IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received August 30, 2017, accepted September 13, 2017, date of publication September 20, 2017, date of current version March 9, 2018.

Digital Object Identifier 10.1109/ACCESS.2017.2754638

Enhanced Blind Interleaver Parameters Estimation Algorithm for Noisy Environment

CHANGRYOUL CHOI AND DONGWEON YOON, (Member, IEEE)
Department of Electronics and Computer Engineering, Hanyang University, Seoul 04763, South Korea

Corresponding author: Dongweon Yoon (dwyoon@hanyang.ac.kr)

This work was supported by the research fund of Signal Intelligence Research Center supervised by Defense Acquisition Program administration and Agency for Defense Development of Korea.

ABSTRACT This paper proposes a blind interleaver parameters estimation method enhanced by identifying relatively error-less partial symbols among intercepted streams. By exploiting the distribution of the ranks of the random matrices, we can choose partial symbols having relatively small errors. Calculating the rank of the matrix constructed using these symbols can improve estimation of the blind interleaver parameters. Experimental results show that the proposed algorithm performs better than the previous ones.

INDEX TERMS Blind detection, cognitive radio, interleaver.

I. INTRODUCTION

Error-control codes (ECC) are indispensable for reliable transmission under the channel impairments by introducing some redundant data. Many ECCs are designed to be robust to the uniformly distributed random errors, but they are vulnerable to burst errors. To handle these burst errors, we introduce an interleaver that mingles the symbols from several codewords so that the symbols from any given codeword are well separated during transmission. In this case, the receiver has to synchronize the data and deinterleave them before a channel decoder can start to correct some errors [1].

In a non-cooperative context, an eavesdropper seeks information without any knowledge of the parameters used during communication. For a perfect recovery of information, one of the essential steps is blind estimation of the interleaver parameters using only the intercepted sequences. Some algorithms exploiting the linearity of ECCs are proposed in the literature [2]–[11]. To the best of our knowledge, there are two fundamental approaches that tackle this problem. The first approach is to exploit the properties of the dual codes [2]–[4]. By finding a basis of a dual code by using the parity check relations, interleaver parameters can be blindly estimated. The second approach uses linear algebra theory [5], [8]–[11]. By using the linear dependence within a codeword, the interleaver parameters can be calculated. Sicot et al. used both of the approaches and showed very good results using both approaches [6]. For non-binary ECC, Zrelli et al. also proposed an identification algorithm of codeword length for non-binary ECC using both approaches [7].

In this paper, we propose an enhanced blind interleaver parameter estimation algorithm by identifying relatively error-less partial symbols. First we propose a new approach in blind estimation of interleaver parameters using the linear dependence among the codewords. Note that almost all the algorithms proposed in the literature use the property of linearity within a codeword. Second, we propose a method of identifying the partial symbols having relatively small errors by exploiting the distribution of the ranks of the square random matrices. Third, since the proposed algorithm uses only the square matrices using the partial intercepted symbols, the proposed algorithm does not suffer from the error propagation which can happen to the typical Gaussian elimination. Finally, by constructing a rectangular matrix using these partial symbols with relatively small errors, we can calculate the interleaver parameters considering the theoretical false positive rate.

The rest of this paper is organized as follows. Section II gives a review of the previous algorithms. In Section III, we explain our proposed algorithm. Simulation results and analyses are in Section IV, and we conclude in Section V.

II. PREVIOUS WORKS

A. SYSTEM MODEL

Let C be an (n, k) linear code over $GF(q)$, where n is the codeword length, k is the code dimension, and $GF(q)$ represents the Galois field of order q. By linearity, we can represent any codeword $\mathbf{c} \in C$ as follows:

$$\mathbf{c} = \mathbf{m}G \tag{1}$$

where $\mathbf{c}$ is a $1 \times n$ row vector, $\mathbf{m}$ is a $1 \times k$ row vector, and G is a $k \times n$ matrix having full rank.

