Digital Watermarking System for Hard Cover Objects Against Cloning Attacks

Valery Korzhik, Vladimir Starostin, Victor Yakovlev, Dmitri Flaksman, Ivan Bukshin
The Bonch-Bruevich Saint-Petersburg State University of Telecommunications
Saint-Petersburg, Russia
val-korzhik@yandex.ru, star_vs_47@mail.ru, viyak@bk.ru, flxdima4951@gmail.com, dr.ivan@yandex.ru

Boris Izotov
Stock Company Scientific instruments
Saint-Petersburg, Russia
izotov@sinstr.ru

Abstract — **We consider an application of digital watermark system technique for hard carriers (paper or plastic cover objects in addition). Algorithms of watermark embedding and extraction are proposed and the corresponding error probabilities of the extracted bits both for informed and blind decoders are presented. The spread spectrum signals used for embedding of watermark are optimized on their parameters. Similar experimental results are presented for data matrices carriers depending on paper sizes of data matrix copies. A protection against so-called "cloning" attack is elaborated where certificates are copied by attack scanner or photo camera and next printed and fixed as forges. The formulas for a missing the cloning attack and false alarm probabilities are proved. A full-scale experiment with a real scanner and printer confirms that the reliability of cloning attack detection can be provided under appropriate selection of watermark system parameters.**

I. Introduction

In today's world, a security of different data is very important for copyright protection and authenticity verification. The challenges in question are detection of fake invoices, bank checks, tax forms, and other valuable documents. Due to development and availability of printing and scanning devices, the number of forged / counterfeited documents and product packages that are manufactured out of paper, photo paper, or special plastic, is increasing.

The mentioned peculiarities require to develop the WM embedding and extraction algorithms more carefully in comparison with ordinary WM executing as the rule with digital cover objects which are stored on computers, CDs, and other electronic devices, but not on such analog carriers as paper or plastic. [1], [2]

In the papers [3], [4] WM systems for graphical QR-codes are proposed based on corruption of separate blocks including bar codes. However, such approach requires a change in bar-code structure itself. Another technique, which embeds a particular random micro-texture into a matrix barcode is presented in paper [5]. In the current paper we suggest to use digital watermarking for analog cover objects (including bar codes) while keeping a reliable extraction of the embedded information even after their printing and next scanning.

However, there exists a more sophisticated attack: first, copying watermarked objects using a scanner or camera, then printing a new paper object and attaching it to another object that no longer meets the declared quality.

At a single glance, such attack cannot be detected at all. However, we suggest a new method for dealing with such type of attacks, based on calculation of noise power after such attack.

WM embedding and extraction algorithm is described in section II. Its efficiency is estimated in terms of the error bit number both for images and for the CO barcode.

Section III presents an algorithm of cloning attack detection and formulas derivation for the probability of cloning attack missing and the false alarm one.

Section IV demonstrates the results of experiments verifying the correctness of the model chosen in Section III.

Section V summarizes the main results and proposes possible directions for further investigations.

II. WM embedding and extraction algorithm for analog cover objects (like paper, photo paper and plastic).

A. Embedding algorithm

Let us first present the spread-spectrum signal following the well-known rule defined in [6]:

$$w(n)=\alpha(-1)^{bi}\pi_i(n), n=1,2,...N_0, i=1,2,...m=\frac{N}{N_0} \quad (1)$$

where α is the depth of embedding, $\pi_i(n)=\pm(1), n=1,2,...N_0$ is a pseudorandom sequence (PRS) of the length N_0 for embedding of i-th message bit, b_i is the i-th embedding bit, N - is the total number of CO samples, m - is the number of the embedding bits.

The scheme of embedding procedure for color (RGB) image is presented in Fig.1. Here notation SSS stands for a generation of 'spread spectrum signals' and IDCT – for an 'inverse discrete cosine transform' [7]. 'Zigzag' is a method of the signal spreading among elements of CO [7]. (We note that zigzag scheme allows to diverse errors after bit extraction).

