# Binary Sequence Family for Chaotic Compressed Sensing

**Cunbo Lu[1], Wengu Chen[1*] and Haibo Xu[1]**
[1] Institute of Applied Physics and Computational Mathematics
Beijing, 100088 - China
[e-mail: 444180647@qq.com, chenwg@iapcm.ac.cn, xu_haibo@iapcm.ac.cn]
*Corresponding author: Wengu Chen

*Received January 9, 2019; revised March 19, 2019; accepted March 30, 2019; published September 30, 2019*

## Abstract

It is significant to construct deterministic measurement matrices with easy hardware implementation, good sensing performance and good cryptographic property for practical compressed sensing (CS) applications. In this paper, a deterministic construction method of bipolar chaotic measurement matrices is presented based on binary sequence family (BSF) and Chebyshev chaotic sequence. The column vectors of these matrices are the sequences of BSF, where 1 is substituted with -1 and 0 is with 1. The proposed matrices, which exploit the pseudo-randomness of Chebyshev sequence, are sensitive to the initial state. The performance of proposed matrices is analyzed from the perspective of coherence. Theoretical analysis and simulation experiments show that the proposed matrices have limited influence on the recovery accuracy in different initial states and they outperform their Gaussian and Bernoulli counterparts in recovery accuracy. The proposed matrices can make the hardware implement easy by means of linear feedback shift register (LFSR) structures and numeric converter, which is conducive to practical CS.

***Keywords:*** Compressed sensing, measurement matrix, coherence, binary sequence family, chaotic sequence

The research is supported by National Nature Science Foundation of China (Nos. 11871109, 61802428, 11675021), NSAF Joint Fund (No. U1830107) and Science Challenge Project (TZ2018001).

**http://doi.org/10.3837/tiis.2019.09.018** **ISSN : 1976-7277**

## 1. Introduction

Different from Nyquist sampling theorem, compressed sensing (CS) is a new revolutionary signal sampling framework proposed by Candès, Romberg, Tao and Donoho in 2006 [1, 2]. It can improve the sampling efficiency by sampling sparse signals at a rate far lower than the Nyquist rate. By exploiting the sparsity property, the original high-dimensional sparse signal can be recovered exactly from the lower-dimensional measurement vector with high probability by solving an optimization problem. The new idea of CS has caused the extensive attention of academic circles and has been applied to various research fields, such as image processing, information theory, wireless communication, encryption and radar imaging. CS has also potential applications in areas, such as big video data [3] and object tracking [4, 5].

The process of CS can be viewed as having two stages: data sampling and signal recovery. Let $\mathbf{x} = \{x_i\}_{i=1}^{N} \in \mathbf{R}^N$ be a $k$- sparse original signal, where $\|x\|_0 = \left|\{i | x_i \neq 0\}\right| \leq k$ . The lower-dimensional observation signal $\mathbf{y} \in \mathbf{R}^M$ can be obtained from its linear measurements with a measurement matrix $\mathbf{A} \in \mathrm{R}^{\mathrm{M\times N}}$, where $M << N$. In matrix representation, $\mathbf{y} = \mathbf{A}\mathbf{x}$. This linear process is the data sampling process of CS. As for the signal recovery stage, the original high-dimensional sparse signal $\mathbf{x}$ can be reconstructed exactly from the lower-dimensional measurement vector $\mathbf{y}$ by solving the following $l_0$ minimization optimization problem

$$\min_{\mathbf{x}} \|\mathbf{x}\|_0 \quad \text{subject to} \quad \mathbf{y} = \mathbf{A}\mathbf{x}. \tag{1}$$

The above solving problem is NP-hard [6]. The CS theory proves that by using a proper measurement matrix $\mathbf{A}$, solving problem (1) can be replaced with solving the following $l_1$ minimization optimization problem

$$\min_{\mathbf{x}} \|\mathbf{x}\|_1 \quad \text{subject to} \quad \mathbf{y} = \mathbf{A}\mathbf{x}, \tag{2}$$

where $\|x\|_1 = \sum_{i=1}^{N} |x_i|$. In this problem, the sparsest estimate of $\mathbf{x}$ can be obtained by basis pursuit (BP) algorithm [7]. Besides, there are some greedy algorithms for solving problem (1) directly, such as orthogonal matching pursuit (OMP) [8].

In CS theory, measurement matrix plays a vital role. In data sampling stage, a better measurement matrix can lead to a smaller number of measurements to achieve the same reconstruction accuracy. In signal recovery stage, a better measurement matrix can lead to a higher reconstruction accuracy at the same number of measurements. Overall, a good measurement matrix $\mathbf{A} \in \mathrm{R}^{\mathrm{M\times N}}$ should ensure that the projected measurements $\mathbf{y} \in \mathbf{R}^M$ maintain all the significant information of original signal $\mathbf{x} \in \mathbf{R}^N$ so that the original signal $\mathbf{x}$ can be reconstructed exactly from the lower-dimensional projected measurements $\mathbf{y}$ with high probability. Candes and Tao [6] proposed a criteria named Restricted Isometry Property (RIP) in which the measurement matrix must satisfy.