Generally, in almost all the communication systems, the interleaver size S is a multiple of the codeword size, i.e., $S = \beta n$, where β is the number of codewords within an interleaver. Let $\mathbf{t}$ be a concatenation of interleaved sequences and $\mathbf{z}$ be an intercepted sequence of length M. Since an eavesdropper has no *a priori* knowledge about the interleaver parameters, the first t_0 symbols may be missed. Without loss of generality, we assume that $0 \leq t_0 < S$. For convenience, we can define the translated sequence $\mathbf{z_d}$ as follows:

$$z_d(i) = t(i + t_0 + d) + e(i), \quad 0 \leq i < M - d \tag{2}$$

where $e(i)$ is a sequence of channel errors. We assume that the channel is a binary symmetric channel (BSC) with transition probability of P_e. Let l be a predicted interleaver period. Using $\mathbf{z_d}$, we construct an interception matrix $Z_{l,d}$ of size $D \times l$ (where $D = \lfloor \frac{M-d}{l} \rfloor$ and $\lfloor \bullet \rfloor$ represents the floor function). We pile up the received symbols from leftmost top to rightmost bottom in raster scanning order.

B. DUAL CODE APPROACH

Given an (n, k) linear code C over $GF(q)$, a dual code $C^{\perp}$ is defined as all the vectors $\mathbf{y}$ of length n satisfying the property

$$\mathbf{c}\mathbf{y}^T = 0, \quad \forall \mathbf{c} \in C \tag{3}$$

where T represents the transpose. Let $\mathbf{y}$ be a dual codeword; then we can identify the interleaver length by calculating the following values:

$$\mathbf{y}Z_{l,d}^T = \mathbf{u} \tag{4}$$

where $\mathbf{u}$ represents a $1 \times D$ matrix. Assume that $d + t_0 = S$ and $l = S$. When no errors occur, then the Hamming weight of $\mathbf{u}$ must be zero. When some errors occur, then the expected Hamming weight of $\mathbf{u}$ is $D \times P$ where P is given as

$$P = \frac{1 - (1 - 2P_e)^w}{2} \tag{5}$$

where w is the Hamming weight of the dual codeword $\mathbf{y}$ [2].

C. LINEAR DEPENDENCE WITHIN CODEWORDS

From (1), we can see that some code components can be expressed as a linear combination of other code components. Therefore, if a predicted interleaver period l is a multiple of S, we can identify this linear dependence within a codeword by calculating the rank of the matrix $Z_{l,d}$. This algorithm is very effective when no errors occur [5].

D. HYBRID APPROACH

An algorithm using Gauss-Jordan elimination through pivoting (GJETP) is proposed in [6]. This algorithm is an extension of the algorithms using the dual codes in that while performing Gaussian elimination it calculates the dual codewords simultaneously. This algorithm is also an extension of the algorithm using the linear dependence within codewords. When some errors occur, even a single dependent column might not exist. This algorithm, instead of finding dependent columns, tries to find almost-dependent columns. In this case, the Gaussian elimination algorithm is performed horizontally for $Z_{l,d}$ to calculate the dual codewords. Note that the rank of the matrix is the same as that of the transposed matrix. After GJETP, the Hamming weights of the independent columns act as a metric for identifying the interleaver period. Note that since the Gaussian elimination algorithm suffers from error propagation, they also proposed an iterative algorithm using the relatively error-less lines based on the sum of the log-likelihood ratios [6].

III. PROPOSED ALGORITHM

A. LINEAR DEPENDENCE AMONG CODEWORDS

All previous algorithms for the blind estimation of interleaver parameters exploit the linear dependence within codewords. Due to this, all the Gaussian elimination algorithms are performed in a horizontal direction. (If the codewords are aligned horizontally, the Gaussian elimination algorithm is performed vertically, and vice versa.) Besides this linear dependence within codewords, we can give a new perspective of linear dependence among codewords. Since an (n, k) linear code C over $GF(q)$ is a k-dimensional subspace in an n-dimensional vector space, there are k basis vectors in the n-dimensional vector space. Therefore, if there are $k + 1$ codewords, at least one of the codewords can be described by the linear combination of k basis vectors. This property of linear dependence among codewords can elucidate the rank behavior better than the property of linear dependence within codewords.