The scheme of WM extraction is presented in Fig. 2, where DCT is a discrete cosine transform.

The feature of extraction from an analog CO is so called '*perspective transforms' (PT)*. They appear due to scanning or photographic occurring not necessary perpendicular to the surface of CO, which results in a specific corruption of CO [7].

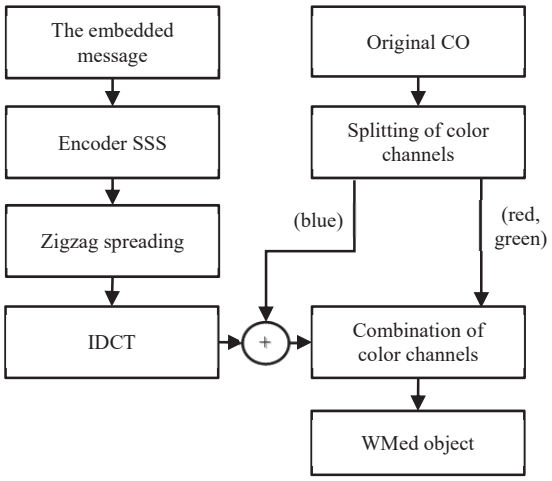


Fig. 1. Scheme of watermark embedding

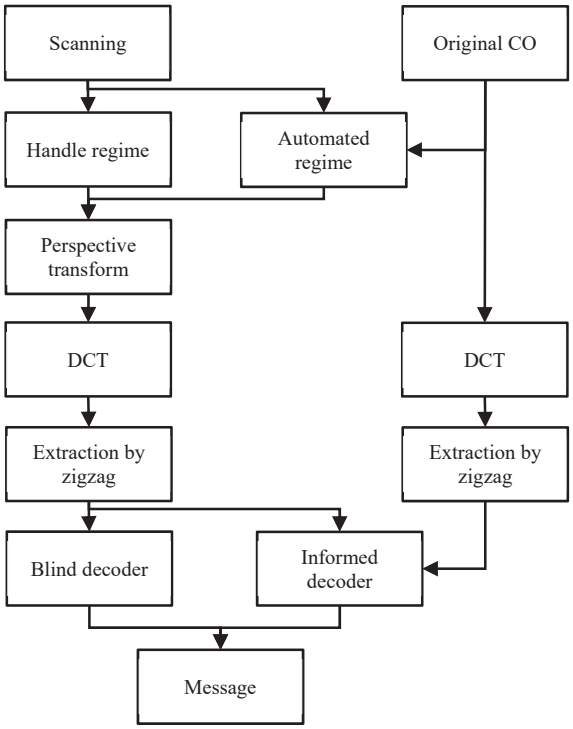


Fig. 2. Scheme of watermark extraction

PT can be described by the following matrix relation:

$$\begin{pmatrix} x' \\ y' \\ w \end{pmatrix} = \begin{pmatrix} t_{11} & t_{12} & t_{13} \\ t_{21} & t_{22} & t_{23} \\ t_{31} & t_{32} & t_{33} \end{pmatrix} \begin{pmatrix} x \\ y \\ 1 \end{pmatrix}, \quad (2)$$

where x', y' are new coordinates, x, y are old coordinates, t_{ij} - are matrix coefficients, w - depth of transform (scale).

In Fig. 3(a) is presented original image (CO) whereas in Fig. 3(b) there is the same image after some perspective transforms.

(a) (b)

Fig. 3. Original CO (a) and CO after a perspective transform (b)

In order to extract WM correctly it is necessary to initially compensate PT, which can be done by different methods (both using manual and automated regimes).

It seems that RANSAC – 'random sample consensus' proposed in 1981 by Fisher and Bolles [9] is the most effective method that has been implemented by a program written on C++ with the use of the "OpenCV" library.

