Proceedings of the 2013 Federated Conference on
Computer Science and Information Systems pp. 585–590

Fingerprinting System for Still Images Based on the Use of a Holographic Transform Domain

Valery Korzhik
(Member of IEEE)
State University
of Telecommunications
Saint-Petersburg, Russia
Email: val-korzhik@yandex.ru

Guilermo Morales-Luna
Computer Science
CINVESTAV-IPN
Mexico City, Mexico
Email: gmorales@cs.cinvestav.mx

Alexander Kochkarev and Ivan Shevchuk
State University of Telecommunications
Saint-Petersburg, Russia
Email: kochkareff@mail.ru, johan92@yandex.ru

***Abstract*—We consider the watermarking method based on a holographic transform domain image proposed by A. Bruckstein. Our testing showed that it is resistant not against all possible attacks declared by his inventor, under the condition of a very high image quality just after WM embedding. Only a small part among 120 bits embedding into the image has an acceptable error probability after extraction if some attacks hold. Therefore we propose to modify this system for fingerprinting where only fixed bits are embedded into the most reliable places of the frequency mask. Systematic linear binary codes with large minimal code distance are used in order to correct errors. Simulation showed that such system provides sufficiently reliable tracing "traitors" under the most types of attacks subjected to remove WM, while keeping a good quality of the image just after embedding.**

***Index Terms*—Watermarking, image processing, error correction codes, tracing traitors**

I. Introduction

DIGITAL watermarks effectively can be used for copyright protection of still images [1], [2], [3], [4]. However, intruders, the so-called "pirates", try to copy and spread these products illegally, and they attempt to remove the WM by performing different (sometimes very sophisticated) transforms over the watermarked products which, not impairing the product itself, should make impossible to extract them. In [3] there has been proposed an approach for watermarking insertion that is invariant to several transforms as rotation, scale and translation. But the use of the log-polar transforms results (confirmed at our experiments) to significant corruption of the cover images after WM embedding. Only a very restricted number of possible transforms are considered in [4]. A good robustness to practically all possible transforms has been obtained in [5] but unfortunately it works only for o-bit watermark. An extension of this method to multiple-bit watermark was presented in [6] but without the use of error correcting codes. Thus it can be concluded that although there were many proposals in the design of WM systems resistant to different attacks, this problem is so far not solved completely.

In [7], a WM system based on a "holographic" transform domain has been proposed, where the embedding procedure is performed in the area of the Fourier amplitude and then the message can be extracted even from cropped WM-ed image. This is why this method was called *holographic*, it is a metaphor of the physical hologram where the whole can be recovered from its small part.

The authors of [7] declare that this method allows to embed up to 120 message bits and to extract them correctly using an informed decoder even after several attacks as cropping, JPEG compression, changing of contrast and some other combinations of them. The embedding procedure is performed then as follows:

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

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

$$W_b(u,v) = 1 + (-1)^b \varepsilon \text{ whenever } (u,v) \in S_{ij}^b, \tag{2}$$

with $\left(S_{ij}^0\right)_{ij}$, $\left(S_{ij}^1\right)_{ij}$ 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, and $I^W = \left(I^W(x,y)\right)_{(x,y)}$ is the resulting watermarked image. An embedding mask can be chosen in different manners. In the paper [7] 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. The extraction of each of the (i,j)-bits is performed by the following rule optimal in additive Gaussian noise attack channel:

$$b_{ij} = \frac{1}{2}\left[1 - \text{Sign}\left(B_{ij}^1 - B_{ij}^0\right)\right] \tag{3}$$

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, $\Re$ 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