***Definition 1.1*** For a matrix $\mathbf{A} \in \mathrm{R}^{\mathrm{M\times N}}$, if there exists the smallest number $\delta_k \in [0,1)$ such that

$$(1-\delta_k)\|\mathbf{x}\|_2^2 \leq \|\mathbf{A}\mathbf{x}\|_2^2 \leq (1+\delta_k)\|\mathbf{x}\|_2^2 \tag{3}$$

holds for any $k$ - sparse signal $\mathbf{x} \in \mathbf{R}^N$. Then the matrix $\mathbf{A}$ is said to satisfy the RIP of order $k$. The $\delta_k$ is called the restricted isometry constant (RIC) of order $k$.

With some conditions on $\delta_k$, RIP implies that the solution of problem (1) is coincident with that of problem (2) [9, 10] if the solution of problem (1) exists.

Coherence is another important criteria to construct RIP matrices.

***Definition 1.2*** Let $\mathbf{a}_1, \mathbf{a}_2, \cdots, \mathbf{a}_N$ be the column vectors of matrix $\mathbf{A}$, then its coherence $\mu(\mathbf{A})$ is defined as

$$\mu(\mathbf{A}) = \max_{1 \le i \ne j \le N} \frac{\left| \left\langle \mathbf{a}_i, \mathbf{a}_j \right\rangle \right|}{\left\| \mathbf{a}_i \right\|_2 \cdot \left\| \mathbf{a}_j \right\|_2}, \tag{4}$$

where $\left\langle \mathbf{a}_i, \mathbf{a}_j \right\rangle = \mathbf{a}_i^T \mathbf{a}_j$ is the inner product of vectors $\mathbf{a}_i$ and $\mathbf{a}_j$.

The following lemma [10-12] relates the RIC $\delta_k$ and the coherence $\mu$.

***Lemma 1.1*** For a matrix $\mathbf{A}$, the relationship between the coherence $\mu(\mathbf{A})$ and the $k$ order RIC $\delta_k$ is $\delta_k \le \mu(\mathbf{A})(k-1)$, where $k < \frac{1}{\mu(\mathbf{A})} + 1$.

From above lemma, it can be seen that the matrices with low coherence satisfy RIP and are natural candidates for CS matrices.

As seen in [13], if $k$ satisfies $k < \frac{1}{2}\left[1 + \frac{1}{\mu(\mathbf{A})}\right]$, any $k$ - sparse signal $\mathbf{x}$ can be reconstructed accurately from its undersampling linear measurements $\mathbf{y} = \mathbf{A}\mathbf{x}$ via BP algorithm or OMP algorithm. Therefore, when we design measurement matrix $\mathbf{A}$, the upper bound of reconstructed signal sparsity $k$ can be increased by reducing the coherence $\mu(\mathbf{A})$, which means an increase in reconstruction performance. To realize the reconstruction of original signal with high accuracy, we should reduce the coherence $\mu(\mathbf{A})$ as far as possible.

The OMP algorithm involves lower complexity than the BP algorithm and requires a shorter running time. Therefore, it is relatively simple and fast in hardware implementation and becomes a widely used algorithm in hardware design [14, 15]. In this paper, considering the practical CS applications, the OMP algorithm is applied for signal recovery to benefit from the low coherence of the CS matrices.

Both RIP [16-19] and coherence [9-13, 20-27] are important tools to analyze the property of measurement matrices. In this paper, coherence will be adopted to analyze and illustrate the property of constructed measurement matrices, because it is easier to compute.

Existing measurement matrices can be divided into two categories: random measurement matrices and deterministic measurement matrices. For the former, the most widely used matrices are Gaussian or Bernoulli ones. Due to that random matrices satisfy RIP with overwhelming probability, they are widely used in scientific research. However, in random matrices, every element obeys certain probability distribution, where randomness exists. In order to realize a random matrix, all elements should be stored and the process is repeated when a new realization is needed, which would cost lots of storage resources. Random number generation has very high requirement to the hardware, which is not conducive to hardware implementation and limits the practical applications of CS. These deficiencies can be overcome by deterministic measurement matrices to get rid of the randomness. Although

deterministic matrices may need a lot of complex mathematical operations during their construction, all elements of these matrices can be computed and generated on the fly only once, thus providing storage efficiency. Recently, many researchers have exploited some existing theories and techniques to construct deterministic measurement matrices, such as Euler Squares [9], extremal set theory [10], near orthogonal systems [12], chaotic systems [20-22], Legendre sequences [23], optimal codebooks [24], bipartite graph [25], low-density parity-check (LDPC) codes [13, 14, 26, 28], equiangular tight frame theory [27], Reed-Muller sequences [29] and sparse fast Fourier transform [30]. In particular, Sasmal et al. [11] proposed an optimal deterministic binary CS matrices by using a specialized composition rule which exploits the properties of existing binary matrices. The above mentioned deterministic measurement matrices show good sensing performance.