Eventually, it can be implemented either by informed or blind decoder following well known relations:

$$b_i = \begin{cases} 1, if\ \Lambda < 0 \\ 0, if\ \Lambda \geq 0, \end{cases} \quad (3)$$

where $\Lambda = \sum_{n=1}^{N_0} (C'_{wi}(n) - C(n))\pi_i(n)$ for informed decoder,

$\Lambda = \sum_{n=1}^{N_0} C'_{wi}(n)\pi_i(n)$ for blind decoder,

where $C'_{wi}(n)$ are the samples of scanned (or photo-made) watermarked object on any i-th bit interval.

A natural experiment was conducted with the use of both grey-scall and color images of the size 9x9cm with 512x512 pixels each. Laser printer "Eyocera Ecosys P6021cdn" and scanner "Canon LiDE220" with resolution 1200dpi were used. The goal of the experiment was to optimize the embedding depth α and the length of PRS (N_0) with a purpose of minimizing the extracted number bit errors while keeping a good quality of CO (image) after embedding. The results of such experiments for optimal embedding PRS length N_0=500 against different embedding depth α and the number of the embedded bits m are presented in Table I.

We can see from Table I that for both informed and blind decoders the number of error bits are acceptable for practice when PRS length is at least 7.

As it was mentioned before, the use of data matrix is very common for paper or plastic certificates. In Fig. 4 both "clear" data matrix a), and the same matrix with SSS-based embedding

TABLE I. THE NUMBER OF THE ERRONEOUSLY EXTRACTED BITS AGAINST THE EMBEDDING DEPTH α AND THE TOTAL NUMBER OF BITS m BOTH FOR INFORMED AND BLIND DECODERS

Decoders	The number of the embedded bits m	Embedding depth α					
		4	5	6	7	8	9
Informed / blind decoders	64	3 / 9	1 / 4	0 / 1	0 / 0	1 / 0	0 / 0
	128	4 / 11	2 / 4	3 / 2	2 / 0	1 / 0	0 / 0
	256	43 / 40	21 / 19	34 / 38	1 / 15	2 / 0	2 / 2

for $N_0 = 700$ and $\alpha = 15$ are shown. We can see from Fig. 4b) that there exists some insignificant black/white modulation due to the use of SSS signals for embedding.

The results for erroneously extracted by informed decoder bits from two different data matrices with parameters $\alpha = 15$, $N_0 = 70$ and different sizes of paper copies are presented in Table II.

We can see from Table II that the number of errors depends on the physical paper size of data matrices. These results show that for the size of at least 3x3cm one can more-less reliably extract 128 bits. For the size 5x5cm one could extract even up to 320 bits.

TABLE II. THE NUMBER OF ERRONEOUSLY EXTRACTED BITS FOR DIFFERENT SIZES OF DATA-MATRICES

The number of embedded bits m	Image 1 / Image 2					
	2×2	3×3	4×4	5×5	6×6	9×9
64	9 / 19	3 / 5	2 / 2	2 / 2	2 / 2	2 / 2
128	40 / 52	6 / 22	3 / 2	2 / 2	2 / 2	2 / 2
256	94 / 101	52 / 76	24 / 17	2 / 3	2 / 2	2 / 2
320	114 / 130	75 / 95	43 / 34	5 / 9	2 / 2	2 / 2

We also conducted experiments for WM extraction from data matrices copied by mobile telephone. The results occurred to be slightly worse, namely, one could reliably extract only about 128 bits out of a 6x6cm size paper.

III. DETECTION OF "CLONING" ATTACK WITH THE HELP OF WATERMARKING PROCEDURE.

Protection of different solid things (or products) is in a great demand now. It can be classified as a very specific area of information security.

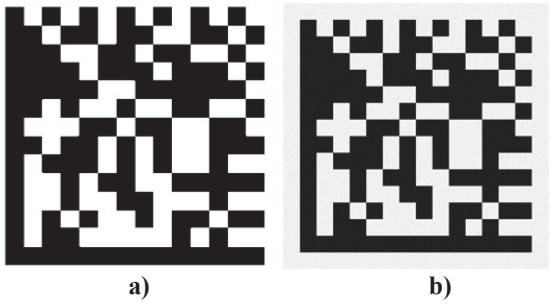
In fact, such items as medical drugs, different materials, etc. should be protected against changing by counterfeits of lower quality. Very often, special certificates are used to protect against such dishonest activities. Usually, they are strongly attached to the objects of certification and are responsible for the appropriate quality of the objects.

