004.056.53

. .   ,   .   .   ,
. .

LUT-

.

(   )   .   -
-
LUT-   .   -

LUT-   .   -
.

:   ,   ,
,   ,   ,   -   , *LUT-*
,   *FPGA*

K. V. Zashcholkin, PhD.,
E. N. Ivanova

INFORMATION TECHNOLOGY OF EMBEDDING SELF-RECOVERY
DIGITAL WATERMARK IN LUT-ORIENTED CONTAINERS

Abstract. *The approaches to the control of use of information objects by means of technology of digital watermarking were reviewed. The necessity to recovery of original of information object (container for digital watermark) after extracting digital watermark from it was marked. We propose an information technology embedding self-recovery digital watermark in containers with LUT-oriented architecture. The technology is based on composition of approaches to organisation self-recovery digital watermarks in passive multimedia containers and approaches to embedding additional information in the LUT-containers. Information about the practical implementation of the proposed technology was presented.*

Keywords: *digital watermarks, control of use of information objects, data protection, steganography, embedding of additional data, hardware stego-container, LUT-oriented architecture, FPGA chips*

. .   ,   .   .   ,
. .

LUT-

.   ,   -
.   )   ,   (-
)   .   -
.   *LUT-*

.   -
LUT-   .   ,   .

:   ,   ,   ,
,   ,   -   , *LUT-*   ,
FPGA

.   -   -
(   ) [1]   :   ,
-                            [2], [3].

.   -
-   ,
.
-   (   ).
DRM-   (Digital Rights Menage-   -
ment),   -   ,   -

[4].   ,
.

,   -   [7], [8]
,   LUT-   .

.   -

,   -

,   -
-    .   -

-   -
-                                    LUT-   .

,   LUT-   **LUT-**
(LUT-   .   -
).   -

,   ,   FPGA (Field Pro-   ,
grammable Gate Array) [5],   ,   ,
,   -

.   -   LUT-   .

-
LUT (Look Up Table –   ),   -   -
-                    -   -   (   )
,   -   [9], [10]   -

,
[6].   LUT   FPGA   [7], [8]   -
-                    LUT-   .

.   LUT   LUT-   -
.   ,   -
, $n,$ LUT   ,   [7].
2^n $[7].$
$n-$ [9], [10]   -
.   _   -

-   -
-                                    : Flipping- $F()$ -
- $f().$
(,   -

)   -   -
.   -   -

,   -   ,   -
.

(,   -
)   -   -
.   ,

,   .   Flipping-

-   -
-   ,   -
.   -   .   -
-
-   -
,   -

LUT- , - , R- .
: - -
– , - -
- S- (-
). . 1, , -
, - S-
(LUT); - -
– - R- . . 1,
Flipping- F(x), , U- (-
, -) -
LUT - U- .
, [7], [8]. -
, -

LUT -

LUT, -

. ,

Flipping- -

$F(F(\mathrm{LUT}_i)) = \mathrm{LUT}_i$, LUT$_i$ -

LUT; -

– ,

, -

LUT$_R$	LUT$_S$		LUT$_S$	LUT$_R$
0	1		0	1
0	1		0	1
0	1		1	0
0	1		1	0
0	1		1	0
0	1		1	0
0	1	F	1	0
0	1	$\Rightarrow$	1	0
0	1		1	0
0	1		1	0
0	1		0	1
0	1		1	0
0	1		1	0
0	1		0	1
0	1		1	0
1	0		1	0

LUT
: LUT -
, -

,
(R-);
, , -
(S-);

LUT -
, -
(U-).
, -
:

LUT$_U$	LUT$_U$
0	1
0	1
0	1
0	1
0	1
0	1
0	1
0	1
1	0
1	0
1	0
1	0
1	0
1	0
1	0
1	0

$$F(\mathrm{LUT}_R) = \mathrm{LUT}_S;$$
$$F(\mathrm{LUT}_S) = \mathrm{LUT}_R; \quad (1)$$
$$F(\mathrm{LUT}_U) = \mathrm{LUT}_U,$$

LUT$_R$, LUT$_S$, LUT$_U$ – LUT, -
R- , S- U- -
; F() – Flipping- .
. 1
Flipping- F() LUT. -
(. 1,)

. 1.

