Improved Method for Blind Interleaver Parameter Estimation Using Matrix Multiplication From Scant Data

YONGSEOK JUNG, MINGYU JANG, AND DONGWEON YOON, (Senior Member, IEEE)

Department of Electronic Engineering, Hanyang University, Seoul 04763, Korea

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

ABSTRACT

Estimation of interleaver parameter from scant received data has recently been researched. In this paper, we propose an improved algorithm for blind estimation of interleaver parameter using matrix multiplication under the condition of scant received data. First, we generate a matrix from the received data and make arbitrary square submatrices by randomly deleting rows and columns from the generated matrix. We then compose additional square matrices by multiplying the square submatrices, and examine the rank deficiencies of the additional square matrices. Finally, we blindly estimate the interleaver parameter based on the average rank deficiency of the additionally composed square matrices. Through computer simulations, we validate the proposed algorithm in terms of detection probability and the number of false alarms, and show that the proposed algorithm outperforms conventional ones.

INDEX TERMS

Blind detection, communication forensics, non-cooperative context, spectrum surveillance.

VOLUME 9, 2021 This work is licensed under a Creative Commons Attribution 4.0 License. For more information, see https://creativecommons.org/licenses/by/4.0/

I. INTRODUCTION

In non-cooperative contexts, such as spectrum surveillance and cognitive radio, a receiver has to recover information from the received data without prior knowledge about the communication parameters, because the receiver does not know the parameters used in the transmitter. Communication forensics, the identification of communication parameters by blind estimation, is therefore essential if the receiver is to recover the information from the received data in non-cooperative contexts. Interleaver parameter is an important communication parameter to be blindly estimated because interleavers are usually used to make communicated data more resilient to noise, fading, and interference in communication channels.

Much research on blind estimation of interleaver parameters has been conducted [1]–[13]. Reference [1] uses the rank of a matrix composed of received data to estimate block interleaver parameter for a noiseless channel, and [2] uses an “almost dependent column” of the matrix to extend the method of [1] to a noisy channel. Further, [3]–[8] estimate various types of interleavers including block, convolutional, helical, and helical scan interleavers, by analysis of the number of ones or zeros in each row (or column). Another strategy for blind estimation of interleaver parameter is using rank deficiencies of square matrices generated from the received data [9]–[11]. Reference [9] chooses vectors having fewer errors to compose square matrices, [10] compares the rank deficiency distribution of the generated square matrices to that of random binary matrices, and [11] presents an improved blind estimation method for more severe channel conditions.

While the methods in [1]–[11] assume a sufficient amount of received data for the blind estimation of interleaver parameter, [12] and [13] blindly estimate interleaver parameter from scant data where the methods in [1]–[11] become infeasible. To solve the problem of scant received data, [12] generates additional data by combining received data, and [13] makes square submatrices from a matrix composed of received data. We expect that estimation performance can be improved if we can compose additional square matrices from the square submatrices in [13].

In this paper, we propose an improved algorithm for blind estimation of interleaver parameter using matrix multiplication under the condition of scant received data. We call the data scant if there is not enough received data to generate a single square matrix for observing rank deficiency.
First, we generate a matrix from the received data and make arbitrary square submatrices by randomly erasing rows and columns from the generated matrix. Then, we compose additional square matrices by multiplying the square submatrices, and examine the rank deficiencies of the additional square matrices. Finally, we blindly estimate the interleaver parameter based on the average rank deficiency of the composed additional square matrices. We validate the proposed method in terms of detection probability and the number of false alarms through computer simulations. Simulation results show that the proposed method is superior to conventional ones, with scant received data. Moreover, under the condition of an even more limited amount of received data, the proposed method can estimate the interleaver parameter while the conventional ones cannot yield a meaningful result.

This paper is organized as follows. Section II introduces the system model and briefly explains the previous methods for blind estimation of interleaver parameter under the condition of scant data. Section III proposes an improved method by using matrix multiplication. Section IV presents simulation results and Section V concludes the work.