But let us consider the following scenario which is called a "*cloning attack"*.

A swindler makes copies of certificates using scanner or photo camera. Then he prints forged certificates and attaches them to counterfeited items (say, a bottle of wine or a box of medical drugs) which are of lower quality and hence cheaper in production.

As the aspired high quality is declared, swindler hopes to sale goods for higher price mentioned in the new "certificate".

At first glance, the problem of detecting a fake certificate could not be resolved at all if the information recorded in the certificate was not related to the content of things.



a) **b)**

Fig. 4. Data matrix-based cover object a) and the same matrix with watermark embedding with parameters $N_0 = 700$, $\alpha = 15$

Of course, you could try to test the properties of the goods and understand that they do not meet the declared certificate requirements. But this way of detecting a forgery would be too pricy. This means that the results of a validated qualification procedure should be *verified before buying*, by analyzing certificate itself only in advance.

This means that if we want to discover certificate cloning attack, we must investigate the difference between procedures of certificate validation between a legal user (buyer) and a swindler. Let us illustrate this difference.

Using (1) we get the following relation for a WMed object:

$$C_{wi}(n) = C(n) + \alpha(-1)^{bi}\pi_i(n), n = 1,2,...N_0, i = 1,2,...m$$

If there is no cloning attack, we get the following on our computer after printing and scanning (for extraction of WM):

$$C'_{wi}(n) = C(n) + \alpha(-1)^{bi}\pi_i(n) + N_{p1}(n) + N_{s1}(n), \quad (4)$$

where $N_{p1}(n)$ is a printing noise sample sequence,

$N_{s1}(n)$ is a scanning noise sample sequence obtained after attack detection.

If there is a cloning attack we get instead of (4), the following relation:

$$C^{"}_{wi}(n) = C(n) + \alpha(-1)^{bi}\pi_i(n) + N_{p1}(n) + N_{s2}(n) + \\ + N_{p2}(n) + N^{'}_{s1}(n), \quad (5)$$

where $N_{s2}(n)$ is a scanning noise which appears when a swindler makes a copy of a certificate,

$N_{p2}(n)$ is a printing noise of swindler,

$N^{'}_{s1}(n)$ is a scanning noise for attack detection.

Comparing (4) and (5) we can see that they differ in two noise sequences $N_{s2}(n)$ and $N_{p2}(n)$ because the noise sequences $N_{s1}(n)$ and $N^{'}_{s1}(n)$, belong both to a legitimate user and hence they have equal characteristics. Let us assume that all noise sequences are zero mean Gaussian ones but with different variances, namely

$$Var\{N_{p1}(n)\} = Var\{N_{s1}(n)\} = Var\{N^{'}_{s1}(n)\} = \sigma^2,$$

$$Var\{N_{s2}(n)\} = Var\{N_{p2}(n)\} = \frac{\sigma^2}{r}, r \geq 1.$$

The last equation means that we assume that a swindler has even some superior noise power situation against legitimate users.

It follows from model of scenario above that there is only one way to distinguish a cloning attack against its absence, namely – a presence of a greater noise power after a cloning attack than for the case of no cloning attack situation.