M-sequence is a type of pseudorandom binary sequence, which is also called maximum length LFSR sequence. The generation of m-sequence depends on the feedback coefficients of LFSR associated with a feedback polynomial. For LFSR, different feedback polynomials generate distinct m-sequences [31]. For m-sequence, the properties of balance, excursion distribution and auto-correlation are similar to the basic properties of random sequence [32]. Therefore, m-sequence is the most widely used pseudorandom sequence. In [31], the BSF is constructed based on the linear combination of m-sequences or their shifts such that the resulting sequences have low correlation. The implementation of BSF is extremely easy by summing LFSR outputs. This paper attempts to relate the notion of BSF to the design of deterministic measurement matrices.

In this paper, inspired by the BSF in [31] and Chebyshev chaotic sequence in [21], we construct a class of deterministic bipolar chaotic measurement matrices named BSFDBC with the elements of +1 and -1. First, we choose the trace representative function given in [31] to generate the set of binary pseudo-random sequences which constitute the BSF. And then, by numeric convert, the BSF is converted to the corresponding bipolar sequence family. By selecting some sequences among the bipolar sequence family and using the chaotic-based permutation algorithm [21] to put them together in designed order as column vectors, the proposed BSFDBC matrix is obtained. The BSFDBC matrices have good potential cryptographic property because a brute force search of the permutation operator is of high complexity.

The coherence of BSFDBC matrices is investigated and compared with their Gaussian and Bernoulli counterparts. Theoretical analysis and simulation experiments show that the proposed BSFDBC matrices have limited influence on the recovery accuracy in different initial states and they outperform their Gaussian and Bernoulli counterparts in recovery accuracy. Simulation experiments also show that the BSFDBC matrix is sensitive to its initial state.

The remainder of this paper is organized as follows. Section 2 introduces some preliminaries about finite field. Section 3 presents the deterministic construction procedure of BSFDBC matrices and a related example. Section 4 uses the coherence to analyze the proposed BSFDBC matrices and compares the coherence of the BSFDBC matrices with their Gaussian and Bernoulli counterparts. Simulation experiments are given to investigate the performance of proposed BSFDBC matrices in Section 5. Finally, Section 6 concludes this paper.

## 2. Preliminaries

***Definition 2.1*** Suppose $\beta$ is a primitive field element of finite field $GF(q)$ with $q$ elements, then all the field elements of $GF(q)$ can be generated with 0 and the powers of $\beta$, that is $GF(q)=\{0,\beta^0=1,\beta,\cdots,\beta^{q-2}\}$.

Among $\{0,1,\beta,\cdots,\beta^{q-2}\}$, the last $q-1$ nonzero elements constitute the multiplicative group $GF(q)\setminus\{0\}$, which is also denoted as $GF(q)^*$. For describing convenience, all elements of $GF(q)$ can also be expressed as $\{0,1,\cdots,q-1\}$.

***Definition 2.2*** Let $m$, $n$ be positive integers and $m$ be the factor of $n$. The trace function from $GF(2^n)$ to $GF(2^m)$, denoted as $Tr_m^n(x)$, is

$$Tr_m^n(x)=x+x^{2^m}+\ldots+x^{2^{m(\frac{n}{m}-1)}},x\in GF(2^n). \tag{5}$$

When $m=1$, $GF(2^m)=GF(2)=\{0,1\}$. For describing convenience, $Tr_1^n(x)$ can also be simply expressed as $Tr(x)$.

## 3. Construction and Example of BSFDBC

### 3.1 Construction of BSFDBC

The proposed BSFDBC matrices are a class of $(2^n-1)\times 2^{n+1}$ deterministic bipolar chaotic matrices with initial state $r_0\in[-1,1]$, where $n\geq 5$. The concrete realization steps of BSFDBC matrices are as follows:

**Step-1:** For given signal length $N=2^{n+1}$, $n$ is judged as odd or even. For odd $n$, choose the trace representative function (6) given in [31]; otherwise for even $n$, choose the trace representative function (7) given in [31], where $x\in GF(2^n)^*$, $\lambda_0,\lambda_1\in GF(2^n)$.

$$s_{\lambda_0,\lambda_1}(x)=Tr(\lambda_0 x)+Tr(\lambda_1 x^3)+\sum_{i=2}^{(n-1)/2}Tr(x^{1+2^i}) \tag{6}$$

$$s_{\lambda_0,\lambda_1}(x)=Tr(\lambda_0 x)+Tr(\lambda_1 x^3)+\sum_{i=2}^{n/2-1}Tr(x^{1+2^i})+Tr_1^{n/2}(x^{1+2^{n/2}}) \tag{7}$$