II. SYSTEM MODEL

Let us assume that the transmitter uses an \((n_c, k_c)\) linear block code and a random interleaver having an interleaving period of \(L\), where \(n_c\) is codeword length, \(k_c\) is the length of message bits in a codeword, and \(L\) is a multiple of the codeword length \(n_c\). In a non-cooperative context, the \(M\)-bit received data sequence \(r\) can be partitioned into \(n\) row vectors of length \(\hat{L}\), where \(\hat{L}\) is a predicted interleaving period, \(n = \left\lceil \frac{M}{L} \right\rceil\), and \(\lfloor \cdot \rfloor\) is the floor function. The received data sequence \(r\) and the \(i\)-th row vector \(s_i\) can respectively be expressed as

\[
\begin{align*}
   r &= \{s_1, s_2, \ldots, s_n\} \\
   s_i &= \{c^1_i, c^2_i, \ldots, c^n_i\}, \quad i = 1, 2, \ldots, n
\end{align*}
\]

where \(c^j_i\) is the \(j\)-th bit of \(i\)-th row vector \(s_i\) and \(c^j_i \in \{0, 1\}\) for \(1 \leq i \leq n, 1 \leq j \leq \hat{L}\). If \(n > \hat{L}\), we can generate an \(L \times \hat{L}\) square matrix \(R\) by selecting \(L\) different row vectors from \(n\) row vectors and placing the selected row vectors row by row. Repeating this process generates \(n\) different square matrices \(R\)’s, where \(\lfloor x \rfloor_y\) is the binomial coefficient.

Now, we examine the rank deficiency of \(R\) for two cases: one is the case when \(L = \hat{L}\), the interleaving period matches exactly, and the other is when \(L \neq \hat{L}\), the interleaving period does not match. Here, the rank deficiency of \(R\) is the difference between the rank of \(R\) and the number of rows (or columns) in \(R\).

If the predicted interleaving period \(\hat{L}\) is different from the original interleaving period \(L\), the linearity in a codeword disappears. In this case, the rank deficiency distribution of \(R\)’s resembles that of random binary matrices. In contrast, if \(\hat{L}\) is equal to \(L\), the linearity in a codeword maintains and the rank deficiency distribution of \(R\)’s becomes different from that of random binary matrices. Using these properties, [9]–[11] estimate the interleaving period by comparing the rank deficiency distribution of \(R\)’s to that of random binary matrices.

However, under the condition of scant received data, not even a single \(L \times L\) square matrix \(R\) can be generated and the methods of [9]–[11] become infeasible: the condition of scant data is assumed that the number of received data bits is limited to \(M = \hat{L} \times L \times \alpha\) bits for \(0 < \alpha < 1\). This is because we need at least \(L \times L\)-bit received data to compose a single square matrix \(R\), and a large number of \(R\)’s are required in [9]–[11] to estimate the interleaver parameter. References [12] and [13] address this problem with methods for blind estimation of interleaver parameter requiring only a limited amount of received data. The method of [12] generates additional vectors by combining the row vectors \(s_i\)’s to estimate the interleaving period, and the method of [13] improves estimation performance by composing square submatrices from the matrix generated from scant received data.

If we can compose additional square matrices from the square submatrices obtained in [13], it is expected that there is room for improvement in estimation performance. In Section III, we present an improved method for blind estimation of the interleaving period, by using matrix multiplication of the square submatrices obtained in [13], under the condition of scant received data.

III. PROPOSED ALGORITHM

In this section, we propose an improved method for blind interleaver parameter estimation using matrix multiplication. We begin with the idea based on [13]. From the received data sequence \(r\), if we place the \(n\) row vectors row by row, we can generate an \(n \times \hat{L}\) matrix \(R_d\) as

\[
R_d = \begin{bmatrix}
   s_1 \\
   s_2 \\
   \vdots \\
   s_n
\end{bmatrix} = \begin{bmatrix}
   c^1_1 & c^1_2 & \cdots & c^n_1 \\
   c^2_1 & c^2_2 & \cdots & c^n_2 \\
   \vdots & \vdots & \ddots & \vdots \\
   c^1_L & c^2_L & \cdots & c^n_L
\end{bmatrix}.
\]

