Weighted Digital Watermarking Approaches Comparison

Natalia Voloshina, Sergey Bezzateev, Konstantin Zhidanov
Department of Information Security Technologies, Saint Petersburg State University of Aerospace Instrumentation
Saint Petersburg, Russia
natali@vu.spb.ru, bsv@aanet.ru, konstantin.zhidanov@gmail.com

***Abstract*—The comparison of efficiency of two such approaches LEBC embedding method and Weighted F5 embedding that are used for weighted structures of container and F5 method that is used for least significant bit(LSB) embedding is made. The comparison metric was found for correct comparison of weighted and unweighted syndrome coding embedding. As a result the efficiency of weighted approach is shown on the example.**

I. Introduction

One of the most popular digital right management method for different applications such as multimedia data protection or DNA protection based on digital watermarking (DWM) approach [1], [2], [3], [4], [5]. One of the most effective approaches for DWM is invisible embedding based on syndrome coding algorithms such as $F5$ [1] that use perfect error correcting codes . Syndrome based embedding based on Hamming code can be expanded from the LSB container model to weighted container model approach [2], [6] that take into account the weighted significance structure of initial container. As a result the more efficient embedding methods could be found. In this paper the comparison of efficiency of two such approaches linear error-block codes(LEBC) embedding method (π-metric) [3] and weighted $F5$ embedding (WH-metric) [2], [5], [6] that are used for weighted structures of container and $F5$ method (H-metric) that is used for LSB embedding is made. The comparison metric was found for correct comparison of weighted and unweighed syndrome coding embedding.

II. Syndrome embedding

For syndrome embedding it is necessary to define error-correcting codes(ECC) for with such parameters as syndrome length and codeword length could be driven [1], [2], [3], [4], [5].

$$\boldsymbol{S} = \boldsymbol{e} \times \boldsymbol{H}^T, \tag{1}$$

where $\boldsymbol{S} = (S_1, S_2, \ldots, S_s)$ is a syndrome vector of the length s, $\boldsymbol{e}$ is an error vector of the length n and $\boldsymbol{H}$ is a $r \times n$ parity-check matrix of the error-correcting code with the length n and redundancy r.
The message $\boldsymbol{m}$ is looked at as a set of syndrome vectors:

$$\boldsymbol{m} = (\boldsymbol{S}^{(1)}, \boldsymbol{S}^{(2)}, \ldots, \boldsymbol{S}^{(\eta)}).$$

The container $\boldsymbol{C}$ is looked at as a set of η vectors of the length n :

$$\boldsymbol{C} = (\boldsymbol{c}^{(1)}, \boldsymbol{c}^{(2)}, \ldots, \boldsymbol{c}^{(\eta)}).$$

To embed message it is necessary to change the initial value of container vectors $\boldsymbol{c}^{(i)}, i = 1, \ldots, \eta$ to container vectors with information $\boldsymbol{e}^{(i)}, i = 1, \ldots, \eta$ in a way to get the set of the syndrome values $(\boldsymbol{S}^{(1)}, \boldsymbol{S}^{(2)}, \ldots, \boldsymbol{S}^{(\eta)})$ that are correspond to the value of the message $\boldsymbol{m}$ [1] in accordance with equation (1):

$$\boldsymbol{S}^{(i)} = \boldsymbol{e}^{(i)} \times \boldsymbol{H}^T.$$

In general case the distortion vector $\boldsymbol{\tau}^{(i)}$ is $\boldsymbol{\tau}^{(i)} = \boldsymbol{e}^{(i)} - \boldsymbol{c}^{(i)}$ and in binary case $\boldsymbol{\tau}^{(i)} = \boldsymbol{e}^{(i)} \oplus \boldsymbol{c}^{(i)}$. Since the number of distortion t is equal to Hamming weight of the vector $\boldsymbol{\tau}$:

$$t = wt_H(\boldsymbol{\tau}).$$

To estimate the distortion that performs for weighted container while embedding the penalty function [2] can be used

$$P = \sum_{i=1}^{\ell} t_i p_i, \tag{2}$$

where t_i- average number of distortions in zone I_i of weighted container, p_i - significance (penalty) of the zone I_i , ℓ- overall zones number.