**Step-2:** For $GF(2^n)$, select a primitive field element $\beta$. Let $b_t^{\lambda_0,\lambda_1}=s_{\lambda_0,\lambda_1}(\beta^t)$, where $t\in\{0,1,\cdots,2^n-2\}$, and $\lambda_0,\lambda_1\in GF(2^n)$. The sequence $\{b_t^{\lambda_0,\lambda_1}\}_{t=0}^{2^n-2}=\{s_{\lambda_0,\lambda_1}(\beta^t)\}_{t=0}^{2^n-2}$, denoted as $\mathbf{b}^{\lambda_0,\lambda_1}$, is a binary pseudo-random sequence of period $2^n-1$. The set of binary sequences $\{\mathbf{b}^{\lambda_0,\lambda_1}\mid\lambda_0,\lambda_1\in GF(2^n)\}$ constitutes the BSF in [31]. By inputting all the elements of binary sequence $\mathbf{b}^{\lambda_0,\lambda_1}=\{b_t^{\lambda_0,\lambda_1}\}_{t=0}^{2^n-2}$ into the numeric convert function (8) one by one, we can obtain the corresponding bipolar pseudo-random sequence $\mathbf{c}^{\lambda_0,\lambda_1}=\{c_t^{\lambda_0,\lambda_1}\}_{t=0}^{2^n-2}$.

$$c_t^{\lambda_0,\lambda_1}=\begin{cases}1, & b_t^{\lambda_0,\lambda_1}=0\\ -1, & b_t^{\lambda_0,\lambda_1}=1\end{cases} \tag{8}$$

Order the elements of $(\lambda_0,\lambda_1)$ lexicographically as $(0,0)$, $(0,1),\cdots,(0,2^n-1)$, $(1,0)$, $(1,1),\cdots,(1,2^n-1)$, $(2,0),\cdots,(2^n-1,2^n-1)$.

When the parameter pair $(\lambda_0,\lambda_1)$ is given, the bipolar sequence $\mathbf{c}^{\lambda_0,\lambda_1}=\{c_t^{\lambda_0,\lambda_1}\}_{t=0}^{2^n-2}$ is deterministic. All sequences of $\{\mathbf{c}^{\lambda_0,\lambda_1}\mid \lambda_0\in GF(2),\lambda_1\in GF(2^n)\}$ are put together indexed by $(\lambda_0,\lambda_1)$ in order as column vectors to form a $(2^n-1)\times 2^{n+1}$ matrix $\mathbf{A}$, which has the following form

$$\begin{aligned}\mathbf{A}&=[\mathbf{c}^{0,0},\mathbf{c}^{0,1},\cdots,\mathbf{c}^{0,2^n-1}\mid\mathbf{c}^{1,0},\mathbf{c}^{1,1},\cdots,\mathbf{c}^{1,2^n-1}]\\&=\left[\begin{array}{cccc|cccc}c_0^{0,0}&c_0^{0,1}&\cdots&c_0^{0,2^n-1}&c_0^{1,0}&c_0^{1,1}&\cdots&c_0^{1,2^n-1}\\c_1^{0,0}&c_1^{0,1}&\cdots&c_1^{0,2^n-1}&c_1^{1,0}&c_1^{1,1}&\cdots&c_1^{1,2^n-1}\\\vdots&\vdots&\ddots&\vdots&\vdots&\vdots&\ddots&\vdots\\c_{2^n-2}^{0,0}&c_{2^n-2}^{0,1}&\cdots&c_{2^n-2}^{0,2^n-1}&c_{2^n-2}^{1,0}&c_{2^n-2}^{1,1}&\cdots&c_{2^n-2}^{1,2^n-1}\end{array}\right]\end{aligned}\tag{9}$$

**Step-3:** Let $R(r_0,s,l)$ be the sampled Chebyshev sequence $\{r_0,r_s,r_{2s},\cdots,r_{(l-1)s}\}$ generated by the Cheyshev map $r_{j+1}=\cos(w\cdot\arccos(r_j))$ given in [21], where $j=0,1,2,\cdots$, $r_0\in[-1,1]$ is the initial state and $w$ is a positive integer larger than 1. The $w$ is also called the degree of the map. For given $r_0$, record each value of $R(r_0,s,l)$ with $w=5$, $s=5$, and $l=N=2^{n+1}$. Then, sort the $\{r_0,r_s,r_{2s},\cdots,r_{(l-1)s}\}$ in descending order and obtain the corresponding index set $\chi$, which will be a chaotic set because of the pseudo-randomness of $R(r_0,s,l)$ [21].

**Step-4:** Permute the column vectors of $\mathbf{A}$ in designed order of set $\chi$ to obtain the proposed BSFDBC matrix $\mathbf{A}_{r_0}$. In matrix representation, $\mathbf{A}_{r_0}=\mathbf{AD}_{r_0}$, where the chaotic-based permutation operator $\mathbf{D}_{r_0}$ is a deterministic column permutation of an identity matrix $\mathbf{I}\in\mathbf{R}^{2^{n+1}\times 2^{n+1}}$ in the designed order of set $\chi$.

From above construction, it can be seen that the sampling rate of BSFDBC matrices is $(2^n-1)/2^{n+1}\approx 0.5$. For odd $n=2l+1$, the process for obtaining a column vector in $\mathbf{A}_{r_0}\in\mathbf{R}^{(2^n-1)\times 2^{n+1}}$ can be understood by first adding $(l+1)$ m-sequences with different feedback polynomials and then converting the result summing sequence using element substituting in (8). In addition, the related Chebyshev chaotic sequence $R(r_0,s,l)$ is deterministic with fixed initial state $r_0$. The corresponding permutation operator $\mathbf{D}_{r_0}$ can be reflected in the permutation of element order $(\lambda_0,\lambda_1)$. Hence, $\mathbf{A}_{r_0}\in\mathbf{R}^{(2^n-1)\times 2^{n+1}}$ is easy to implement by summing LFSR outputs and using numeric converter, which is conducive to practical CS.

