel area, $W_b = (W_b(u,v))_{(u,v)}$ is an embedding mask,

$$W_b(u,v) = 1 + (-1)^b \varepsilon \text{ whenever } (u,v) \in S^b_{ij},$$

with $\left(S^0_{ij}\right)_{ij}$, $\left(S^1_{ij}\right)_{ij}$ being some collections of selected areas, corresponding to the chosen embedding mask in the frequency area for the (i,j)-th message bit 0 or 1, respectively, ε is a depth of embedding, $\mathcal{F}$, $\mathcal{F}^{-1}$ are, respectively, the direct and the inverse Fourier transforms with `fft-shift` operation, and $I^W = \left(I^W(x,y)\right)_{(x,y)}$ is the resulting watermarked image. The `fft-shift` operation is a procedure that moves the zero-frequency component to the center of the array.

In [4] it is used the so called "equally radius" geometry shown on Fig. 1. For such mask it is possible to embed 120 message bits in the whole image of the standard size 512×512 pixels. The extraction of each of the (i,j)-bits is performed by the following rule optimal in additive Gaussian noise attack channel:

$$b_{ij} = \frac{1}{2}\left[1 - \text{Sign}\left(B^1_{ij} - B^0_{ij}\right)\right] \tag{1}$$

Table 1. The results of error probability P (in percents) in the extraction procedure after several different attacks.

Name of attack	P (%)
Cropping of window 200 × 200 pixels	4
Cropping of window 170 × 170 pixels	8
Saving in JPEG format with $Q = 60\%$	3
Saving in JPEG format with $Q = 50\%$	6
Saving in JPEG format with $Q = 20\%$	25
Saving in JPEG format with $Q = 10\%$	30
Addition of Gaussian noise with a variance $d = 25$	15

where

$$B_{ij}^{b} = \sum_{(i,j)\in S_{ij}^{b}} \Re\left(\overline{q_{ij}}\, s_{ij}\right) \quad , \quad b \in \{0,1\},$$

$\left(s_{ij}\right)_{(i,j)} = \mathcal{F}(I)$ is the array of complex values obtained as the Fourier transform of the original image I, $\left(q_{ij}\right)_{(i,j)} = \mathcal{F}(I^{W})$ is the array of complex values obtained as the Fourier transform of the watermarked image I^{W}, and $\Re$ is the "real part" operator and the overline denotes complex conjugation.

Since the knowledge of original image $\left(I(x,y)\right)_{(x,y)}$ is necessary for the extraction procedure, this method is called an *informed decoder*.

We tested this WM method in our paper [8] and it has been shown that the quality of WM-ed image is determined by the depth of embedding ε. So, the fidelity of the WM-ed image is still acceptable for $\varepsilon = 0.05$ but indeed unacceptable if $\varepsilon > 0.2$. The results of message extraction for different attacks are presented in Table 1.

This testing shows that although a cropping of small "windows" gives excellent results as well as JPEG compression with quality factor $Q \geq 60\%$, further decreasing of the window's sizes and a quality of the JPEG compression results in a degradation of the WM system as well as an addition of a Gaussian noise with variance larger 25. Thus the claim [4] that such WM system satisfies the required conditions for being resistant against any attacks is only partly correct. We maintain a good idea proposed at [4] regarding the holographic transform domain and portioning of decision bit area into two subareas $(\left(S_{ij}^{0}\right)_{ij}, \left(S_{ij}^{1}\right))$ in line with the decoding rule (1). But we suggest to modify WM system in order to improve it.

Firstly, we investigated the probabilities of errors after extraction of bits on different places into the frequency mask and after different attacks. The results of such investigation are shown in Tables 2-5.

By observing these tables, we can conclude that there are some bit locations where the probabilities of errors are unacceptable even if we would use some error correction codes, while there are some other bit locations where the probabilities of errors approach to zero. Then the following natural idea arises – let us embed message bits only in such "cells" of the mask where there appears a moderate number of errors.

The amount of bits which have the acceptable error probability is about 64 and they are displayed at columns 2-9 at Tables 2-5. This value is not sufficient in order to embed large amount of information but it may be enough at a scenario of fingerprinting. In such

Table 2. The probability (in percents) of the (i, j)-th bit error after a JPEG transform with quality factor $Q = 10\%$.