In order to improve a statistical estimate of noise power, let us assume that watermarked object $C_{wi}(n)$ is strictly known (say stored) by a legitimate user. Then we should compare the following noise sequences.

$$\lambda^{'}(n) = C^{'}_{wi}(n) - C_{wi}(n) = N_{p1}(n) + N_{s1}(n), \quad (6)$$

and

$$\lambda^{"}(n) = C^{"}_{wi}(n) - C_{wi}(n) = N_{p1}(n) + N_{s2}(n) + \\ + N_{p2}(n) + N^{'}_{s1}(n). \quad (7)$$

Taking into account our previous suggestion regarding noise powers (variances) of $\lambda^{'}(n)$ and $\lambda^{"}(n)$ we get the following relations:

$$Var\{\lambda^{'}(n)\} = 2\sigma^2, Var\{\lambda^{"}(n)\} = 2\sigma^2 r^{'} \quad (8)$$

where $r^{'} = \frac{r+1}{r}$

Then the decision rule about a presence or absence of cloning attack will be the following:

If $\Omega \geq \Omega_0$ - there is a cloning attack, (9)

if $\Omega < \Omega_0$ - there is no cloning attack,

where Ω_0 is some threshold (chosen in advance),

$$\Omega = \frac{1}{N}\sum_{n=1}^{N}\lambda^2(n),$$

$$\lambda(n) = C_w(n) - C_{wi}(n), n = 1, 2, ...N$$

$C_w(n)$ is the sequence extracted from testing a WMed object.

Next problem is to prove the formulas that describe efficiency of cloning detection algorithm in terms of P_m (missing of cloning detection) and P_{fa} (false alarm of cloning detection).

Follow to the Central Limit Theorem of probability theory [10], we assume that for large N the random value Ω in (9) belongs to the Gaussian distribution. Then one only has to find the variance and expectation of the random value Ω.

Using (8) we get easy that [11]:

a) For an absent cloning attack – (H_0 hypothesis)

$$E\{\Omega\} = 2\sigma^2$$
$$Var\{\Omega\} = \frac{8}{N}\sigma^4 \quad (10)$$

b) For the presence of a cloning attack (H_1 - hypothesis)

$$E\{\Omega\} = 2\sigma^2 r^{'}$$

$$Var\{\Omega\} = \frac{8}{N}\sigma^4 (r^{'})^2. \quad (11)$$

Then using (10), (11) we get the formulas for probabilities P_m and P_{fa}:

$$P_m = \Pr\{\Omega < \Omega_0 / H_1\} = 0,5 + \\ + \Phi(\sqrt{N}\frac{\Omega_0 - 2\sigma^2\frac{r+1}{r}}{\sigma^2 2\sqrt{2}} \times \frac{r}{r+1}) \quad (12)$$

$$P_{fa} = \Pr\{\Omega \geq \Omega_0 / H_0\} = 0,5 - \Phi(\sqrt{N}\frac{\Omega_0 - 2\sigma^2}{\sigma^2 2\sqrt{2}})$$

where

$$\Phi(x) = \frac{1}{\sqrt{2\pi}}\int_0^x \exp(-\frac{t^2}{2})dt \quad (13)$$

The threshold Ω_0 controls a tradeoff between the probabilities P_m and P_{fa}. To optimize Ω_0 let us minimize the average error probability

$$P_e = \frac{P_m + P_{fa}}{2} = \frac{1}{2}(1 + \Phi(\sqrt{N}\,\frac{\Omega_0 - 2\sigma^2\,\frac{r+1}{r}}{\sigma^2 2\sqrt{2}} \times \frac{r}{r+1}) - \\ -\Phi(\sqrt{N}\,\frac{\Omega_0 - 2\sigma^2}{\sigma^2 2\sqrt{2}})) \quad (14)$$

In order to find such optimal Ω_0, we have to differentiate (14) on variable Ω_0 and equal the result to zero:

$$\frac{r\sqrt{N}}{2\sqrt{2}\sigma^2(r+1)}\Phi(\sqrt{N}\,\frac{\Omega_0 - 2\sigma^2\,\frac{r+1}{r}}{\sigma^2 2\sqrt{2}} \times \frac{r}{r+1}) - \\ -\frac{\sqrt{N}}{2\sqrt{2}\sigma^2}\Phi(\sqrt{N}\,\frac{\Omega_0 - 2\sigma^2}{\sigma^2 2\sqrt{2}}) = 0 \quad (15)$$

where $\varphi(t) = \frac{1}{\sqrt{2\pi}} e^{-\frac{t^2}{2}}$

After a simplification of equation (15) we get:

$$\Omega_0(1 - \frac{r}{r+1})(\Omega_0(1 + \frac{r}{r+1}) - 4\sigma^2) = \frac{16\sigma^4}{N}(1 + \frac{1}{r}) \quad (16)$$