***Remark 1*** Suppose the adversary knows $\mathbf{A}$ and wants to know $\mathbf{A}_{r_0}=\mathbf{AD}_{r_0}$, the permutation operator $\mathbf{D}_{r_0}$ is required which corresponds to a permutation of integers $[1,2,\cdots,2^{n+1}]$. A brute force search of the permutation is needed and the complexity is $(2^{n+1})!$.

Note that $n \geq 5$, $(2^{n+1})! \geq 64!$. The cost of guessing the permutation operator $\mathbf{D}_{r_0}$ is very high, which is too expensive for the adversary to be practical. Therefore, the BSFDBC matrices have good potential cryptographic property.

***Remark 2*** The initial state $r_0$ of the BSFDBC determines the permutation order according to the construction steps. A different $r_0$ will lead to a different permutation order, which will further generate a different BSFDBC matrix. Therefore, $r_0$ can be considered as the secret key to construct the BSFDBC matrix, which would be favorable in practical CS applications.

***Remark 3*** Since $r_0$ can be any value among the interval $[-1,1]$, a large number of BSFDBC matrices can be obtained. These matrices can be used as encryption keys for cryptography, which implies that encryption occurs implicitly in the data sampling stage.

### 3.2 An Example of BSFDBC

In the following, we give an example of a column vector of BSFDBC $\mathbf{A}_{r_0}$ of size $127 \times 256$.

Let $GF(2^7)$ be the finite field with the primitive field element $\beta$ satisfying $\beta^7 + \beta + 1 = 0$. In matrix $\mathbf{A}$, the binary sequence $\mathbf{b}^k = \{b_t^k\}$, which corresponds to $k$ th column vector, is given by (6) at $n = 7$, and $x = \beta^t$ for $0 \leq t \leq 126$.

For $k = 128i_0 + i_1 + 1$ with $i_0 = 0,1$ and $0 \leq i_1 \leq 127$, if $i_1 \neq 127$, $b_t^k = Tr(\beta^{i_0}\beta^t + \beta^{i_1}\beta^{3t} + \beta^{5t} + \beta^{9t})$; if $i_1 = 127$, $b_t^k = Tr(\beta^{i_0}\beta^t + \beta^{5t} + \beta^{9t})$. For different values of $(i_0, i_1)$, 256 cyclically distinct binary sequences $\mathbf{b}^k = \{b_t^k\}$ are obtained, which correspond to all column vectors of BSFDBC. Let $\mathbf{g} = \{g_t\}$, $g_t = Tr(\beta^t)$ and $\mathbf{g}^{(j)} = \{g_{jt}\}$. Then $\mathbf{g}$ is given by

$$\begin{aligned}\{g_t\} = & 10000001000001100001010001111001 \\ & 00010110011101010011111010000111 \\ & 00010010011011010110111101100011 \\ & 01001011101110011001010101111111.\end{aligned} \tag{10}$$

From above, it is seen that $\mathbf{b}^k = \{b_t^k\}$ can be obtained from the linear combination of m-sequences $\mathbf{g}$, $\mathbf{g}^{(3)}$, $\mathbf{g}^{(5)}$, $\mathbf{g}^{(9)}$ or their shifts. For $k = 128i_0 + i_1 + 1$ with $i_0 = 0,1$ and $0 \leq i_1 \leq 127$, if $i_1 \neq 127$, $b_t^k = g_{t+i_0} + g_{3t+i_1} + g_{5t} + g_{9t}$; otherwise if $i_1 = 127$, $b_t^k = g_{t+i_0} + g_{5t} + g_{9t}$. By inputting all the elements of binary sequence $\mathbf{b}^k = \{b_t^k\}$ into the numeric convert function (8) one by one, we can obtain the corresponding bipolar sequence $\mathbf{c}^k = \{c_t^k\}$, which is the $k$ th column vector of $\mathbf{A}$. After the permutation operator $\mathbf{D}_{r_0}$, the column vector $\mathbf{c}^k = \{c_t^k\}$ is mapped into the corresponding position of $\mathbf{A}_{r_0} = \mathbf{A}\mathbf{D}_{r_0}$.

## 4. Coherence Analysis

In this section, for proposed BSFDBC matrix $\mathbf{A}_{r_0} = \mathbf{AD}_{r_0}$ constructed in section 3, the coherence $\mu(\mathbf{A}_{r_0})$ is used to analyze and compare the performance of BSFDBC matrix with its Gaussian and Bernoulli counterparts.

In order to derive the coherence of proposed BSFDBC matrix $\mathbf{A}_{r_0}$, the following one definition and one lemma are first introduced [31].