LUT

LUT-
.

1.
LUT   ,   -
.

LUT   *R-*   ,
, *S-*   *U-*

RS-   :   -
LUT
R-   ,   *RS-*   -
0;
S-   ,   *RS-*
1;   *U-*   *RS-*
.
2.
RS-

RS_{com}.   -
,   *RS_{com}*
RS.
L.
3.   *RS_{com}*
,

L.
RS* -
RS
.

$$RS* = RS_{com}.DWM.Add,   (2)$$

«.» –   ;
DWM –
Add –   *RS**
RS.
4.
LUT   ,   -
.   *U-*
,   *R-*   *S-*
Flipping-
.

1.   LUT

- LUT_i	- *RS**	
R	0	—
R	1	LUT*i* *S-*
S	0	LUT*i* *R-*
S	1	–

,   Flipping-
LUT   -
-
[7], [8],   -
LUT-   -
-
.   -

:
key = (order, classification, RSrule,   L), (3)
order –   ,   -
LUT   (-
)
;
classification –
LUT (
);
RSrule –   -
RS, RS_{com}, RS*:   *R-*
RS-   0,
S-   – 1,   ;
L –   *RS*
RS_{com}.
-
-
LUT-
.
1.
LUT   ,   -
.   ,
,
LUT,   *RS'.*
2.   *RS** (2),
RS'   -
L   *RS'*
-
.

.
3.
,   -
,
.   -
RS_{decom}.
4.   ,   -
RS_{decom},

- 1,2% 65% (-
,) FPGA.
. .
LUT , -
, -
RS_{decom}. :
U- , *R-* 1)
S- (, , -
Flipping- . 1.) ,
- ;
. 2) -
: ;
1) , LUT- 3)
, - , ;
, 4) -
; ;
2) 5) .
- -
. . -
:) - 40 -
, - -
, -
;) , -
- . , -
;) - , -
;) . , -
. , -
- -
- , -
FPGA Altera Cyclone II Altera ( ) -
Quartus II. TCL . -
, - -
Altera Quartus II - .
LUT. -
- -
, - -
, . -
C# .Net. - , 1,2 % -
- 65 %
Altera FPGA, -
Quartus II Timing Analyzer (- . (-
) Power Play (40) -
). - 0,18 %, -
- -
- – 0,22 %. -

. .
- .
-
40 FPGA- -
. LUT-
.

-
-
.   -
                                                          LUT-   [7]   [8],
                        LUT-
                                                          -
,   .
                                                          -
                ,   -

                        ,   :
        –   Flipping-
                ,   -
        ;
                                                          -

        –
                                          ;
                                                          -
        –

(LUT),   -
        .

,   ,   -
                                        ,   -
                        ,   -
                        LUT-   ,
        .   -

,   -
                        .   -

                ,   -

                        ,   -
                ,   -
        LUT-   -
(, FPGA   -
).

                                :   FPGA
,   FPGA,   -
        .

                                                          -
                        LUT-   .

1. Cox I., Miller M., Bloom J., and Fridrich J. (2008), Digital Watermarking and Steganography, *Burlington: Morgan Kaufmann Publishers,* 592 p.

2.   . .   -
                [   ]/ . .   , . .   -
        . – .:   -   , 2006. – 288 .

3.   . .   ,
[   ]/ . .   , . .   ,
        . .   . – .:   , 2009.
– 220 .

4. Shih F., (2012), Watermarking, Steganography, and Forensics, New York, *CRC Press,* 424 p.

5.   . .   -

                                [   ] / . .   , . .
        .   ,   . .   . –   .:   ,
2010. – 650   .

6. Paul S., Bhunia S., (2008), Reconfigurable Computing Using Content Addressable Memory for Improved Performance and Resource Usage, *Proceedings of Design Automation Conference ACM/IEEE (DAC-2008),* Anaheim,   . 786 – 791.

7.   . .   -
                                        LUT-
                                [   ] / . .   -
        ,   . .   //   -
                                        . –   . : 2013. –
12 (88). –   . 83 – 90.