For example, consider a (7, 4) linear code C over $GF(q)$ and a 7×7 matrix of $(\mathbf{c}_1, \mathbf{c}_2, \mathbf{c}_3, \mathbf{c}_4, \mathbf{c}_5, \mathbf{c}_6, \mathbf{c}_7)^{\mathrm{T}}$ where $\mathbf{c}_{\mathrm{i}} \in C$. In this case, by the property of linear dependence within a codeword, the rank of this matrix is predicted as 4. In contrast, by the property of linear dependence among codewords, the maximum rank of this matrix is predicted as 4. Let us further assume two errors in $\mathbf{c}_1$ and we consider a 7×7 matrix as $(\mathbf{c}_1', \mathbf{c}_2, \mathbf{c}_3, \mathbf{c}_4, \mathbf{c}_5, \mathbf{c}_6, \mathbf{c}_7)^{\mathrm{T}}$. In this case, by the property of linear dependence within a codeword, the predicted rank of this matrix is 6, and by the property of linear dependence among codewords, the maximum rank of this matrix is predicted to be 5 (because at least 2 codewords among $\mathbf{c}_{\mathrm{i}}$'s ($i = 2, 3, 4, 5, 6, 7$) are linear combinations of other codewords and the corrupted codeword $\mathbf{c}_1'$ is linearly independent with the other codewords). Note that the actual maximum rank of this matrix is 5.

B. DISTRIBUTION OF THE RANKS OF THE RANDOM MATRICES

In general, we assume that the occurrence of codewords follows uniform distribution. Consequently, we can also assume that the occurrence of the symbols within codewords follows uniform distribution. When we construct an $l \times l$ square random matrix whose entries take the values in $GF(q)$ with equal probability, the probability P_r that the rank of this

TABLE 1. P_s for some different values of s.

s	P_s
0	0.288788
1	0.577576
2	0.128350
3	0.005238
4	4.65669×10^{-5}
5	9.69136×10^{-8}

matrix is r can be calculated as [12], [13]

$$P_r = q^{-l^2} \frac{\left[\prod_{i=0}^{r-1}(q^l - q^i)\right]\left[\prod_{i=0}^{r-1}(q^l - q^i)\right]}{\prod_{i=0}^{r-1}(q^r - q^i)}. \quad (6)$$

Note that, since the proposed algorithm exploits only the distribution of the ranks of the random matrices, we can also apply the proposed algorithm to the non-binary channel codes straightforwardly. From now on, we will consider only the binary channel codes.

For an efficient presentation of the proposed algorithm, we also introduce the probability P_s as the probability that the rank of the $l \times l$ square matrix is $l - s$ ($s \neq 0$) when $l \to \infty$. In [14], P_s is given by

$$P_s = 2^{-s^2}\left(\prod_{i=s+1}^{\infty}(1 - 2^{-i})\right)\left(\prod_{i=1}^{s}(1 - 2^{-i})^{-1}\right) \quad (7)$$

and when $s = 0$, P_0 is given by

$$P_0 = \prod_{i=1}^{\infty}(1 - 2^{-i}). \quad (8)$$

Table 1 shows the values of P_s for some different values of s. Note that as l increases, the calculated P_s rapidly converges to theoretical values. For example, when l is 8, all the differences between the calculated values of P_s and the theoretical values in Table 1 are within 0.41% (up to $s = 5$). From Table 1 we can see that an $l \times l$ square binary random matrix would very rarely have a rank as low as l–s ($s \geq 3$).

If we assume that an $l \times l$ square binary matrix A has a rank of l–s ($s \geq 3$), there are two possible explanations of this low rank. The first one is when the matrix A is purely random and its low rank is purely by chance. For example, if $s = 4$, this can happen once in 21,505 trials on average, which is very rare. Another possibility is that there are some structures in this matrix A. That is, we can presume that the matrix has l–s–m ($m \geq 1$) basis vectors and m distinct errors. If we plug such data into the blind interleaver parameters estimation algorithm, when $l = S$, low ranks can happen frequently. When $l \neq S$, the rank of matrix A follows the distribution in Table 1.