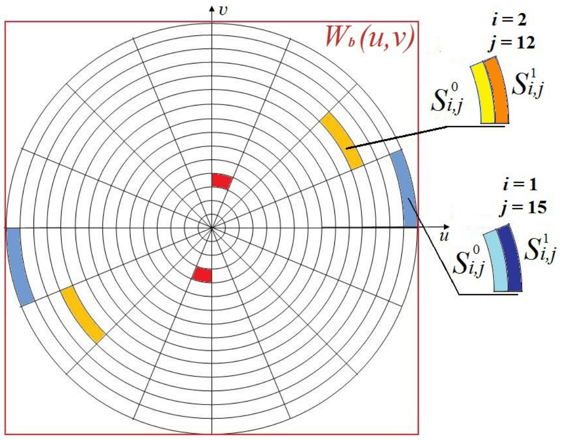


Fig. 1. Equally radius geometry embedding mask.

an *informed decoder*. Moreover, if the WM-ed image has suffered some attack, say cropping of windows or the removal of some rows and columns, it is necessary to know the changed version of the original image after such attacks. This means that the decoder should know the exact place of the window or the locations of rows and columns removed after the attack. Such problem is called the *registration problem*. Sometimes it can be solved very easily (because both attacked and original image are available for the decoder) but sometimes it requires a solution of an additional problem, known as the *registration one*. But we leave the registration problem outside our investigation.

II. Abounding on testing a commonly used method

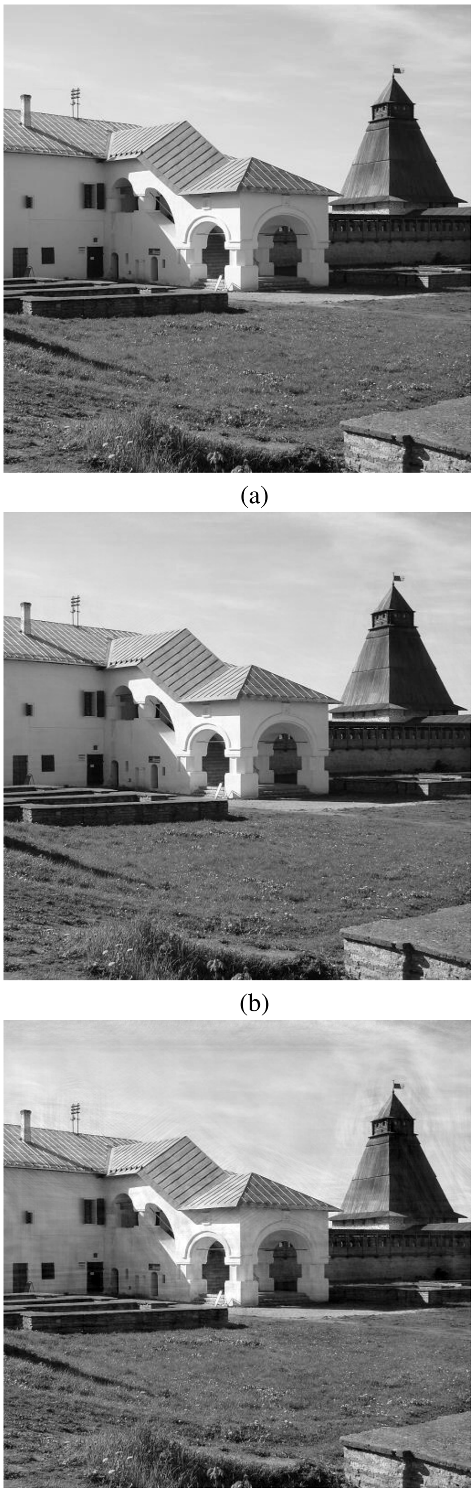
Let us present the tests realized in accordance with the method proposed at [7].

The quality of the watermarked image is determined by the depth of embedding ε. In the Fig. 2, an original image and its watermarked images with $\varepsilon = 0.05$ and $\varepsilon = 0.2$ are presented.

We can see that the quality of the WM-ed image is still acceptable for $\varepsilon = 0.05$ but indeed unacceptable if $\varepsilon > 0.2$. (This claim has been confirmed after a testing of many typical images on computer screens.)