We can then construct different \(l \times l\) square submatrices \(R_j\)’s by randomly erasing rows and columns from the generated matrix \(R_d\), where \(l\) is the number of rows of the submatrix and an integer smaller than \(\min(n, \hat{L})\), and \(\min(x, y)\) is the minimum operation [13]. For a given \(l\), we can generate a total number of \(\binom{n}{l} \times \binom{\hat{L}}{l}\) different \(R_j\)’s. The method in [13] uses \(R_j\)’s to obtain rank deficiency distribution and estimate the interleaver parameter. As mentioned in Section II, if we can compose additional square matrices from \(R_j\)’s under the condition of scant received data, we expect improved estimation performance. To do this, we compose additional square matrices by multiplying \(R_j\)’s and observe their rank deficiencies.

Note that when we obtain a matrix \(Q\) by multiplying matrices \(S_1, S_2, \ldots, S_m\), the inherent linearity of the matrices \(S_1, S_2, \ldots, S_m\) are well known to remain in the matrix \(Q\), and the
rank of $Q$ follows the rank inequality [14]:

$$\text{Rank}(Q) \leq \min\{\text{Rank}(S_1), \text{Rank}(S_2), \ldots, \text{Rank}(S_m)\}. \quad (4)$$

Therefore, we can compose an additional square matrix $R_q$ by multiplying $k$ different $R_q$’s while maintaining their inherent linearities. If we select $k$ different $R_{\tilde{q}}$’s and multiply the selected $R_{\tilde{q}}$’s, then we can have $Y C_q$ additional square matrices $R_q$’s where $Y$ is the total number of different $R_q$’s which can be constructed from $R_d$. For example, if there are 2520 ($60 \times 60 \times 0.7$) bits of received data and the predicted interleaving period is 50, we can generate a $50 \times 50$ matrix $R_d$. In this case, when $l$ is $50(50 - 1)$, we can generate a total number of $50 C_1 \times 50 C_1 = 2500$ square submatrices $R_{\tilde{q}}$’s. Moreover, if we select 2 different $R_q$’s and multiply them, we can compose $2^{50} C_2 = 3123750$ additional square matrices $R_q$’s about $1.2495 \times 10^3$ times more matrices than $R_q$’s.

Now, we examine the rank deficiency of $R_q$ for two cases: one is the case when $\tilde{L} = L$, the interleaving period matches exactly, and the other is when $\tilde{L} \neq L$, the interleaving period does not match. When $\tilde{L} = L$, there is a linearity in a codeword in $R_q$ [13]. The linearity in a codeword remains in $R_q$ because $R_q$ is obtained by multiplying $R_q$’s. Therefore, rank deficiency of $R_q$ occurs because of the linearity in a codeword and the rank deficiency distribution of $R_q$’s differs from that of random binary matrices when $\tilde{L} = L$, as in [13]. On the other hand, when $\tilde{L} \neq L$, the linearity in a codeword is lost in $R_q$ [13], and therefore, the linearity is also lost in $R_q$. However, rank deficiency of $R_q$ is different from that of $R_q$ because of the rank inequality in (4) and the rank deficiency distribution of $R_q$’s becomes different from that of random binary matrices even when $\tilde{L} \neq L$, unlike [13]. Therefore, a different method from [13] is required to blindly estimate interleaver parameter.

In order to examine the rank deficiency distribution of $R_q$’s when $\tilde{L} \neq L$, we show the rank deficiency distribution of $R_q$’s by varying $k$ from 2 to 4 in Fig. 1, where we assume that the original interleaving period $L$ is 60, predicted interleaving period $\tilde{L}$ is 55, the number of scant received data is 3240 ($60 \times 60 \times 0.9$) bits, (15, 11) BCH code is used, and $l$ is min$(58, 55) - 1$. For comparison, we also show the rank deficiency distribution of random binary matrices in Fig. 1. From Fig. 1, we can see that the rank deficiency distribution of $R_q$’s is different from that of the random binary matrices even when $\tilde{L} \neq L$. Therefore, unlike the method in [13], we cannot estimate the interleaver parameter by comparing rank deficiency distributions. Although we began with the idea based on [13], we have to adopt a different method from [13] to estimate the interleaver parameter under the condition of scant data. Thus, instead of rank deficiency distribution of $R_q$’s, we adopt the average rank deficiency of $R_q$’s. We will now examine it in detail.