***Definition 4.1*** Let $\mathbf{a} = (a_0, a_1, \cdots, a_v)$ and $\mathbf{b} = (b_0, b_1, \cdots, b_v)$ be two different binary sequence of period $v$. The cross-correlation of $\mathbf{a}$ and $\mathbf{b}$ is defined as $C_{\mathbf{a},\mathbf{b}}(\tau) = \sum_{i=0}^{v-1} (-1)^{a_i + b_{i+\tau}}$ for $0 \le \tau \le v-1$, where $i+\tau$ is computed modulo $v$. If $\mathbf{a}$ and $\mathbf{b}$ are cyclically equivalent, $C_{\mathbf{a},\mathbf{b}}(\tau)$ is the auto-correlation of sequence $\mathbf{a}$.

***Lemma 4.1*** For odd $n$, the cross-correlation of any two binary sequences $\mathbf{a}$ and $\mathbf{b}$ given by (6) is $C_{\mathbf{a},\mathbf{b}}(\tau) \in \{-1, -1 \pm 2^{(n+1)/2}, -1 \pm 2^{(n+3)/2}\}$. For even $n$, the cross-correlation of any two binary sequences $\mathbf{a}$ and $\mathbf{b}$ given by (7) is $C_{\mathbf{a},\mathbf{b}}(\tau) \in \{-1, -1 \pm 2^{n/2}, -1 \pm 2^{n/2+1}, -1 \pm 2^{n/2+2}\}$.

***Theorem 4.1*** Let $\mathbf{A}_{r_0}$ be a $(2^n - 1) \times 2^{n+1} (n \ge 5)$ BSFDBC matrix constructed in Section 3, where $\mathbf{A}_{r_0} = \mathbf{AD}_{r_0}$, and $r_0 \in [-1, 1]$. If $n$ is odd, $\mu(\mathbf{A}_{r_0}) \le \dfrac{1 + 2^{(n+3)/2}}{2^n - 1}$; if $n$ is even, $\mu(\mathbf{A}_{r_0}) \le \dfrac{1 + 2^{n/2+2}}{2^n - 1}$.

***Proof:*** For matrix $\mathbf{A}_{r_0} \in \mathbf{R}^{(2^n-1) \times 2^{n+1}}$, we have $\mu(\mathbf{A}_{r_0}) = \mu(\mathbf{AD}_{r_0}) = \mu(\mathbf{A})$ according to the definition of coherence in (4), because $\mathbf{D}_{r_0}$ only permute the column vectors of $\mathbf{A}$ in designed order. To compute $\mu(\mathbf{A}_{r_0})$, we can compute $\mu(\mathbf{A})$. Let $\mathbf{A}^i$ be the $i$ th column of $\mathbf{A}$. Then

$$\mu(\mathbf{A}) = \max_{1 \le i \ne j \le 2^{n+1}} \frac{\left| \left\langle \mathbf{A}^i, \mathbf{A}^j \right\rangle \right|}{\left\| \mathbf{A}^i \right\|_2 \cdot \left\| \mathbf{A}^i \right\|_2}. \tag{11}$$

Note that sequence $\mathbf{A}^i$ and $\mathbf{A}^j$ are bipolar sequences of period $2^n - 1$ with the elements of +1 and -1. We have

$$\left\| \mathbf{A}^i \right\|_2 = \left\| \mathbf{A}^j \right\|_2 = (2^n - 1)^{1/2}. \tag{12}$$

It can be seen from the construction in Section 3 that the matrix $\mathbf{A} \in \mathbf{R}^{(2^n-1) \times 2^{n+1}}$ has a BSF $\{\mathbf{b}^{\lambda_0, \lambda_1} \mid \lambda_0, \lambda_1 \in GF(2^n)\}$ and a bipolar sequence family $\{\mathbf{c}^{\lambda_0, \lambda_1} \mid \lambda_0, \lambda_1 \in GF(2^n)\}$ correspondingly. The column vector $\mathbf{A}^i$ of $\mathbf{A}$ is the bipolar sequence $\mathbf{c}^i$ in $\{\mathbf{c}^{\lambda_0, \lambda_1} \mid \lambda_0 \in GF(2), \lambda_1 \in GF(2^n)\}$.

Let $\mathbf{b}^i = \{b_t^i\}_{t=0}^{2^n-2}$ and $\mathbf{b}^j = \{b_t^j\}_{t=0}^{2^n-2}$ be any two binary sequences of $\{\mathbf{b}^{\lambda_0, \lambda_1} \mid \lambda_0 \in GF(2), \lambda_1 \in GF(2^n)\}$. From (8), the corresponding two bipolar sequences

$\mathbf{c}^i = \{c_t^i\}_{t=0}^{2^n-2}$ and $\mathbf{c}^j = \{c_t^j\}_{t=0}^{2^n-2}$ are obtained, both of which belong to $\{\mathbf{c}^{\lambda_0,\lambda_1} \mid \lambda_0 \in GF(2), \lambda_1 \in GF(2^n)\}$. We have

$$\left\langle \mathbf{A}^i, \mathbf{A}^j \right\rangle = \left\langle \mathbf{c}^i, \mathbf{c}^j \right\rangle = \sum_{t=0}^{2^n-2} c_t^i(s) c_t^j(s) = \sum_{t=0}^{2^n-2} (-1)^{b_t^i + b_t^j} = C_{\mathbf{b}^i, \mathbf{b}^j}(0). \tag{13}$$

Notice that

$$\begin{aligned} \mathbf{b}^i, \mathbf{b}^j &\in \{\mathbf{b}^{\lambda_0,\lambda_1} \mid \lambda_0 \in GF(2), \lambda_1 \in GF(2^n)\} \\ &\subset \{\mathbf{b}^{\lambda_0,\lambda_1} \mid \lambda_0, \lambda_1 \in GF(2^n)\}, \end{aligned}$$

where $\{\mathbf{b}^{\lambda_0,\lambda_1} \mid \lambda_0, \lambda_1 \in GF(2^n)\}$ is the BSF in [31].