The results of message extraction for different images are presented at Table I, once a given image has been attacked through several transforms, while keeping good image quality after the embedding and attacks.

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 [7] that such WM system satisfies the required conditions for being resistant against any attacks is only partly correct. (It is true only for some specific images). But in order to maintain a good idea proposal in [7] regarding the holographic transform domain and portioning of decision bit area into two subareas in line with the decoding rule (3) we suggest to modify WM system in some manner to adopt it in a modified form.


(a)

(b)

(c)

Fig. 2. Image before and after watermarking. (a) Original image, (b) WM-ed image with $\varepsilon = 0.05$, (c) WM-ed image with $\varepsilon = 0.2$.

TABLE I
THE RESULTS OF ERROR PROBABILITY IN EXTRACTION PROCEDURE AFTER DIFFERENT ATTACKS.

Name of attack	PC
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

PC: Percent of corrupted bits on average of several images.

A description of the extraction procedure results, by simulation after different attacks, within this new approach and and the original method are presented in Section III and IV, respectively.

III. Description of the modified WM system

Firstly, the results of our simulations, which show the probabilities of errors after extraction of bits on different places into the frequency mask and after different attacks, are presented in the Tables II-V.

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.

We could try of course to execute a diversity concept. This means that the same bit is embedded in several cells. But experiments show that a soft decoding occurs useless in this case because the values q_{ij} in eq. (3) are falsely increased for some cells after the JPEG transforms and make worse the result of decision in a comparison with hard decision. One can use the hard (majority) decoding rule but it requires a large multiplicity of diversity and to find the gain to remove bits from "bad" cells which are providing the negligible effect. The amount of bits which have the acceptable probability of error is about 64 and they are displayed at columns 2–9 at Tables III–V. This value is not sufficient in order to embed reasonable information but it may be enough for a scenario of fingerprinting.

Let us consider a situation in which the owner of some image sales it legally to a set of M users without a permission to distribute this product further outside of this buyer set. But some members of the set did illegal redistribution of the product. Fortunately, the owner has access to the illegally redistributed copies. The owner of the product wants to recognize who was the illegal distributor (the "pirate" in other words). It is worth to note that such digital fingerprinting (FP) has very important role in enabling an early-release HD movie window for VOD [8].

In order to solve this problem, the owner can proceed in the following manner: he embeds an 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 trace the pirate. We propose to select unique strings of the length equal to the number of practically error-moderate bits (in our case it is 64). Let us denote by R the area consisting of the columns labelled 2-9 at each of the Tables II-V (emphasized at their displays). The other bits, displayed at columns 10-15 are free of embedding.

Since there may occur errors even among the specially selected 64 bits, it is reasonable to use error-correction codes.

First of all we consider the use of BCH codes of length 63 with a hard decoding on Hamming distance [9], namely the codes $(63, 7)$, $(63, 10)$ and $(63, 16)$. But since the probabilities of bit errors, even among the columns 2-9, depend (as it can be seen from Tables II-V) on the positions of these bits, it is reasonable to use a more effective maximum likelihood decoding algorithm, namely, let:

$$\tilde{j} = \arg \max_{j} \left[\prod_{i \in I(e_{j1})} P_i \cdot \prod_{i \in I(e_{j0})} (1 - P_i) \right] \tag{4}$$

where $\tilde{j}$ is the number of codeword after decoding, P_i is the error probability at the i-th bit, $I(e_{j1})$ is the set of components with value one at the vector e_j (the *support* of e_j), $I(e_{j0})$ is the set of components with value zero at the vector e_j (the *null set* of e_j), and $e_j = u \oplus v_j$ where u is the received binary vector after demodulation by (3), and v_j is the j-th code word at the BCH code.

In the next Section we consider the results of simulation of the proposed approach after attacks by different transforms.