In order to examine the average rank deficiency of $R_q$’s we show the average rank deficiency of $R_q$’s by varying $L$ from 8 to 65 in Fig. 2, when the original interleaving period is 60, the number of scant received data is 3240 ($60 \times 60 \times 0.9$) bits, (15, 11) BCH code is used, $l$ is min$(n, \tilde{L}) - 1$, and $k$ is 2 for a noiseless channel. In Fig. 2, the average rank deficiency of $R_q$’s is obtained by averaging over rank deficiencies of 1000 $R_q$’s and we denote the average rank deficiency of $R_q$’s for a given $\tilde{L}$ as $m(\tilde{L})$. From Fig. 2, it can be seen that $m(\tilde{L})$ is largest when $\tilde{L} = L$, and $m(\tilde{L})$’s are all similar when $\tilde{L} \neq L$. Therefore, we can determine that $\tilde{L}$ is the original interleaving period $L$ when $m(\tilde{L})$ has the largest value as follows:

$$L = \arg \max_\tilde{L} m(\tilde{L}). \quad (5)$$

However, in a noisy channel, even if $\tilde{L} = L$, $m(\tilde{L})$ may not be the largest value. This is because the linearity in a codeword can be lost by error bits caused by noise. In this case, a false alarm will occur. Therefore, to control the false alarm occurrence, we use the gap between the largest value of $m(\tilde{L})$ and the second largest value of $m(\tilde{L})$. For this, we set the threshold as $\gamma$. Only when the gap between the largest value of $m(\tilde{L})$ and the second largest value of $m(\tilde{L})$ is greater than threshold $\gamma$, we declare that the interleaving period obtained by (5) is the original interleaving period $L$. Note that increasing the value of $\gamma$ decreases the number of false

**FIGURE 1.** Rank deficiencies of additional square matrices and random binary matrices.

**FIGURE 2.** Average rank deficiency according to predicted interleaving period.
alarms, and we set $\gamma$ to a design parameter to control false alarms.

Algorithm 1 provides a step-by-step summary of our proposed method in the context of the scant received data.

After estimating the interleaving period, we need to perform synchronization to blindly deinterleave the received data. We can synchronize the received data simply by repeating the proposed method with delay shifts of received data sequence $r$ [10]. For example, we can shift $r$ from 0 to $L - 1$ for synchronization when the interleaving period obtained by (5) is $L$.

Algorithm 1: Blind Interleaver Parameter Estimation Using Matrix Multiplication From Scant Data

**Notation of Variable:** $L_{min}$ and $L_{max}$ are the minimum and maximum values of $\tilde{L}$, respectively, and $\text{Crd}$ denotes the number of $R_q$'s composed to calculate average rank deficiency.

**Input:** The scant received data sequence $r$

1: For $L = L_{min}$: $L_{max}$ do
2: Generate an $n \times L$ matrix $R_d$ from (3)
3: For $i = 1$: $\text{Crd}$ do
4: Randomly erase rows and columns from $R_d$ and generate $k$ different $l \times l$ square submatrices $R_s$’s
5: Compose additional square matrix $R_q$ by multiplying generated $k$ different $R_s$’s
6: Calculate the rank deficiency of $R_q$
7: End
8: Average the rank deficiencies of additional square matrices $R_q$’s to calculate $m(\tilde{L})$
9: End
10: Decide $L$ in (5) and calculate the gap between the largest value of $m(\tilde{L})$ and the second largest value of $m(\tilde{L})$
11: When the gap is larger than $\gamma$, declare $L$ in (5) as the original interleaving period

**Output:** Estimated interleaving period $L$

### IV. SIMULATION RESULTS

In this section, through computer simulations, we first examine the detection probability of the proposed method by varying $k$, the number of square submatrices $R_s$’s to be multiplied to compose additional square matrices $R_q$’s. Then, we investigate the detection performance of the proposed method according to $\gamma$, the threshold to control false alarms. Finally, we validate the proposed method according to $M$, the number of received data bits, in terms of detection probability and the number of false alarms, and compare the result of the proposed method to that of the conventional method in [13]. In the simulations, we assume a random interleaver with interleaving period $L$, binary phase shift keying modulation, and an additive white Gaussian noise channel. We further assume a number of received data bits as scant as $M = L \times L \times \alpha$ bits for $0 < \alpha < 1$ to show that the proposed method provides superior estimation performance of the interleaving period under scant received data.