$i\backslash j$	1	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	10	11	12	13	14	15
1	3	1	4	3	7	21	39	34	32	42	48	38	52	46	47
2	3	2	5	16	19	31	44	35	49	47	49	41	56	44	38
3	2	0	4	12	19	36	29	45	42	42	45	56	50	46	44
4	3	0	1	8	6	15	25	40	43	50	55	48	38	47	46
5	2	2	2	5	10	15	32	35	41	48	51	43	48	48	39
6	2	3	4	7	21	28	43	53	44	45	50	44	57	51	45
7	0	1	4	15	27	36	46	36	45	42	53	44	50	45	53
8	0	1	1	5	8	28	35	40	41	40	38	47	44	51	50

Table 3. The probability (in percents) of the (i, j)-th bit error after a JPEG transform with quality factor $Q = 20\%$.

$i\backslash j$	1	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	10	11	12	13	14	15
1	0	1	1	2	2	8	7	24	30	41	42	38	43	46	35
2	2	0	2	2	10	16	34	32	55	44	44	54	52	44	38
3	2	2	2	1	6	15	33	40	36	41	38	51	49	42	48
4	2	0	1	3	3	7	7	13	38	40	38	49	57	51	41
5	0	0	1	0	2	5	13	14	42	51	47	52	51	44	38
6	0	1	1	2	3	9	33	45	43	42	44	57	52	47	45
7	0	1	2	2	2	17	27	41	38	50	40	42	48	47	49
8	1	1	2	0	2	7	10	30	42	33	45	51	35	45	42

Table 4. The probability (in percents) of the (i, j)-th bit error after cropping of window with size 200×200 pixels.

$i\backslash j$	1	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	10	11	12	13	14	15
1	43	9	2	0	1	0	0	1	0	0	0	0	1	1	3
2	38	1	2	0	0	0	0	0	0	0	0	0	0	1	0
3	43	13	0	1	1	0	1	0	1	0	0	0	1	0	0
4	32	3	1	1	0	1	2	3	2	2	5	5	6	3	5
5	46	2	1	1	1	1	1	1	1	1	2	2	3	2	3
6	25	3	1	1	1	0	1	0	0	2	0	2	2	1	0
7	23	2	1	1	1	0	1	0	0	0	0	1	0	0	0
8	45	3	1	1	0	0	1	0	0	0	1	0	0	0	2

a scenario, the owner of the product (say some still image) wants to recognize who was the illegal distributor (the "pirate" in other words). In order to solve this problem, the owner can embed the unique bit string in every copy sold to legal users, he extracts the embedded WM (which is called usually the fingerprint) from illegally redistributed copy and traces the pirate.

Since errors may occur even among the specially selected 64 bits, it is reasonable to use error-correction codes. We proposed in [8] to use BCH codes [9] of length 63 with a hard decoding on minimum Hamming distance. The results of simulation (in terms of

Table 5. The probability (in percents) of the (i, j)-th bit error after an addition of Gaussian noise with variance $d = 25$.

$i\backslash j$	1	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	10	11	12	13	14	15
1	1	1	1	3	4	6	10	11	10	20	19	20	21	25	24
2	0	1	3	12	11	14	18	15	15	17	21	20	40	31	29
3	5	4	3	9	9	11	11	14	13	22	22	28	33	25	30
4	0	3	1	4	3	10	6	13	13	16	13	22	16	29	29
5	1	2	2	1	5	11	14	10	15	14	26	21	22	28	39
6	1	4	3	7	13	8	20	14	16	24	23	23	23	28	25
7	1	0	4	7	8	11	20	20	22	22	20	24	26	35	33
8	1	0	5	3	4	10	9	7	13	21	18	23	29	23	28

Table 6. The probabilities of incorrect decoding by minimum Hamming distance for different BCH codes, different attack transforms and different embedding depths ε.