IV. Results of fingerprinting system simulation after different transforms

We use the embedding according to the relations (1), (2) into the area R, the bit extraction by the rule (3) and the decoding of the code words of the BCH codes $(63, 7)$, $(63, 10)$ and $(63, 16)$, by the minimal Hemming distance and maximum likelihood algorithm (4). As image transforms we apply the following ones:

- cropping of windows;
- removal of rows and columns;
- JPEG compression with different quality;
- addition of Gaussian noise.

We selected 1000 grey scaled images from the bank of images [10] and each of these images was tested 10 times with randomly chosen bit embedding. In reality we try BCH codes of the length 63 for more variants on the number of information bits, other than 3, but we show now only those cases in order to justify that there is no sense to take $k > 10$, because it results in poor probability of correct decoding even after the use of an optimal decoding algorithm.

In the Fig. 3 a fingerprinted image and its cover image after different transforms are presented.

TABLE II
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 III
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 IV
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

TABLE V
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

In all cases we assume that the original image is known during the extraction procedure. Sometimes this condition can be provided very easily, whereas sometimes it requires to solve an additional problem for the original image registration, in this last case we refer to cropping (where it is necessary to know the window) or to row and column removal (where it is necessary to know which of them have been removed).

It is worth to note that the pirates can remove rows or columns in two different ways.

Consider the first way. A pirate selects some rows (or columns) and changes them to another ones, which can be obtained by interpolation of neighboring lines. In this case the image size and places of another rows are not changed. Hence it is the case when it is not necessary to solve a problem of original image registration.

Another case arises where the pirate deletes the lines and then he shifts the remaining lines to make invisible the removal place. In this case, the image size and places of several lines