First, we show the detection probability of the proposed method by varying $k$ from 2 to 4 in Fig. 3, when $L$ is 60, (15, 11) BCH code is used, $\gamma$ is 0.75, $M$ is 3240 ($60 \times 60 \times 0.9$) bits, and $l$ is $\min(n, \tilde{L}) - 1$. Fig. 3 shows that the detection probability improves as $k$ increases. This is because we can construct more matrices for obtaining rank deficiencies as $k$ increases. However, the complexity of the proposed method increases because we need more matrix multiplications as $k$ increases. Therefore, we set $k$ to a design parameter.

Then, we present the detection probability and the number of false alarms of the proposed method for various values of $\gamma$ in Figs. 4 and 5, respectively, when $L$ is 60, (15, 11) BCH code is used, $k$ is 2, $M$ is 3240 ($60 \times 60 \times 0.9$) bits, and $l$ is $\min(n, \tilde{L}) - 1$. We can see from Figs. 4 and 5 that, as $\gamma$ decreases, the detection probability increases, but the number of false alarms also increases. Therefore, we can confirm that there is a trade-off between the detection probability and the number of false alarms according to the threshold $\gamma$; we also set $\gamma$ to a design parameter.

Finally, we validate the proposed method according to $M$ by showing the detection probability and the number of false alarms in Figs. 6 and 7, respectively, when $L$ is 60, (15, 11) BCH code is used, $\gamma$ is 0.75, $k$ is 2, and $l$ is $\min(n, \tilde{L}) - 1$. For comparison, we include performance of the conventional

![FIGURE 3. Detection probability according to $k$.](image-url)

![FIGURE 4. Detection probability according to $\gamma$.](image-url)
them, the linearity remaining in $R_q$ becomes larger than the linearity remaining in $R_s$’s. As the linearity remaining in $R_q$ increases, the rank deficiency of $R_q$ also increases, and therefore detection performance improves. This property becomes more apparent as $M$ decreases, and so the performance gap between both methods increases as $M$ decreases.

For example, in Fig. 6, when $M$ is $3240 \times 60 \times 0.9$ bits, detection probability of the proposed method and that of the method in [13] reach 0.9 at signal-to-noise ratio (SNR) of about 5.5 dB. When $M$ decreases to $2520 \times 60 \times 0.7$ bits, the proposed method achieves SNR gains of about 0.7 dB compared to [13] at a detection probability of 0.9. Moreover, using an even smaller number of received data, when $M$ is $2412 \times 60 \times 0.67$ bits, the detection probability of the proposed method reaches 0.9 at SNR of about 7.7 dB, while the conventional method in [13] cannot give any meaningful result. The results in Figs. 6 and 7 indicate that the proposed method is better than the conventional methods under the same condition of scant received data.

V. CONCLUSION

In this paper, we proposed an improved blind interleaver parameter estimation method using matrix multiplication under the condition of scant received data. We first generated a matrix from the received data and made arbitrary square submatrices by randomly deleting rows and columns from the generated matrix. Then, we composed additional square matrices by multiplying the square submatrices and examined the rank deficiencies of the additional square matrices. Finally, we blindly estimated the interleaver parameter based on the average rank deficiency of composed additional square matrices.

To validate the proposed method, we presented detection probability and the number of false alarms through computer simulations. Simulation results showed that the proposed method works better than the conventional ones for scant received data. Moreover, under the condition of an even more limited amount of received data, the proposed method can estimate the interleaver parameter while the conventional ones cannot give a meaningful result. Since the proposed method uses the hidden linearity in the received data, which remains even in a limited amount of received data, it is straightforwardly applicable to other blind communication parameter estimation, such as estimation of channel code where intrinsic linearity resides.