BCH codes	(63, 7)	(63, 10)	(63, 16)	(63, 7)	(63, 10)	(63, 16)
$(1)\backslash(2)$	0.05			0.1		
Saving in JPEG format with Q=20%	9.0×10^{-2}	1.6×10^{-1}	2.5×10^{-1}	2.3×10^{-2}	4.7×10^{-2}	7.9×10^{-2}
Saving in JPEG format with Q=30%	2.8×10^{-2}	5.7×10^{-2}	9.7×10^{-2}	5.7×10^{-3}	1.4×10^{-2}	2.5×10^{-2}
Saving in JPEG format with Q=60%	3.4×10^{-3}	6.6×10^{-3}	1.4×10^{-2}	1.2×10^{-3}	1.7×10^{-3}	3.8×10^{-3}
Cropping of window 200 × 200 pixels	1.8×10^{-2}	2.7×10^{-2}	3.6×10^{-2}	1.5×10^{-2}	2.0×10^{-2}	2.8×10^{-2}
Cropping of window 250 × 250 pixels	5.5×10^{-3}	8.3×10^{-3}	1.0×10^{-2}	4.1×10^{-3}	5.5×10^{-3}	7.9×10^{-3}
20 rows and 20 columns removal	2.7×10^{-2}	5.4×10^{-2}	1.1×10^{-1}	5.0×10^{-3}	1.2×10^{-2}	2.5×10^{-2}
Addition of Gaussian noise with $d = 25$	8.4×10^{-2}	1.4×10^{-1}	2.1×10^{-1}	1.3×10^{-2}	2.3×10^{-2}	3.9×10^{-2}

(1) Attack transform. (2) Embedding depth (ε).

incorrect block decoding probabilities) after testing 1000 grey scaled images taken from the image repository [3] for different attacks, different number of information bits of BCH code and two embedding depths are presented at Table 6.

From this table, it can be seen that the maximum number of information bits k, that can still provide the acceptable probability of incorrect decoding after all attack transforms is 10. But unfortunately the watermarking technique based on the use of holographic transform domain is not resistant to geometric attacks (including a rotation on small angles). In order to prevent this type of attacks it is known another technique, namely the *image* *normalization-based method.* We will consider this method in Section 3. In Section 4 we propose and investigate concatenated method of digital watermarking that combines both "holographic" and "normalization" techniques in order to be resistant to a bunch of attacks.

3. Watermarking based on image normalization

This approach to WM designing has been proposed by Dong *et al.* [7]. The idea was to get the so called *normalized image* from the original one by a geometric transformation procedure that would be invariant to any affine distortion of the original image. Let us specify some notations.

An image $\left(\tilde{I}(x,y)\right)_{(x,y)}$ is an *affine transform* of the original image $(I(x,y))_{(x,y)}$ of size $M \times N$ if there is a matrix $A = \begin{pmatrix} \alpha\ \beta \\ \gamma\ \delta \end{pmatrix}$ and a vector $d = \begin{pmatrix} d_1 \\ d_2 \end{pmatrix}$ such that

$$\forall x, y:\ \tilde{I}(x,y) = I\left(A\begin{pmatrix} x \\ y \end{pmatrix} - d\right).$$

The following determine particular cases of affine transforms, by special selection of the matrix A:

- *Shearing in direction x*: $A_x = \begin{pmatrix} 1\ \beta \\ 0\ 1 \end{pmatrix}$
- *Shearing in direction y*: $A_y = \begin{pmatrix} 1\ 0 \\ \gamma\ 1 \end{pmatrix}$
- *Scaling in both x and y*: $A_s = \begin{pmatrix} \alpha\ 0 \\ 0\ \delta \end{pmatrix}$
- *Rotation by an angle ϕ*: $A_r = \begin{pmatrix} \cos\phi & \sin\phi \\ -\sin\phi & \cos\phi \end{pmatrix}$

It is straightforward to show that any affine transform A can be factored as a composition of the above transforms, provided that $\alpha \neq 0$ and $\det(A) \neq 0$. The normalization transform is:

$$\begin{pmatrix} x \\ y \end{pmatrix} \mapsto \varPhi\begin{pmatrix} x \\ y \end{pmatrix} = A_s\, A_x\, A_y \begin{pmatrix} x \\ y \end{pmatrix} - \begin{pmatrix} d_1 \\ d_2 \end{pmatrix}$$

where

$$\forall p, q \in \{0,1\}:\ m_{pq} = \sum_{x=0}^{M-1}\sum_{y=0}^{N-1} x^p y^q\, I(x,y),$$