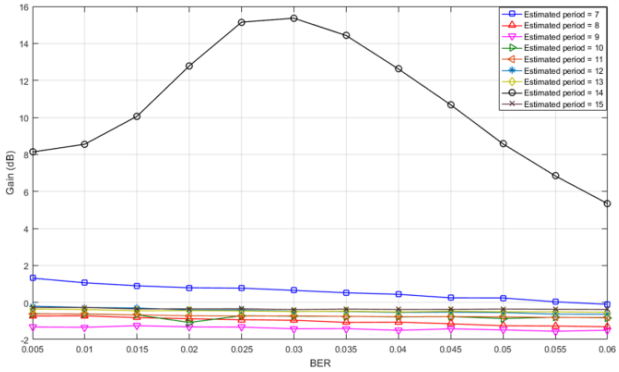

FIGURE 1. Gain of the BER compared with the actual BER. (7, 4) Hamming codes are used, interleaver period $S = 14$, and the number of received symbols $M = 50,000$.

C. IDENTIFICATION OF SYMBOLS HAVING SMALL ERRORS

Given an (n, k) binary linear code C and the interleaver of size $S = \beta n$, we can partition the intercepted and translated sequence $\mathbf{z_d}$ as a sequence of vectors of length l. Let these vectors be $\boldsymbol{w}_i(j)$ $(0 \leq i < D, 0 \leq j < l)$. As can be seen from Section III-B, when the rank of an $l \times l$ square matrix is less than l–s ($s \geq 2$), we can presume with high confidence that the rows of this matrix are drawn from some channel codes having some errors. Assume that $l = S$ and $d + t_0 = S$. If we randomly select l vectors of $\boldsymbol{w}_i(j)$ among D vectors, and all the vectors $\boldsymbol{w}_i(j)$ are distinct, the rank of a square matrix constructed from selected l vectors must be in the range $\beta k \leq rank \leq l$.

Therefore, if there are many errors in the matrix, we can assume that its rank is close to l; otherwise its rank is assumed to be far less than l. Using this result, we can identify vectors with small errors among D vectors. The identification algorithm of small errors is summarized as follows:

1) Randomly select l vectors wi(j) and construct a square matrix.
2) Calculate the rank of the matrix.
3) If the rank is l–s ($s \geq 3$), record indices of l vectors $\boldsymbol{w}_i(j)$.
4) Repeat steps 1) to 3) N times.
5) Find K most recorded indices of vectors $\boldsymbol{w}_i(j)$.

To check whether this algorithm can identify the vectors with small errors, we compare the actual bit error rate (BER) and the BER of the K vectors which are identified vectors as relatively small errors. Fig. 1 shows the results when we use (7, 4) Hamming codes and the interleaver period $S = 14$. In this case, the number of intercepted symbols is 50,000, $N = 1,000$, $K = 38$, and the gain is represented as follows:

$$Gain(dB) = 10\log\left(\frac{Actual\ BER}{BER\ of\ K\ vectors}\right). \quad (9)$$

We calculate the average gains over 10,000 iterations. From Fig. 1, we can see that when $l = S$, the proposed algorithm can find the vectors with small errors very effectively. To be specific, when the actual BER $= 3.00 \times 10^{-2}$ (the average

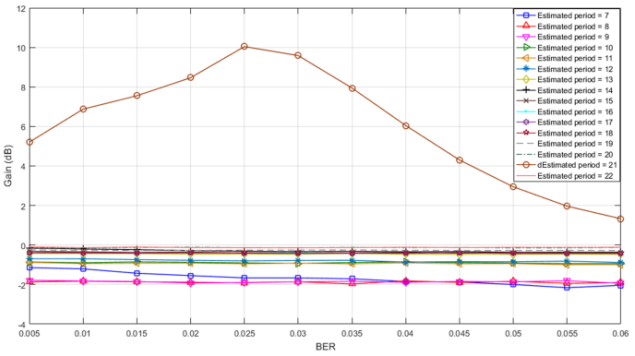

FIGURE 2. Gain of the BER compared with the actual BER. (7, 4) Hamming codes are used, interleaver period $S = 21$, and the number of received symbols $M = 50,000$.

number of errors in 100,000 bits is 3,000), the BER of the K vectors is 7.6×10^{-4} (the average number of errors in 100,000 bits is 76), having a gain of 15.36dB. As expected, when $l \neq S$, the gains fluctuate around 0dB. Fig. 2 depicts the results when we change the interleaver period from 14 to 21 and hold the other parameters the same as those of Fig. 1. Compared with Fig. 1, the gain is reduced slightly. We can increase gain by increasing s, say to 4 or 5. Note that, by varying the rank threshold of $l - s$, we can identify the vectors with relatively small errors for non-binary channel codes.