With respect to variable $\omega = \Omega_0 / \sigma^2$ it is quadratic equation:

$$\omega^2\,\frac{2r+1}{(r+1)^2} - \omega\,\frac{4}{r+1} - \frac{16}{N}\ln(1 + \frac{1}{r}) = 0 \quad (17)$$

The positive root of (17) is:

$$\Omega_0 = \sigma^2\,\frac{r+1}{2r+1}(2 + \sqrt{4 + \frac{16}{N}(2r+1)\ln(1 + \frac{1}{r})}) \quad (18)$$

For large N (as it is in line with practice),

we get from (18)

$$\Omega_0 = 4\sigma^2\,\frac{r+1}{2r+1} \quad (19)$$

The values of optimal threshold depending on different parameter's r values are presented in Table III.

Substituting (9) into (14) we obtain after a simple, but tedious transforms the following relation for the value P_e:

$$P_e = \frac{P_m + P_{fa}}{2} \approx \frac{1}{2}\left(1 + \Phi\left(-\frac{\sqrt{N}}{\sqrt{2}(2r+1)}\right) - \Phi\left(\frac{\sqrt{N}}{\sqrt{2}(2r+1)}\right)\right) = \\ = \frac{1}{2} - \Phi\left(\frac{\sqrt{N}}{\sqrt{2}(2r+1)}\right) \quad (20)$$

In order to simplify (20) one can use the following approximation of the Laplace function $\Phi(x)$ [12].

$$\Phi(x) \approx \frac{1}{2} - \frac{1}{\sqrt{2\pi}}\,\frac{e^{-\frac{x^2}{2}}}{x} \quad (21)$$

Substituting (21) into (20) we get approximately:

$$P_e \approx \frac{e^{-\frac{x^2}{2}}}{2\pi x} \quad (22)$$

where

$$x = \frac{\sqrt{N}}{2(2r+1)}.$$

The results of calculation P_e against the total number of samples N for different parameters $r = 1, 2, 4, 8, 16.$ are shown in Fig. 5.

TABLE III. THE VALUES OF OPTIMAL THRESHOLD DEPENDING ON PARAMETER r

r	1	2	4	8	16
Ω_0	$2{,}66\sigma^2$	$2{,}4\sigma^2$	$2{,}22\sigma^2$	$2{,}06\sigma^2$	$1{,}94\sigma^2$

In Table IV are presented (for better visibility) the values P_e for real lengths of testing sequence and parameter's r values.

We can see from this Table that if for example $N_0 = 500$ and $m = 64$, we get $N = N_0 m = 3\times10^4$, then P_e will be much less than 5×10^{-2} even for $r = 16$. On the other hand, it is unlikely that noise power will be in 16 times less for swindler's devices than it is for the legitimate ones.

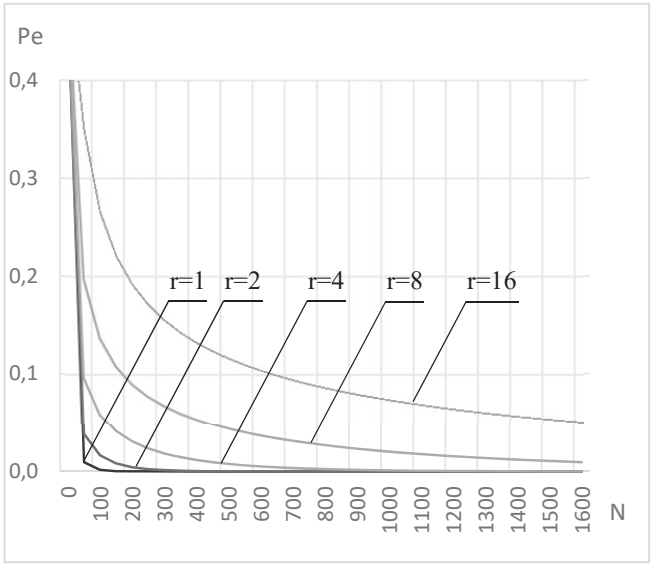


Fig. 5. The probabilities P_e of cloning detection error against the total number N of sample, for different parameters r