$$d_1 = \frac{m_{10}}{m_{00}}\ ,\ \ d_2 = \frac{m_{01}}{m_{00}}\ ,$$

β is a solution of the cubic equation

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

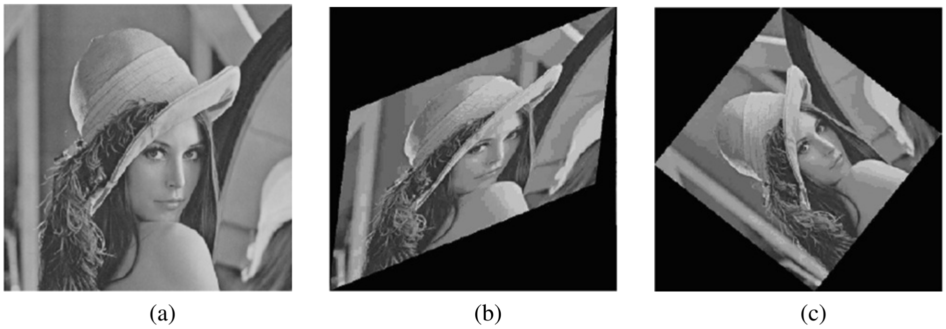


Fig. 2. (a) Original image `Lena`. (b) `Lena` after distortion. (c) Normalized image for both (a) and (b).

whose coefficients are given by the relation

$$\forall p, q \in \{0, 3\} : \ \mu_{pq} = \sum_{x=0}^{M-1} \sum_{y=0}^{N-1} (x - d_1)^p (y - d_2)^q \, I(x, y), \tag{2}$$

the parameter γ in the matrix A_y is determined by the relation

$$\gamma = \frac{\mu'_{11}}{\mu'_{20}}$$

where μ'_{11}, μ'_{20} are calculated according to (2) for $(x', y') = A_x(x, y)$, and the parameters α, β at matrix A_s are given by the relations

$$\alpha = \frac{M'}{M''} \ , \ \beta = \frac{N'}{N''} \ ,$$

where M', N' are, respectively, the width and the height of the normalized image, and M'', N'' are, respectively, the width and the height of the normalized image for $(x'', y'') = A_y(x', y')$.

In Figure 2 there are presented an original image `Lena` (a), the same image after an affine distortion (b), and the normalized image (c), for both the original image (a) and its affine distortion (b). This experiment confirms the fact proved in [7], namely an image and its affine transforms have the same normalized image. Two normalization-based watermarking methods have been proposed in [7]. The first one embeds the WM into the normalized image and it requires to restore the normalized image to the original size and position. Some distortion of the original image may result, and as a consequence, a decreasing of its value, which is unacceptable. The second method keeps the original image without normalization but it adds the WM after normalized spread spectrum-based WM. This scheme of watermark embedding process (taken from [7]) is shown at Figure 3.

We investigated the above method using *spread spectrum signals* (SSS) based on pseudo-random sequence of length 500 that allows to embed a WM of about 64 bits into a standard size (512 × 512 pixels) image, and with the two types of decoders shown in Figure 4.This parameters of embedding were chosen in order to embed 64 bits like in holographic method.

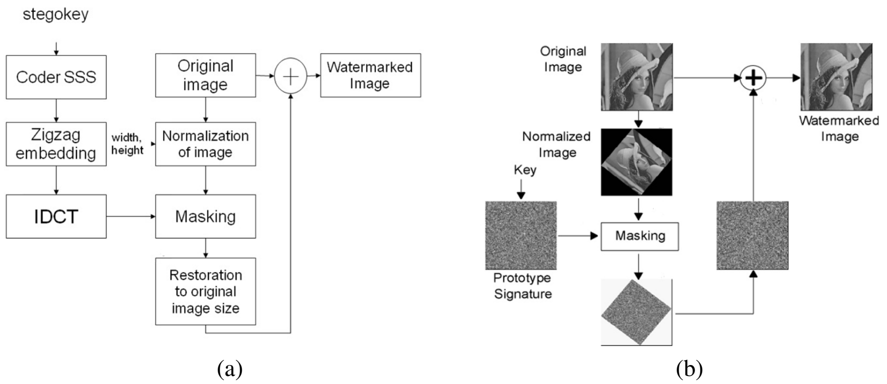


Fig. 3. Illustration of watermark normalized-based embedding process.