Using Lemma 4.1, we can obtain that if $n$ is odd,

$$\max_{1 \le i \ne j \le 2^{n+1}} \left| \left\langle \mathbf{A}^i, \mathbf{A}^j \right\rangle \right| = \max_{1 \le i \ne j \le 2^{n+1}} \left| C_{\mathbf{b}^i, \mathbf{b}^j}(0) \right| \le \max \left| -1, -1 \pm 2^{(n+1)/2}, -1 \pm 2^{(n+3)/2} \right| = 1 + 2^{(n+3)/2}.$$

Similar to the derivation process for odd $n$, for even $n$, $\max_{1 \le i \ne j \le 2^{n+1}} \left| \left\langle \mathbf{A}^i, \mathbf{A}^j \right\rangle \right| = 1 + 2^{n/2+2}$.

Theorem 4.1 is proved after substitution of above conclusion and (12) into (11).

□

***Remark of Theorem 4.1*** Theorem 4.1 demonstrates that the initial state $r_0$ of BSFDBC matrix $\mathbf{A}_{r_0}$ has no influence on the upper bound of coherence $\mu(\mathbf{A}_{r_0})$. From the proof, we can see that if $r_0 \ne r_1 \in [-1,1]$, $\mu(\mathbf{A}_{r_0}) = \mu(\mathbf{A}_{r_1}) = \mu(\mathbf{A})$. This means that the value of coherence $\mu(\mathbf{A}_{r_0})$ of BSFDBC matrix $\mathbf{A}_{r_0}$ has no relation with its initial state $r_0$.

In order to compare the coherence of proposed BSFDBC matrices with their Gaussian and Bernoulli counterparts, the following two lemmas are introduced [33].

***Lemma 4.2*** Let $\{x_i\}_{i=1}^p$ and $\{y_i\}_{i=1}^p$ be sequences of independent and identically distributed zero-mean Gaussian random variables with variance $\sigma^2$. Then

$$\Pr\left( \left| \sum_{i=1}^p x_i y_i \right| \ge t \right) \le 2 \exp\left( -\frac{t^2}{4\sigma^2 (p\sigma^2 + t/2)} \right). \tag{14}$$

***Lemma 4.3*** Let $\{x_i\}_{i=1}^p$ and $\{y_i\}_{i=1}^p$ be sequences of independent and identically distributed zero-mean bounded random variables which satisfy $|x_i| \le a$ and $|x_i y_i| \le a^2$. Then

$$\Pr\left( \left| \sum_{i=1}^p x_i y_i \right| \ge t \right) \le 2 \exp\left( -\frac{t^2}{2pa^4} \right). \tag{15}$$

***Theorem 4.2*** For a $(2^n - 1) \times 2^{n+1} (n \ge 5)$ BSFDBC matrix $\mathbf{A}_{r_0}$, its coherence $\mu(\mathbf{A}_{r_0})$ is smaller than the corresponding Gaussian matrix $\mathbf{B}$ and Bernoulli matrix $\mathbf{D}$ with the elements of +1 and -1.

***Proof:*** Suppose $\mathbf{B} = [\mathbf{b}_1, \mathbf{b}_2, ..., \mathbf{b}_{2^{n+1}}] \in \mathbf{R}^{(2^n-1) \times 2^{n+1}}$ and $\mathbf{D} = [\mathbf{d}_1, \mathbf{d}_2, ..., \mathbf{d}_{2^{n+1}}] \in \mathbf{R}^{(2^n-1) \times 2^{n+1}}$, where $\mathbf{b}_i$ and $\mathbf{d}_i$ are column vectors of the matrices $\mathbf{B}$ and $\mathbf{D}$ for $1 \le i \le 2^{n+1}$, respectively.

Without loss of generality, we prove the theorem in case of even $n$.