TABLE IV. THE PROBABILITIES P_e FOR TOTAL NUMBER OF SAMPLE FOR TESTING AND DIFFERENT PARAMETERS r

N / r	600	800	1000	1200	1500	30000
1	0	0	0	0	0	0
2	0.000046	0.0000053	0.00000065	0.000000079	0.0000000036	0
4	0.0052	0.0024	0.0012	0.00058	0.00021	0
8	0.037	0.027	0.021	0.016	0.011	0
16	0.11	0.087	0.074	0.065	0.054	0.00002

IV. EXPERIMENTAL RESULTS VERIFYING OF THE MAIN MODEL

Our scheme of the cloning detection attack is presented in Fig.6.

We can see from Fig.6 that the watermarked certificate is performed on personal computer (PC) and next it is printed on ordinary paper.

To check a validation of certificate in case of no cloning attack it is read by scanner into PC, $\lambda'(n), n = 1, 2, ...N$ is calculated by (6) and stored. This procedure is repeated many, say M, times. Eventually decision about the presence or absence of a cloning attack is taken following the decision rule (9) given some threshold Ω_0.

To simulate a cloning attack the certificate is read by the same (or another, less noisy) scanner, printed, read by legitimate scanner, processed by (7) $\lambda_i(n), n = 1, 2, ...N$ and stored on a PC. This procedure is repeated many (say M) times and eventually one takes decisions on presence or absence of a cloning attacks following to the formula (9). Given threshold Ω_0, the average error probability P_e is calculated by the left side of (14) for both cases (cloning or no cloning attacks). Varying the threshold Ω_0, we try to minimize P_e.

It is worth noting that it is impossible to simulate all values $\lambda'(n)$, $\lambda''(n)$ using PC only because it requires experiments with real hardware devices. This means that such simulation requires a "lot of time" if we want to get a reliable estimation for the probability P_e and to specify the correct choice of optimal threshold Ω_0.

Therefore, we restrict our experiment by reasonable number of repetitions M, say 20 or 50 in the current paper. A more detailed experimental investigation we are going to put off until our next publications.

The values of the average error probabilities P_e against different threshold Ω_0 are presented in Table V.

We can see from this Table that, in fact, the value P_e is depends on the value of threshold Ω_0 and the value P_e is minimized by $\Omega_0 = 744.855$.

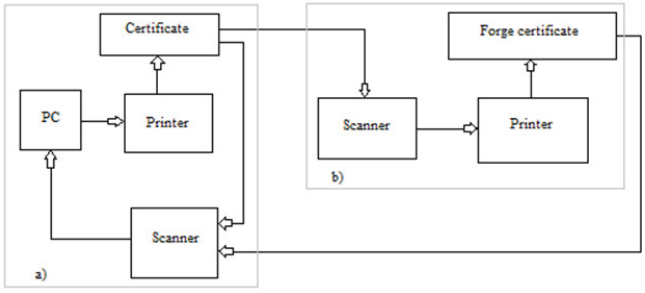


Fig. 6. a) Certificate validation without and with cloning attack, b) creation of forge certificate by cloning attack.

TABLE V. THE EXPERIMENTAL DEPENDANCE OF THE AVERAGE ERROR PROBABILITY P_e AGAINST DIFFERENT THRESHOLD VALUES Ω_0 UNDER CONDITION r =1. (THE EMBEDDING DEPTH IS 10, THE PRS LENGTH IS TAKEN EQUAL TO 700, THE NUMBER OF TRIAL M=100).