ACKNOWLEDGMENT

(Yongseok Jung and Mingyu Jang contributed equally to this work.)

REFERENCES

[1] G. Burel and R. Gautier, “Blind estimation of encoder and interleaver characteristics in a non-cooperative context,” in Proc. IASTED, Scottsdale, AZ, USA, 2003, pp. 275–280.
[2] G. Sicot, S. Houcke, and J. Barbier, “Blind detection of interleaver parameters,” Signal Process., vol. 89, no. 4, pp. 450–462, Apr. 2009.
[3] J. Jeong, D. Yoon, J. Lee, and S. Choi, “Blind reconstruction of a helical scan interleaver,” in *Proc. IEEE ICICS*, Singapore, Dec. 2011, pp. 1–4.

[4] 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.

[5] S. Ramabadr, 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.

[6] 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, pp. 463–478, Sep. 2017.

[7] R. Swaminathan, A. S. Madhukumar, G. Wang, and T. S. Kee, “Blind reconstruction of Reed–Solomon encoder and interleavers over noisy environment,” *IEEE Trans. Broadcast.*, vol. 64, no. 4, pp. 830–845, Dec. 2018.

[8] Y. Xu, Y. Zhong, and Z. Huang, “An improved blind recognition method of the convolutional interleaver parameters in a noisy channel,” *IEEE Access*, vol. 7, pp. 101775–101784, 2019.

[9] C. Choi and D. Yoon, “Enhanced blind interleaver parameters estimation algorithm for noisy environment,” *IEEE Access*, vol. 6, pp. 5910–5915, 2017.

[10] C. Choi and D. Yoon, “Novel blind interleaver parameter estimation in a noncooperative context,” *IEEE Trans. Aerosp. Electron. Syst.*, vol. 55, no. 4, pp. 2079–2085, Aug. 2019.

[11] G. Kim, M. Jang, and D. Yoon, “Improved method for interleaving parameter estimation in a non-cooperative context,” *IEEE Access*, vol. 7, pp. 92171–92175, 2019.

[12] M. Jang, G. Kim, Y. Kim, and D. Yoon, “Blind estimation of interleaver parameter with a limited number of data,” *IEEE Access*, vol. 8, pp. 69160–69166, 2020.

[13] M. Jang, G. Kim, D. Kim, and D. Yoon, “Blind interleaver parameter estimation from scant data,” *IEEE Access*, vol. 8, pp. 217282–217289, 2020.

[14] G. Strang, *Introduction to Linear Algebra*, 5th ed. Wellesley, MA, USA: Wellesley Cambridge Press, 2016.

**YONGSEOK JUNG** received the B.S. degree from Korea Military Academy, Seoul, Korea, in 2008, and the M.S. degree in electrical and electronic engineering from Yonsei University, Seoul, in 2018. He is currently pursuing the Ph.D. degree with the Department of Electronic Engineering in Hanyang University, Seoul. His research interests include military communications and satellite communications.

**MINGYU JANG** received the B.S. degree in electronic engineering from Hanyang University, Seoul, Korea, in 2019, where he is currently pursuing the Ph.D. degree with the Department of Electronic Engineering. His research interests include digital communication theory and wireless communications.

**DONGWEON YOON** (Senior Member, IEEE) received the B.S. (summa cum laude), M.S., and Ph.D. degrees in electronic communications engineering from Hanyang University, Seoul, Korea, in 1989, 1992, and 1995, respectively. From March 1995 to August 1997, he was an Assistant Professor with the Department of Electronic and Information Engineering, Dongseo University, Busan, Korea. From September 1997 to February 2004, he was an Associate Professor with the Department of Information and Communications Engineering, Daejeon University, Daejeon, Korea. Since March 2004, he has been on the faculty of Hanyang University, where he is currently a Professor with the Department of Electronic Engineering and the Director of the Signal Intelligence Research Center. His research interests include digital communications theory and systems, detection and estimation, satellite and space communications, and communication forensics.