D. PROPOSED ALGORITHM CONSIDERING FALSE ALARM RATE

Given an $l \times (l + q)$ $(q > 0)$ binary rectangular random matrix, the probability of the matrix being rank deficient (the matrix having a non-full rank) P_R can be approximated as follows [15]:

$$P_R \approx 2^{-q}(1 - 2^{-l}). \tag{10}$$

Using this fact, we can control the false alarm rate of the algorithm of blind interleaver parameter estimation. That is, when we construct an $l \times (l + q)$ matrix, if its rank is less than l, we assume that the rows of this matrix are drawn from some channel codes with the false alarm probability of (10). The proposed algorithm can be summarized as in Fig. 3.

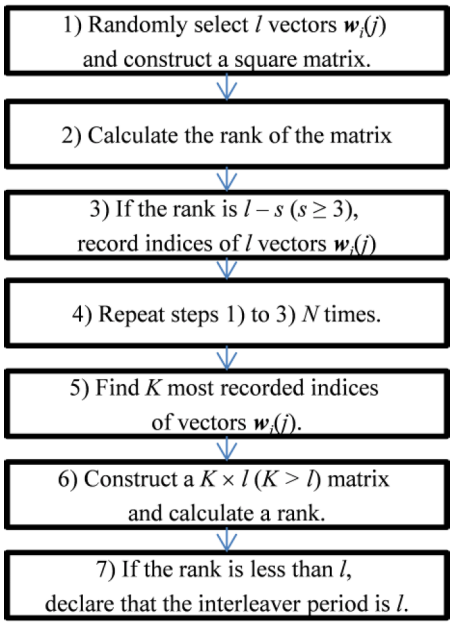

FIGURE 3. Generic block diagram for interleaver parameter estimation.

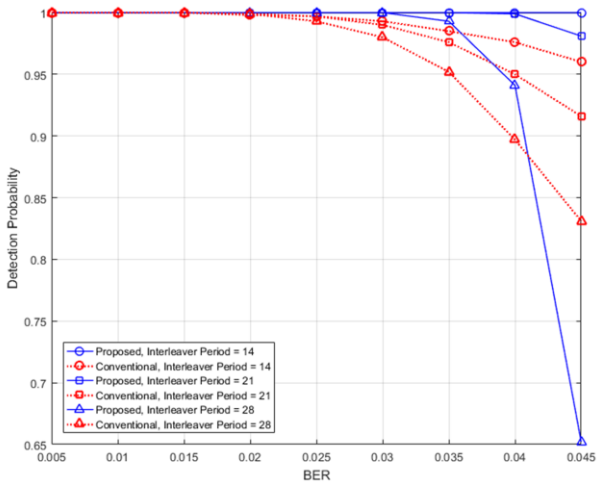

FIGURE 4. Detection probability when the number of intercepted symbols is 5,000, interleaver sizes are 14, 21, and 28, and (7, 4) Hamming codes are used.

IV. EXPERIMENTAL RESULTS

We carried out some experiments to validate the proposed algorithm. We depict the detection probabilities of the proposed algorithm in Figs. 4 and 5, including for comparison the results of the algorithm of [6] as conventional ones. In all the experiments in Figs. 4 and 5, we use (7, 4) binary Hamming code and the random interleaver of periods 14, 21, and 28. When the interleaver period is S, the search range of the interleaver period is set from 7 to $S + 1$ and the delay parameter is chosen randomly from 0 to $S - 1$. For an identification of small errors, we set $N = 1,000$ and $K = l + 24$ where l is the predicted interleaver period. Theoretically, the false positive rate of this value is about 5.96×10^{-8}.