Ω_0	730	740	744.855	750	760
$P_e(\Omega_0)$	0.2	0.075	0	0.075	0.125

V. CONCLUSION.

Protection of various solid objects (or products) is in high demand nowadays. It can be classified as a very specific area of information security.

The first of our contributions was the verification of the fact that WM technique can be applied not only to digital CO but to "analog carriers" like paper, photo paper, plastic etc., in such a way as to maintain a good quality of the images (also including data matrices).

The efficiency of watermarking was estimated in terms of the BER for extracted information after embedding and depends on the main WM system parameters (PRS length and embedding depth). Similar approach can be found in [13].

Our main contribution is the proposal of a cloning attack detection algorithm and proving the formula for the probabilities of incorrect detection of such attacks in terms of P_m, P_{fa} and P_e depending on chosen threshold Ω_0 of the decision scheme. Also, one unexpected fact was established: the average probability P_e of the incorrect cloning detection attack does not depend on the noise powers of both legitimated and adversary devices but it does on the ratio of those noise powers only!

Although natural (based on real devices) experiments were conducted with insufficiently large statistics, that the main idea of cloning attack detection surviving in real conditions was confirmed.

We are going to extend our investigations by providing more statistical data in future.

Another interesting problem for further investigations in the nearest future can be a consideration of a larger set of certificate carriers including as well as stained paper.

ABBREVIATIONS

CD	Compact disk
CO	Cover Object
DCT	Discrete cosine transform
IDCT	Inverse discrete cosine transform
PC	Personal Computer
PT	Perspective transform
PRS	Pseudo random sequence
RGB	Color image standard (red, green, blue)
SSS	Spread spectrum signals
WM	Watermark

REFERENCES

[1] S. Duan, H. Wang, Y. Liu, Li Huang, and X. Zhou, “A novel comprehensive watermarking scheme for color images”, *Security and communication networks*, 2020.

[2] M. Begum, M. S. Uddin, “Analysis of digital image watermarking techniques through hybrid methods”, *Advances in Multimedia*, 2020.

[3] I. Tkachenko, “Generation and analysis of graphical codes using textured patterns for printed document authentication”, *Signal and Image processing. Université de Montpellier*, 2015.

[4] I. Tkachenko, “Generation and analysis of graphical codes using textured patterns for printed document authentication”, *D.Sc Thesis, Montpellier: Université de Montpellier*, 2015.

[5] H. P. Nguyen, F. Retraint, F. Morain-Nicolier, A. Delahaies, “A watermarking technique to secure printed matrix barcode - application for anti-counterfeit packaging”, *IEEE Access (Volume: 7)* 2019.

[6] V. I. Korzhik, et al *Digital steganography and digital watermarks. Part 1. Steganography*, Monograph, SPb, SUT, 226p., 2016 (in Russian).

[7] V. I. Korzhik, etal *Digital steganography and digital watermarking. Part 2. Digital Watermarking*, Monograph, SPb, SUT, 198p., 2017 (in Russian).

[8] Y. Fridrich, *Steganography in digital media: principles, algorithms and applications*, 2010, Cambridge Press.

[9] M. A. Fischler, R. C. Bolles “Random sample consensus: a paradigm for model fitting with applications to image analysis and automated cartography”, *Communications of the ACM,* 1981, 24(6):381–395.

[10] Van der Warden, *Mathematische statistic*, Springer Verlag, 1957.

[11] V. I. Korzhik, D. F. Flaksman, “Digital Watermark System with an Ability of its Extraction from Hard Copies of Data”, *Proc. of Telecom. Universities*, 2019, 5(3):75–85. (in Russian).

[12] V. I. Korzhik, etal “Calculation of BER for digital communication”, *Handbook, Radio and Com.*, 1981 (in Russian).

[13] A. T. S. Ho., F. Shu. “A print-and-scan resilient digital watermark for card authentication.” *Proceedings of the Fourth International Conference on Information, Communications and Signal Processing and The Fourth Pacific Rim Conference on Multimedia*, 15–18 December 2003, Singapore. IEEE; 2003. vol.2. p.1149–1152.