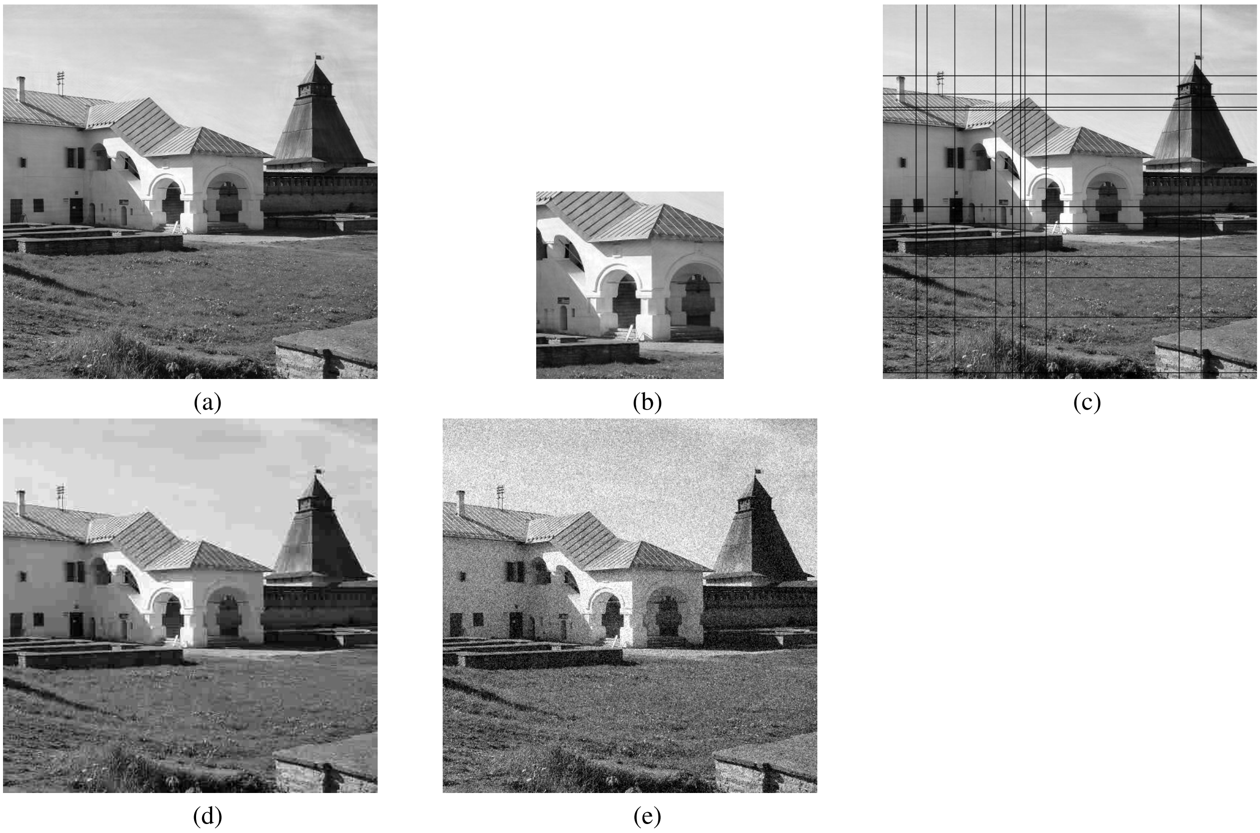


Fig. 3. Fingerprinted image (a) and the same image after different transforms: (b) cropping of window 200×200 pixels, (c) removal of rows and columns, (d) JPEG compression with factor $Q = 20$, (e) addition of Gaussian noise with $d = 25$.

are changed. Therefore for extraction procedure it is necessary to solve a registration problem.

The results of simulation (in terms of the incorrect decoding probabilities) depending on the type of code and different attack transforms are presented in Table VI.

Similar results for optimal decoding algorithm are shown in Table VII.

We note that for those attacks that can be easily recognized by a legal user (removal of rows and columns, cropping, addition of noise) the values of the symbol probabilities P_i, that are necessary for optimal decoding by the algorithm (4) can be taken from Tables IV–V, whereas it is hard to establish the quality factor Q used in the JPEG transform. The probabilities for the worst case ($Q = 20\%$) can be used because we proved that it results in the minimal probability of incorrect decoding on average.

From Tables VI–VII 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 and the optimal decoding algorithm given by (4) is superior to the minimal Hamming distance algorithm.

V. Conclusion

Traitor tracing is a very important problem in the case of an early release of HD movie window for VOD. In the current paper we adopt a general idea to embed WM using the so called “holographic” concept [7] when the embedding procedure is performed in the Fourier domain. However we showed that such WM system is vulnerable to different image transforms which provide still a good image quality after them. Therefore we propose a modification of the WM system considered in [7] to a fingerprinting system, where it is sufficient to provide only a limited number of identification code words corresponding to different users that can be potential pirates. In a particular case we have selected 64 bits which survive after most of the transforms and we propose to execute a binary $(63, 10)$-BCH code to correct errors. We propose also to use a maximum likelihood decoding algorithm instead of the minimum Hamming distance algorithm since that is more effective

The simulation results showed that for many typical images the proposed fingerprinting scheme is resistant to such transforms as cropping, removal of rows and columns, JPEG compression and addition of Gaussian noise. Therefore we are rather sure that the proposed scheme can be recommended for practical applications to copyright protection within fingerprinting procedures.

But the problem of original image registration arises.

Sometimes it is easy to solve because the original images always are at the disposition of their owners. But sometimes it requires to know some parameters of transforms (as numbers

TABLE VI
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)\(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).