Fig. 4 shows the simulation results when the number of intercepted symbols is 5,000: dotted lines stand for the algorithm of [6] and solid lines for the proposed algorithm. Fig. 4 shows that the proposed algorithm gives better results than the conventional one [6]. When the interleaver size is 28 and BER = 0.045, the performance of the proposed algorithm is slightly worse than that of [6]. However, the false positive rate of the proposed algorithm is about 7.41×10^{-5} and that of [6] is about 7.41×10^{-4}, which is almost 10 times higher than the proposed algorithm. Note that the detection probabilities of the conventional algorithm of [6] are hard to be strictly 1 even when BER is low. To be specific, when BER is 0.02, the detection probabilities of the conventional algorithm of [6] are 99.8% ($S = 14$), 99.9% ($S = 21$), and 98.9% ($S = 28$), respectively. And when BER is 0.03, the detection probabilities of the conventional algorithm of [6] are 99.7% ($S = 14$), 99.0% ($S = 21$), and 98.0% ($S = 28$), respectively.

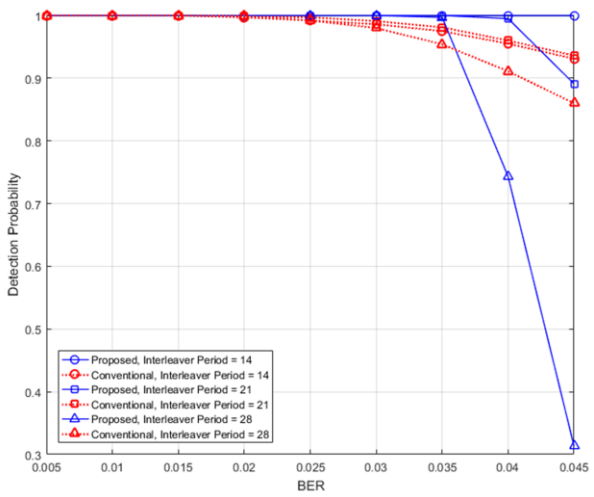

FIGURE 5. Detection probability when the number of intercepted symbols is 50,000, interleaver sizes are 14, 21, and 28, and (7, 4) Hamming codes are used.

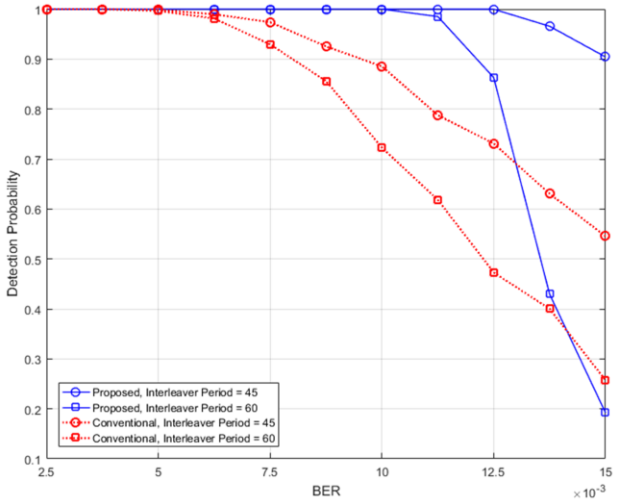

FIGURE 6. Detection probability when the number of intercepted symbols is 50,000, interleaver sizes are 45 and 60, and (15, 11) BCH codes are used.

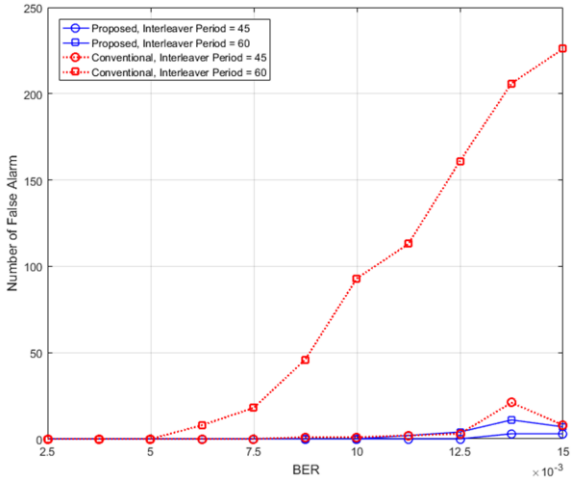

FIGURE 7. False alarm events out of 10,000 trials when the number of intercepted symbols is 50,000, interleaver sizes are 45 and 60, and (15, 11) BCH codes are used.