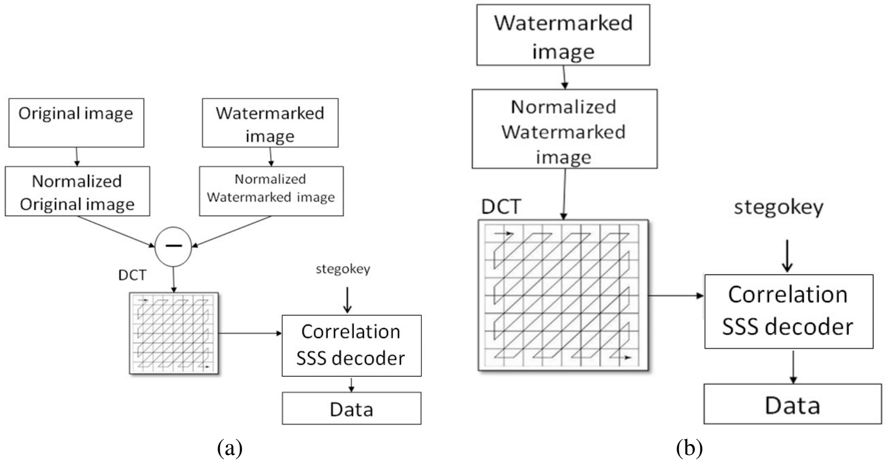
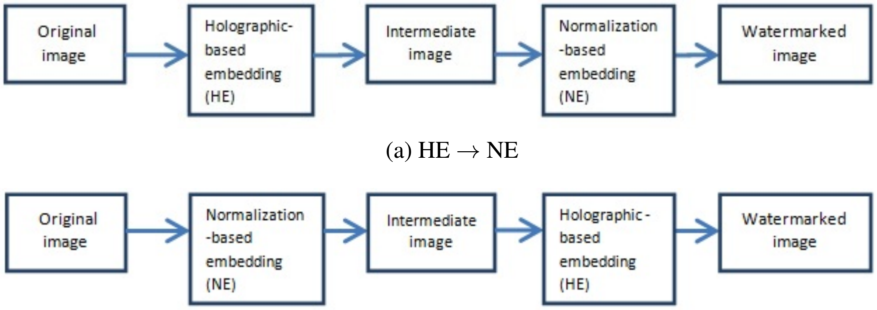


Fig. 4. Two types of normalization-based WM decoders: (a) informed, (b) blind decoder.

The results of our simulation based on testing 100 images (taken from the image repository [3]) showed that, for 48 different geometric attacks, the average percent of errors was 2.1. (In the case of removal of "anomalous" images, the average percent goes down to 0.5%).

We investigated also the normalization-based method against other types of attacks. It was observed a resistance to JPEG transform with quality factor $Q > 20\%$ (small errors) and an additive noise attack with variance 3 (no errors). But this method was very sensitive to row and column removal, as well as cropping attacks. If we remember (see Table 6) that the "holographic-based" method is resistant to these attacks then the following natural idea arises: let us combine both methods (holographic-based and normalization-based) into one WM method to extend the robustness of such a system. This approach is investigated in the following Section.


Original image
Holographic-based embedding (HE)
Intermediate image
Normalization-based embedding (NE)
Watermarked image
Original image
Normalization-based embedding (NE)
Intermediate image
Holographic-based embedding (HE)
Watermarked image

(a) HE → NE

(b) NE → HE

Fig. 5. Two versions of concatenated-based WM.

4. Concatenated method of watermarking

The idea to design a WM based on a concatenation of the two previously considered methods, called *concatenated-based WM*, aroused from the following observation: the normalized image can be considered as an original image with respect to holographic-based embedding view (and vice versa).

We have two main versions according to the following approaches:

$$\text{holographic-based embedding} \longrightarrow \text{normalized-based embeddings}$$