8.   . .   -
                                                          LUT-

[   ] / . .   , . .   //
                                                          -
        . –   . : 2014. –   13 (89). –   . 231 – 239.

9. Fridrich J., Goljan M., and Du R., (2002), Lossless Data Embedding – New Paradigm in Digital Watermarking, *Journal on Applied Signal Processing: Emerging Applications of Multimedia Data Hiding,* USA, New York, *Hindawi Publishing,* pp. 185 – 196.

10. Goljan M., Fridrich J., and Du R. (2001), Distortion-Free Data Embedding for Images, *Proceedings of the 4th International Workshop on Information Hiding (IHW-01)*, USA, *Pittsburg,* p. 27 – 41.

25.1.2014

References

1. Cox I., Miller M., Bloom J., and Fridrich J., (2008), Digital Watermarking and Steganography, Burlington, *Morgan Kaufmann Publishers*, 592 p. (In English), doi: 10.1016/b978-012372585-1.50015-2.

2. Konahovich G.F., and Puzirenko A.U., (2006), Kompyuternaya steganografiya [Computer Steganography], Kiev, Ukraine, *-Press Publ.*, 288 p. (In Russian).

3. Agranovsky A.V., Balkin A.V., and Gribunyn V.G., (2009), Steganografiya, tsifrovye vodyanye znaki i stegoanaliz [Steganography, Digital Watermarks and Stegoanalysis], Moscow, Russian Federation: *University Book Publ.*, 220 p. (In Russian).

4. Shih F. (2012), Watermarking, Steganography, and Forensics, New York, *CRC Press Publ.*, 424 p. (In English), doi: 10.1201/b12697-6.

5. Grushvitsky R.I., Mursaev A.H. and Ugryumov E.P. (2010), Proektirovanie sistem na mikroskhemakh s programmiruemoi strukturoi [Design of Systems on a Chip with Programmable Structure], St. Petersburg, Russian Federation, *BHV Publ.*, 650 p. (in Russian).

6. Paul S., and Bhunia S., (2008), Reconfigurable Computing Using Content Addressable Memory for Improved Performance and Resource Usage, *Proceedings of Design Automation Conference ACM/IEEE (DAC-2008),* Anaheim, . 786–791, (in English), doi: 10.1145/1391469.1391670.

7. Zashcholkin K.V. and Inanova E.N., (2013), Metod steganograficheskogo skrytiya dannykh v LUT-orientirovannykh apparatnykh konteinerakh [Method of Steganographical Hiding of Information in LUT-oriented Hardware Containers], *Electrotechnic and Computer Systems*, Kiev, Ukraine, No. 12 (88), pp. 83 – 90 (In Russian).

8. Zashcholkin K.V. and Inanova E.N., (2014), Razvitie metoda steganograficheskogo skrytiya dannykh v LUT-orientirovannykh apparatnykh konteinerakh [Method Development for Implementing the Steganography Data Hiding in LUT-oriented Hardware Containers], *Electrotechnic and Computer Systems*, Kiev, Ukraine, No. 13 (89), pp. 231 – 239 (In Russian), doi: 10.15276/etks.13.89.2014.33.

9. Fridrich J., Goljan M. and Du R., (2002), Lossless Data Embedding – New Paradigm in Digital Watermarking, *Journal on Applied Signal Processing: Emerging Applications of Multimedia Data Hiding*, USA, New York: *Hindawi Publishing,* pp. 185 – 196 (in English), doi: 10.1155/s1110865702000537.

10. Goljan M., Fridrich J., and Du R., (2001), Distortion-Free Data Embedding for Images, *Proceedings of the 4th International Workshop on Information Hiding (IHW-01)*, USA, Pittsburg, pp. 27 – 41 (in English), doi: 10.1007/3-540-45496-9_3.

,

.   .   ,   .   .

-

.   -

.   - ,
.: (048) 734-83-22,
e-mail: const-z@te.net.ua

,

.   .

.   -

.   - ,
.: (048) 734-83-91,
e-mail: enivanova@ukr.net