On the contrary, the detection probabilities of the proposed algorithm are 100% in that BER range. That is, the required BERs for a perfect detection for the conventional algorithm of [6] are all 0.015, however, those of the proposed algorithm are 0.045 ($S = 14$), 0.035 ($S = 21$), and 0.03 ($S = 28$), respectively.

Fig. 5 shows the results when the number of intercepted symbols is 50,000. In general, the results of the proposed algorithm outperform those of [6]. As BER increases, there are some points where the proposed algorithm performs slightly worse than that of [6]. In this case, the false positive rate of the proposed algorithm is about 1.85×10^{-4} and that of [6] is 1.13×10^{-2}, which is about 61 times higher than the proposed algorithm. We presume that the performance of [6] is heavily dependent upon the size of the intercepted symbols from the experiments. And the required BERs for a perfect detection for the conventional algorithm of [6] are 0.015 ($S = 14$), 0.02 ($S = 21$), and 0.015 ($S = 28$), respectively. However, those of the proposed algorithm is 0.045 ($S = 14$), 0.035 ($S = 14$), and 0.03 ($S = 14$), respectively.

To see the performance of the proposed algorithm for different ECCs with long interleaver sizes, we also performed simulations using (15, 11) BCH codes with interleaver sizes of 45 and 60. Figs. 6 and 7 show the experimental results. All the experimental setup is the same as in Figs. 4 and 5 except the channel codes used and the interleaver sizes. The number of intercepted symbols is 50,000.

Fig. 6 shows the detection probabilities of the proposed algorithm and the conventional algorithm. As can be seen from Fig. 6, the proposed algorithm outperforms the conventional algorithm. Note that since the code rate of (15, 11) BCH codes is much higher than (7, 4) Hamming codes, the detection probabilities of both algorithms start to decay at lower BERs than in Fig. 5. The required BER for a perfect detection for the proposed algorithm is 0.03 and that of the conventional algorithm is 0.015 when the interleaver size is 28 with (7, 4) Hamming codes. On the other hand, when the interleaver sizes are 45 and 60 with (15, 11) BCH codes, the required BERs for a perfect detection for the proposed algorithm are 0.0125 ($S = 45$) and 0.01 ($S = 60$) and those of the conventional algorithm are 0.0025 ($S = 45$ and 60).

Fig. 7 depicts the false alarm events in 10,000 trials; we see that the number of false alarm events of the proposed algorithm is extremely low. Here there is a maximum of 3 false alarm events with the proposed algorithm (when BER = 0.01375, $S = 45$) and 11 (when BER = 0.01375, $S = 60$). In contrast, the number of false alarm events of the conventional algorithm is very high. To be specific, the maximum false alarm events of the conventional algorithm are 21 (when BER = 0.01375, $S = 45$) and 226 (when BER = 0.01375, $S = 60$). We presume that this high number of false alarm events of the conventional algorithm is due to the short series

of intercepted symbols compared with the long interleaver size.

V. CONCLUSIONS

In this paper, we proposed an enhanced algorithm for blind estimation of interleaver parameters. The chief innovation of the proposed algorithm can be described as follows: First, we proposed a new approach of exploiting the linear dependence among the codewords, which can better describe the behavior of the ranks in the interception matrix. Second, we proposed a method of identifying the partial symbols having relatively small errors by exploiting the distribution of the ranks of the square random matrices. Third, by using only the square matrices constructed from the partial intercepted symbols, the proposed algorithm did not suffer from the error propagation which can happen to the typical Gaussian elimination. Finally, by constructing a rectangular matrix using these partial symbols having relatively small errors, we could calculate the interleaver parameters considering the theoretical false positive rate. For validation, we compared experimental results, where the proposed algorithm outperformed conventional ones.

REFERENCES

[1] S. B. Wicker, *Error Control Systems for Digital Communication and Storage*. Englewood Cliffs, NJ, USA: Prentice-Hall, 1995.

[2] A. Valembois, "Detection and recognition of a binary linear code," *Discrete Appl. Math.*, vol. 111, pp. 199–218, Jul. 2001.

[3] A. Canteaut and F. Chabaud, "A new algorithm for finding minimum-weight words in a linear code: Application to McEliece's cryptosystem and to narrow-sense BCH codes of length 511," *IEEE Trans. Inf. Theory*, vol. 44, no. 1, pp. 367–378, Jan. 1998.