III. Error-correcting codes for weighted structure

Linear error-block codes based on special partition π of the codeword length. This partition is defined as a composition of blocks $v_1, v_2, \ldots, v_\ell$ with lengths $n_1, n_2, \ldots, n_\ell$, $(n_1 \geq n_2 \geq \ldots \geq n_\ell)$ [7]. For these codes so-called $\pi-$ distance is used.

$$d_\pi(\mathbf{u}, \mathbf{v}) = \sharp\{i : 1 \leq i \leq \ell, u_i \neq v_i\}.$$

In [7], [8] it is shown that there exist a perfect LEBC codes of minimal distance $3, 4$ and 5.
To define the error-correcting codes in weighted Hamming metric let us associate with each block v_i its unique weight $w_i \in \mathbf{Z}, w_1 < w_2 < \ldots < w_\ell$. Then the distance $d_{WH}(\mathbf{u}, \mathbf{v})$ between two vectors $\mathbf{u} = (u_1, u_2, \ldots, u_\ell)$ and $\mathbf{v} = (v_1, v_2, \ldots, v_\ell)$ in weighted Hamming metric defined as follows:

$$d_{WH}(\mathbf{u}, \mathbf{v}) = \sum_{i=1}^{\ell} d(u_i, v_i) w_i, \tag{3}$$

where $d(\mathbf{u}, \mathbf{v})$ - the distance between two vectors $\mathbf{u}$ and $\mathbf{v}$ in classical Hamming metric. In [9] the construction and parameters of error correcting codes perfect in such weighted Hamming metric obtained from Goppa codes is described.

978-1-5090-4231-9/16/$31.00 ©2016 IEEE

IV. Comparison examples

LEBC code parameters are $n = 7(n_1 = 3, n_2 = 2, n_3 = 1, n_4 = 1), s = 4$ [3]. Weighted Hamming code parameters are $n = 9(n_1 = 3, n_2 = 3, n_3 = 3), s = 5$ [5]. Hamming code parameters are $n = 7, s = 3$. To compare these three approaches let's assume message length $\mu = 60$ bit. The length of container is equal to $\frac{\mu \times n}{s}$. To perform a comparison let's use coefficients of efficiency as for number embedding messages per container K_m as for penalty function values K_P .

$$K_m = \frac{N_{WM}}{N_{UWM}},\ K_P = \frac{P_{WM}}{P_{UWM}},$$

where N_{WM}, N_{UWM} - number of embedded syndromes and P_{WM}, P_{UWM} - average penalty function for all message for weighted and unweighted approaches consequently.

The values of P_{WM}, P_{UWM} could be calculated from the tables of coset leaders for parity check matrix of selected codes.

To estimate the distortions that could occur while information embedding process (syndrome coding) we use penalty function P (2). Penalty for errors that occur in i- th bit plane is defined as p_i. In simplest case penalties could be defined as $p_i = i$ where i is the number of bit plain when $i = 1$ for the least significant bit plain. For the partition $[3][2][1][1]$ that was defined in [3] the error vectors was found. The parameters of this code are represented in Table I.

TABLE I
Coset leaders, syndromes and corresponding penalties defined for partition $[3][2][1][1]$ for LEBC embedding.

Coset leader				Syndrome
000	00	0	0	0000
100	00	0	0	1011
010	00	0	0	1100
001	00	0	0	1101
101	00	0	0	0110
110	00	0	0	0111
011	00	0	0	0001
111	00	0	0	1010
000	01	0	0	0100
000	11	0	0	0010
000	00	1	0	0011
000	00	0	1	1000
100	01	0	0	1111
001	01	0	0	1001
011	01	0	0	0101
111	01	0	0	1110
Number of distortions for bitplanes				
19		7	1	1

This example shows how to use MLSB weighted embedding in case when it is impossible to get or send pixel levels matrix of the image. In this case it is possible to use such weighted structure:

- for the first block with length $n_1 = 3$ we define weight $w_1 = 1$,
- for the second block $n_2 = 3$ we define weight $w_2 = 4$ and
- for the third block $n_3 = 3$ we define weight $w_3 = 6$.

The total length of the codeword is $n = n_1 + n_2 + n_3 = 3 + 3 + 3 = 9$. For this partition $[3][3][3]$ it is possible to construct ECC in weighted Hamming metric so that syndrome length is equal to 5. The coset leaders and their weights for this code are represented in Table II. For our multi-level significance bit approach the weighted container model [6] could be defined in accordance to the structure $[3][2][1][1]$. To construct similar structure for weighted information embedding it is necessary to define weights of corresponding blocks [9]. For the first block with length n_1 we define weight $w_1 = 2$, for the second block with length n_2 we define weight $w_2 = 3$ and for the third block with length n_3 we define weight $w_3 = 5$. The total length of the codeword $n = n_1 + n_2 + n_3 = 3 + 2 + 1 = 6$. The syndrome length is equal to 4. For all error vectors the following inequality is valid.

TABLE II
Coset leaders and their weights in the weighted Hamming metric and corresponding penalties defined for partition $[3][3][3]$.