TABLE VII
THE PROBABILITIES OF INCORRECT DECODING BY OPTIMAL DECODING ALGORITHM 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)\(2)	0.05			0.1		
Saving in JPEG format with Q=20%	1.0×10^{-2}	1.4×10^{-1}	3.9×10^{-1}	1.5×10^{-3}	4.1×10^{-3}	1.0×10^{-2}
Saving in JPEG format with Q=30%	2.1×10^{-3}	3.8×10^{-3}	1.1×10^{-2}	1.0×10^{-4}	1.0×10^{-3}	3.5×10^{-3}
Saving in JPEG format with Q=60%	4.0×10^{-4}	9.0×10^{-4}	2.1×10^{-3}	1.0×10^{-4}	1.0×10^{-4}	1.0×10^{-4}
Cropping of window 200 × 200 pixels	8.5×10^{-3}	1.2×10^{-2}	2.2×10^{-3}	4.3×10^{-3}	9.1×10^{-3}	1.6×10^{-2}
Cropping of window 250 × 250 pixels	1.9×10^{-3}	3.8×10^{-3}	6.1×10^{-3}	2.1×10^{-3}	3.0×10^{-3}	4.7×10^{-3}
20 rows and 20 columns removal	2.8×10^{-3}	6.5×10^{-3}	1.4×10^{-2}	4.0×10^{-4}	1.3×10^{-3}	3.9×10^{-3}
Addition of Gaussian noise with $d = 25$	1.5×10^{-2}	3.1×10^{-2}	7.5×10^{-2}	2.0×10^{-3}	4.3×10^{-3}	1.2×10^{-2}

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

of the removed rows and columns and their places) executed by pirates. This is still an open problem in general. Another problem is to change the equality radius geometry embedding mask (see Fig. 1) to another one in order to try to use the area with columns 10-15 (or maybe areas structured by another manner) to embed more than 10 bits with good enough probability of correct decoding. We are going to investigate these problems in the near future.

REFERENCES

[1] I. J. Cox, M. L. Miller, and J. A. Bloom, *Digital Watermarking*. Morgan Kaufman Publishers, 2002.

[2] M. Barni and F. Bartolini, *Watermarking systems engineering: enabling digital assets security and other applications*, ser. Signal processing and communications. Marcel Dekker, 2004. [Online]. Available: http://books.google.co.uk/books?id=DUuyektSYH0C

[3] J. Ó Ruanaidh and T. Pun, "Rotation, scale and translation invariant digital image watermarking," in *IEEE Int. Conf. on Image Processing ICIP1997*, 1997, pp. 536–539.

[4] C.-S. Woo, J. Du, and B. Pham, "Geometric invariant domain for image watermarking," in *IWDW*, ser. Lecture Notes in Computer Science, Y.-Q. Shi and B. Jeon, Eds., vol. 4283. Springer, 2006, pp. 294–307.

[5] S. Anfinogenov, V. I. Korzhik, and G. Morales-Luna, "Robust digital watermarking system for still images," in *FedCSIS*, M. Ganzha, L. A. Maciaszek, and M. Paprzycki, Eds., 2011, pp. 685–689.

[6] ——, "A multiple robust digital watermarking systems fro still images," *International Journal of Computer Science and Application*, vol. 9, no. 3, pp. 37–46, 2012.

[7] A. Bruckstein and T. Richardson, "A holographic transform domain image watermarking method," *Circuits, Systems, and Signal Processing Journal Special Issue*, vol. 17, no. 3, pp. 361–389, 1998.

[8] D. W. Alliance, "The digital watermarking alliance overview presentation," http://www.digitalwatermarkingalliance.org/docs/presentations/dwa_presentation.pdf, 2006–2011.

[9] F. J. Macwilliams and N. J. A. Sloane, *The Theory of Error-Correcting Codes*, ser. North-Holland Mathematical Library. North Holland, January 1983. [Online]. Available: http://www.amazon.com/exec/obidos/redirect?tag=citeulike07-20\&path=ASIN/0444851933

[10] P. Bas, T. Filler, and T. Pevný, ""Break our steganographic system": the ins and outs of organizing BOSS," in *Proceedings of the 13th international conference on Information hiding*, ser. IH'11. Berlin, Heidelberg: Springer-Verlag, 2011, pp. 59–70. [Online]. Available: http://dl.acm.org/citation.cfm?id=2042445.2042452