[4] M. Cluzeau and M. Finiasz, "Recovering a code's length and synchronization from a noisy intercepted bitstream," in *Proc. ISIT*, Seoul, South Korea, Jun./Jul. 2009, pp. 2737–2741.

[5] G. Burel and R. Gautier, "Blind estimation of encoder and interleaver characteristics in a non cooperative context," in *Proc. IASTED*, Scottsdale, AZ, USA, Nov. 2003, pp. 275–280.

[6] G. Sicot, S. Houcke, and J. Barbier, "Blind detection of interleaver parameters," *Signal Process.*, vol. 89, pp. 450–462, Apr. 2009.

[7] Y. Zrelli, R. Gautier, E. Rannou, M. Marazin, and E. Radoi, "Blind identification of code word length for non-binary error-correcting codes in noisy transmission," *EURASIP J. Wireless Commun. Netw.*, vol. 2015, p. 43, Dec. 2015.

[8] S. Ramabadran, A. S. Madhukumar, N. W. Teck, and C. M. S. See, "Parameter estimation of convolutional and helical interleavers in a noisy environment," *IEEE Access*, vol. 5, pp. 6151–6167, 2017.

[9] R. Swaminathan, A. S. Madhukumar, W. T. Ng, and C. M. S. See, "Parameter estimation of block and helical scan interleavers in the presence of bit errors," *Digit. Signal Process.*, vol. 60, pp. 20–32, Jan. 2017.

[10] R. Swaminathan and A. S. Madhukumar, "Classification of error correcting codes and estimation of interleaver parameters in a noisy transmission environment," *IEEE Trans. Broadcast.*, vol. 63, no. 3, Sep. 2017.

[11] L. Lu, K. H. Li, and Y. L. Guan, "Blind detection of interleaver parameters for non-binary coded data streams," in *Proc. ICC*, Dresden, Germany, Jun. 2009, pp. 1–4.

[12] È. M. Gabidulin, "Theory of codes with maximum rank distance," *Problems Inf. Transmiss.*, vol. 21, no. 1, pp. 1–12, Jan. 1985.

[13] X. Li, "Rank analysis of sparse random matrices over finite fields with network coding applications," Ph.D. dissertation, Dept. Electron. Comput. Eng., Hong Kong Univ., Hong Kong, Aug. 2013.

[14] V. F. Kolchin, *Random Graphs*. New York, NY, USA: Cambridge Univ. Press, 1999.

[15] P. J. S. G. Ferreira, B. Jesus, J. Vieira, and A. J. Pinho, "The rank of random binary matrices and distributed storage applications," *IEEE Commun. Lett.*, vol. 17, no. 1, pp. 151–154, Jan. 2013.

CHANGRYOUL CHOI received the B.S. degree in radio science engineering and the M.S. and Ph.D. degrees in electronic communication engineering from Hanyang University, South Korea, in 1997, 1999 and 2010, respectively. He is currently a Research Professor with the Signal Intelligence Research Center, Hanyang University. His research interests include data hiding, video coding, and channel coding.

DONGWEON YOON received the B.S. *(summa cum laude)* degree, the M.S. and Ph.D. degrees in electronic communications engineering from Hanyang University, Seoul, South Korea, in 1989, 1992 and 1995, respectively. From 1995 to 1997, he was an Assistant Professor with the Department of Electronic and Information Engineering, Dongseo University, Pusan, South Korea. From 1997 to 2004, he was an Associate Professor with the Department of Information and Communications Engineering, Daejeon University, Daejeon, South Korea. Since 2004, he has been on the Faculty of Hanyang University, Seoul, South Korea, where he is currently a Professor with the Department of Electronic Engineering and the Director of Signal Intelligence Research Center. He has twice been an Invited Researcher with the Electronics and Telecommunications Research Institute, Daejeon, in 1997, 2002, and 2005. He was a Visiting Professor with the Pennsylvania State University, University Park, Pennsylvania, from 2001 to 2002, and with the University of California, Riverside, California, from 2010 to 2011. He was the Department Chair from 2011 to 2013. He is currently the Director of Signal Intelligence Research Center. His research interests include digital communications theory and system, satellite, and space communications, wireless communications, military communications, and signal intelligence.