Coset leader		
000	000	000
100	000	000
010	000	000
001	000	000
110	000	000
101	000	000
011	000	000
111	000	000
000	100	000
000	010	000
000	001	000
100	100	000
010	100	000
001	100	000
100	010	000
010	010	000
001	010	000
100	001	000
010	001	000
001	001	000
110	100	000
011	100	000
101	100	000
110	010	000
011	010	000
101	010	000
110	001	000
011	001	000
101	001	000
000	000	100
000	000	010
000	000	001
Number of distortions for bitplanes		
39	21	3

$$\tau_1 w_1 + \tau_2 w_2 + \tau_3 w_3 \leq 5$$

The coset leaders and their syndromes for this code are represented in Table III.

978-1-5090-4231-9/16/$31.00 ©2016 IEEE

TABLE III
COSET LEADERS, THEIR SYNDROMES AND WEIGHTS IN THE WEIGHTED HAMMING METRIC AND CORRESPONDING PENALTIES DEFINED FOR PARTITION [3][2][1].

Coset leader	Syndrome
000 00 0	0000
100 00 0	0001
010 00 0	0010
001 00 0	0100
101 00 0	0101
110 00 0	0011
011 00 0	0110
000 01 0	1111
100 01 0	1110
001 01 0	1011
010 01 0	1101
000 10 0	1000
100 10 0	1001
001 10 0	1100
010 10 0	1010
000 00 1	0111
Number of distortions for bitplanes	
15 8 1	

TABLE IV
COMPARISON EXAMPLE FOR FOUR TYPES OF PENALTY DISTRIBUTION

Embedding method (structure)	K_m	Penalty distribution $\{1,1,1,1\}$		Penalty distribution $\{1,2,3,4\}$	
		P	K_P	P	K_P
LEBC (3211)	1.33	840	1.5	1200	0.86
WF5 (321)	1.33	576	1.03	816	0.58
WF5 (333)	1.66	756	1.35	1080	0.77
F5 (331)	1	560	1	1392	1

Embedding method (structure)	Penalty distribution $\{1,2,4,8\}$		Penalty distribution $\{1,4,8,16\}$	
	P	K_P	P	K_P
LEBC (3211)	1350	0.95	2130	1.12
WF5 (321)	840	0.59	1320	0.69
WF5 (333)	1116	0.79	1764	0.93
F5 (331)	1416	1	1896	1

Embedding method (structure)	Penalty distribution $\{1,4,16,32\}$	
	P	K_P
LEBC (3211)	2850	1.36
WF5 (321)	1512	0.72
WF5 (333)	2052	0.98
F5 (331)	2088	1

where penalty distribution$\{p_1, p_2, p_3, p_4\}$ array is a set of significance values for difference container zones.

V. CONCLUSION

In this paper we present the comparison of effectiveness of three classes of perfect codes (in common Hamming metric, in π- metric and in weighted Hamming metric) in steganography approach. It is shown that in case when we have zones with different significance value perfect codes in weighted Hamming metric give us better results in both penalty function and container efficiency.

ACKNOWLEDGMENT

This work was partly financially supported by the Russian Ministry of Education and Science within a framework of the basic task to the university in 2014 (project number 2452).

REFERENCES

[1] A. Westfeld , "A steganographic algorithm", *Proceedings of the 4th International Workshop on Information Hiding*, 2001, pp. 289-302.
[2] S. Bezzateev, N. Voloshina , K. Zhidanov , "Steganographic method on weighted container", *Problems of Redundancy in Information and Control Systems (RED), 2012 XIII International Symposium*, 2012, pp. 10 - 12.
[3] R. Darit, E.M. Souidi, "An Application of Linear Error Block Codes in Steganography" , *International Journal of Digital Information and Wireless Communications (IJDIWC)*, 1(2), 2011, pp. 426-433.
[4] D.Heider and A. Barnekow, "DNA Watermarking: Challenging Perspectives for Biotechnological Applications", *Current Bioinformatics*, 6, , 2011, pp.375-382.
[5] S.Bezzateev, N. Voloshina, K. Zhidanov, "Multi-level Significant Bit (MLSB) Embedding Based on Weighted Container Model and Weighted F5 Concept", *Advances in Intelligent Systems and Computing*, 427, 2016, pp. 293-303.
[6] N. Voloshina, K. Zhidanov, S. Bezzateev , "Optimal weighted watermarking for still images", *Proc. of XIV Int. Symposium on Problems of Redundancy in Information and Control System , Saint-Petersburg, Russia*, 2014, pp. 98-102
[7] K.Feng, L. Xu, F. Hickernell, " Linear error-block codes", *Finite Fields Appl.*, (6), 2006, pp.638-652.
[8] R. Darit, E.M. Souidi," New families of perfect linear error-block codes" *International Journal of Information and Coding Theory (IJICOT)*, 2(2/3), 2013, 84-95.
[9] S. Bezzateev, N. Shekhunova, "Class of generalized Goppa codes perfect in weighted Hamming metric", *Designs, Codes and Cryptography*, 66(1-3),2013, pp. 391-399.

978-1-5090-4231-9/16/$31.00 ©2016 IEEE