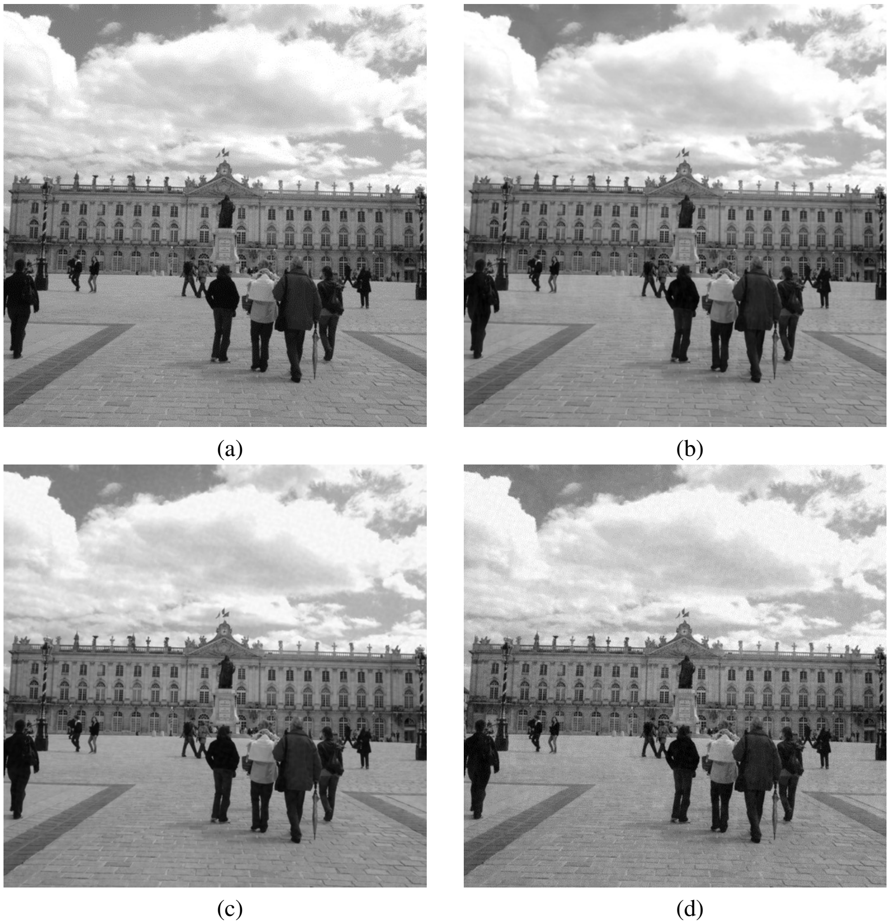
(see Figure 5 (a)), and the opposite embedding order (see Figure 5 (b)).

If the concatenated method is used, then the following problems should be considered:

- how distortions, owing the next embedding on the extraction of WM, do affect?
- how one can get the "original" image that is needed for the informed decoder (both for holographic and normalization methods)?
- what is the image quality degradation after double embeddings?
- how to select the WM extraction method between holographic and normalization decoders if the same WM bits have been embedded for both methods?
- which of two versions (HE → NE, NE → HE) is preferable with respect to all above problems?

In order to determine which of the two versions (HE → NE, NE → HE) is preferable we performed a set of experiments with 200 images.In order to detect differences between HE → NE and NE → HE schemes we embed 160 bits with normalization method with weak value of depth of embedding (α=2) and extracted with normalization method.Parameters of holographic method were kept as before and were constant. The results of this experiment showed that the average percent of errors was 9 for HE → NE scheme and 13 for NE → HE.This experiment was repeated with another values of depth and another number of embedded bits. The results were similar. This can be clarify by the fact that normalized-based embedding suffers less from holographic embedding in the scheme HE → NE. So we have taken a solution that HE → NE is superior to opposite one.

In Figure 6 there are presented the original image (a), the watermarked image after holographic-based embedding (b), the normalization-based embedding (c) and the



(a) (b)

(c) (d)

Fig. 6. The original image (a), holographic-based watermarked image (b), normalization-based watermarked image (c) and concatenated-based watermarked image (d).

concatenated-based (HE → NE) embedding(d). It can be seen that the image fidelity in the last case is very close to the fidelity of all previous cases. PSNR of figure 6(b) is 30 dB,PSNR of figure 6(c) is 35 dB,PSNR of figure 6(d) is 28 dB. We also use 15 experts and 10-point scale in order to estimate fidelity of images. Average expert mark of figure 6(b) is 7.3, average expert mark of figure 6(c) is 8.6, average expert mark of figure 6(d) is 6.9. Experts marks of holographic-based watermarked images are close to marks of concatenated-based watermarked images. This means that the concatenated method does not degrade the image noticeably.

The supporting signal for the informed normalization decoder can be obtained by different ways:

1. Using the original image (although it was distorted as the cost of holographic embedding in the scheme at Figure 5 (a)).

Table 7. The results of concatenated-based (HE → NE) WM simulation for different embedding depths and without attacks.

Depths of embedding		The probabilities of bit errors (%)	
ε: Depth of HE	α: Depth of NE	Holographic decoder	Normalization decoder
0.05	2	0	0.5
0.1	2	0	1.0
0.05	4	0	0.2
0.1	4	0	0.9

Table 8. The results of concatenated-based (HE → NE) WM simulation for different decoders and different attacks.

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
Cropping attack (of window 200 × 200 pixels)	3	49.0
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
Addition of Gaussian noise with d = 25	8.0	48.0
Median Filtering with mask of size 3 × 3	4.5	10.5

2. Using an approximation of the holographic-based watermarked signal given an original image and the WM bits extracted by holographic-based decoder (while the extracted bits can be corrupted by attacks for which the holographic method is fragile).
3. Using an approximation of the holographic based watermarked signal given an original image and the randomly generated WM bits.

Our experiments showed that the last two methods are significantly better that the first one. In Table 7, there are presented the results of concatenated based (HE → NE) WM simulation in terms of averages over 200 images the bit error probabilities after the extraction by holographic and normalization informed decoders without attacks. (This result was obtained for 64 bit sequences embedded both in NE and HE, where the supporting signal has been obtained by the 3-rd method.)

Since holographic-based WM is the most vulnerable to geometric attacks, whereas the normalization-based are vulnerable to cropping attacks, we tested these attacks especially. The results are presented in Table 9 for the best parameters $\varepsilon = 0.1$, $\alpha = 4$ chosen to provide simultaneously good image quality after embedding and acceptable bit error probabilities after extraction. As it is evident from Table 9, the embedded bit can successfully be extracted by the holographic decoder after a cropping attack (or rows-columns removal attack) while the extraction procedure is failed for normalization decoder, and the embedded bit can successfully be extracted by the normalization decoder after a geometric attack while the extraction procedure is failed for holographic decoder. In case of JPEG transform or Gaussian noise addition the embedded bit can successfully be extracted both by the normalization and holographic decoder.

Because the same 64 bits are embedded both by the holographic and the normalization decoder, we can compare the extracted bits, and if the difference is more that some threshold λ then we take a decision based on one decoder which is tolerant to this attack. We have proposed before, in [8], the use of the BCH code (63, 10) in order to correct errors after bit extraction. This code also can be used in order to detect a presence of many errors in code words. In fact it is sufficiently to find the Hamming distance between the received vector word and the nearest to it code word and compare the result with some threshold λ'. If this threshold is exceeded, then we assume that the corresponding decoder should be ignored, otherwise, it can be used.

On the other case, if the first threshold λ is not exceeded than we may assume that both decoders are able to extract the WM. Therefore it is possible to erase "unreliable" bits for which we have disagreement between two decoders. After such solution, a procedure of decoding based on minimum Hamming distance (with a removal of the erased bits) can be performed.

5. Conclusion

Traitor tracing is a very important problem in the case of an early release of a HD movie window for VOD, where it can effectively be used a fingerprinting system with a limited number of "fingers" (say corresponding to 10-20 bits). But it should be resistant to a "bunch" of attacks trying to remove the WM by keeping a good quality of the image.

In the current paper, we proposed a new watermarking algorithm that was called concatenated WM, because it inserts one WM algorithm (namely holographic-based) into another one (namely normalized-based) similar to the well known concatenated codes [9]. We demonstrate by numeral experiments that for appropriately chosen parameters the proposed algorithm can achieve low BER even for such set of attacks as cropping, row and column removal, additive noise, JPEG compression and geometry attacks. We propose also to use binary (63,10)-BCH codes to correct errors on maximum Hamming distance decoding algorithm jointly with erasing of unreliable bits at the output of two receivers. It has been proved also that the image quality is kept acceptable after implementation of the concatenated method.

Unfortunately the proposed method is ineffective against a simultaneously combining of attacks (say removal of rows or columns and geometric attack). But such complex attack results as a rule in significant image distortion. Concatenated WM can be extended in the future to other components and to more than two stages of concatenations.

References

1. Anfinogenov, S., Korzhik, V.I., Morales-Luna, G.: Robust digital watermarking system for still images. In: Ganzha, M., Maciaszek, L.A., Paprzycki, M. (eds.) FedCSIS. pp. 685–689 (2011)
2. Barni, M., Bartolini, F.: Watermarking systems engineering: enabling digital assets security and other applications. Signal processing and communications, Marcel Dekker (2004), http://books.google.co.uk/books?id=DUuyektSYH0C

3. Bas, P., Filler, T., Pevný, T.: "Break our steganographic system": the ins and outs of organizing BOSS. In: Proceedings of the 13th international conference on Information hiding. pp. 59–70. IH'11, Springer-Verlag, Berlin, Heidelberg (2011), http://dl.acm.org/citation.cfm?id=2042445.2042452
4. Bruckstein, A., Richardson, T.: A holographic transform domain image watermarking method. Circuits, Systems, and Signal Processing Journal Special Issue 17(3), 361–389 (1998)
5. Cox, I.J., Miller, M.L., Bloom, J.A.: Digital Watermarking. Morgan Kaufman Publishers (2002)
6. Dehghan, H., Safavi, S.E.: Robust image watermarking in the wavelet domain for copyright protection. arXiv preprint arXiv:1001.0282 (2010)
7. Dong, P., Brankov, J.G., Galatsanos, N.P., Yang, Y., Davoine, F.: Digital watermarking robust to geometric distortions. IEEE Transactions on Image Processing 14(12), 2140–2150 (2005)
8. Korzhik, V.I., Morales-Luna, G., Kochkarev, A., Shevchuk, I.: Fingerprinting system for still images based on the use of a holographic transform domain. In: Ganzha, M., Maciaszek, L.A., Paprzycki, M. (eds.) FedCSIS. pp. 589–594 (2013)
9. Macwilliams, F.J., Sloane, N.J.A.: The Theory of Error-Correcting Codes. North-Holland Mathematical Library, North Holland (January 1983), http://www.amazon.com/exec/obidos/redirect?tag=citeulike07-20&path=ASIN/0444851933
10. Ó Ruanaidh, J., Pun, T.: Rotation, scale and translation invariant digital image watermarking. In: IEEE Int. Conf. on Image Processing ICIP1997. pp. 536–539 (1997)
11. Tsougenis, E., Papakostas, G., Koulouriotis, D.: Introducing the separable moments for image watermarking in a tottaly moment-oriented framework. In: Digital Signal Processing (DSP), 2013 18th International Conference on. pp. 1–6. IEEE (2013)
12. Woo, C.S., Du, J., Pham, B.: Geometric invariant domain for image watermarking. In: Shi, Y.Q., Jeon, B. (eds.) IWDW. Lecture Notes in Computer Science, vol. 4283, pp. 294–307. Springer (2006)

Valery Korzhik has received the MSc degree in Electrical Engineering from the Military Communication Academy, Leningrad, Soviet Union, in 1959, the MSc degree in mathematics from the State Leningrad University, Soviet Union, in 1969, the PhD degree and the Doctor of Philosophy degree from the Military Communication Academy in 1965 and 1974 respectively. He has been professor at the Military Communication Academy, and at the State University of Telecommunications, both in St. Petersburg, Russia, as well as in CINVESTAV-IPN, Mexico. His main research interests are in coding theory, signal processing, cryptography and information hiding.

Guillermo Morales-Luna has received the BSc degree in mathematics from the Mexican National Polytechnic Institute in 1977, the MSc degree in mathematics from Mexican CINVESTAV-IPN, in 1978, and the PhD degree from the Mathematics Institute of the Polish Academy of Sciences in 1984. Since 1985 he is a researcher at CINVESTAV-IPN. His research interest include cryptography, complexity theory, and mathematical logic. He is a Mexican national and he also holds Polish citizenship.

Alexander Kochkarev is an Information Security engineer (magister) graduated in 2011, currently a PhD student at the Bonch-Bruevich Saint-Petersburg State University of Telecommunications (Department of Protected Communication Systems). At present, he works as engineer at Yandex LLC. His scientific interests include digital watermarking, fingerprinting, image processing, steganography, computer programming (MatLab, Java)

Dmitriy Flaksman is an Information Security engineer (magister) graduated in 2013, currently works as an assistant at the Department of Protected Communication Systems at the Bonch-Bruevich Saint-Petersburg State University of Telecommunications. At present continues his education as a Master student at the Faculty of Infocommunication Networks and Systems. His scientific interests include digital watermarking, steganography, computer programming (C++, OpenCV, Qt) and image processing.

Received: December 18, 2013; Accepted: August 18, 2014.