Let $\{x_i\}_{i=1}^{2^n-1}$ and $\{y_i\}_{i=1}^{2^n-1}$ be any two column vectors of Gaussian matrix $\mathbf{B}$. Based on Lemma 4.2 with $p=2^n-1,\ t>\dfrac{1+2^{n/2+2}}{2^n-1}$, and $\sigma^2=\dfrac{1}{2^n-1}$, we have

$$\Pr\left(\left|\sum_{i=1}^{2^n-1}x_i y_i\right|\geq t\right)\leq 2\exp\left\{-\frac{(2^n-1)t^2}{4+2t}\right\}. \tag{16}$$

Let $z(n,t)=2\exp\left\{-\dfrac{(2^n-1)t^2}{4+2t}\right\}$. It is easy to obtain that $z(n,t)$ increases as $n$ decreases. Thus, we have $z(n,t)\leq z(6,t)$. It can be further derived that

$$\Pr\left(\left|\sum_{i=1}^{2^n-1}x_i y_i\right|\geq t\right)\leq z(6,t)=2\exp\left\{-\frac{63t^2}{4+2t}\right\}. \tag{17}$$

We observe that $z(6,t)$ increases as $t$ decreases. Thus, we have $z(6,t)<z(6,\dfrac{1+2^{n/2+2}}{2^n-1})$.

Let $z_1(n)=z(6,\dfrac{1+2^{n/2+2}}{2^n-1})$. We can also observe that $z_1(n)$ increases as $n$ decreases. Thus, we have $z(6,t)<z_1(n)\leq z_1(6)\approx 2\exp(-3.4245)$. Further, we have

$$\Pr\left(\left|\sum_{i=1}^{2^n-1}x_i y_i\right|\geq t\right)<z_1(6)\approx 2\exp(-3.4245)\approx 0.065. \tag{18}$$

For matrix $\mathbf{B}$, $\left|\sum_{i=1}^{2^n-1}x_i y_i\right|$ can characterize its coherence $\mu(\mathbf{B})$ according to the definition of coherence in (4). Let $S=\{\mathbf{b}_1,\mathbf{b}_2,...,\mathbf{b}_{2^{n+1}}\}$. We have

$$\mu(\mathbf{B})=\max_{\{x_i\},\{y_i\}}\left\{\sum_{i=1}^{2^n-1}x_i y_i\middle|\{x_i\}\subset S,\{y_i\}\subset S\setminus\{x_i\}\right\}. \tag{19}$$

Further, we have $\Pr\left(\min\limits_{\{x_i\},\{y_i\}}\left|\sum_{i=1}^{2^n-1}x_i y_i\right|\geq t\right)<\{z_1(6)\}^{\frac{|S|(|S|-1)}{2}}\approx 0.065^{2^n(2^{n+1}-1)}$.

Let $\delta_b(n)=0.065^{2^n(2^{n+1}-1)}$ with $n\geq 6$. Obviously, we can obtain that

$$\Pr\left(\min_{\{x_i\},\{y_i\}}\left|\sum_{i=1}^{2^n-1}x_i y_i\right|\leq t\right)\geq 1-\delta_b(n)\approx 1. \tag{20}$$

Hence, $\mu(\mathbf{B})=\max\limits_{\{x_i\},\{y_i\}}\sum_{i=1}^{2^n-1}x_i y_i\geq t$. By $t>\dfrac{1+2^{n/2+2}}{2^n-1}$, and $\mu(\mathbf{A}_{r_0})\leq\dfrac{1+2^{n/2+2}}{2^n-1}$, we have $\mu(\mathbf{B})>\mu(\mathbf{A}_{r_0})$.

Let $\{l_i\}_{i=1}^{2^n-1}$ and $\{h_i\}_{i=1}^{2^n-1}$ be any two column vectors of Bernoulli matrix $\mathbf{D}$. Similar to the above derivation process, we have $\Pr\left(\left|\sum_{i=1}^{2^n-1} l_i h_i\right| \geq t\right) < 2\exp\left\{-\frac{(1+2^{n/2+2})^2}{2(2^n-1)}\right\}$ based on the Lemma 4.3 with $p = 2^n - 1$, $t > \frac{1+2^{n/2+2}}{2^n-1}$, and $a = \frac{1}{\sqrt{2^n-1}}$.

Let $w_1(n) = 2\exp\left\{-\frac{(1+2^{n/2+2})^2}{2(2^n-1)}\right\}$. It is easy to obtain that $w_1(n)$ increases as $n$ decreases. Thus, we have $w_1(n) \leq w_1(6) \approx 2\exp(-8.6429)$. Further, we have

$$\Pr\left(\left|\sum_{i=1}^{2^n-1} l_i h_i\right| \geq t\right) < w_1(6) \approx 2\exp(-8.6429), \tag{21}$$

and

$$\Pr\left(\min_{\{l_i\},\{h_i\}}\left|\sum_{i=1}^{2^n-1} l_i h_i\right| \geq t\right) < \{w_1(6)\}^{2^n(2^{n+1}-1)} \approx \{2\exp(-8.6429)\}^{2^n(2^{n+1}-1)}. \tag{22}$$

Let $\delta_d(n) = \{2\exp(-8.6429)\}^{2^n(2^{n+1}-1)}$ with $n \geq 6$. Obviously, we can obtain that

$$\Pr\left(\min_{\{l_i\},\{h_i\}}\left|\sum_{i=1}^{2^n-1} l_i h_i\right| \leq t\right) \geq 1 - \delta_d(n) \approx 1. \tag{23}$$

Hence, $\mu(\mathbf{D}) = \max_{\{l_i\},\{h_i\}}\left|\sum_{i=1}^{2^n-1} l_i h_i\right| \geq t$. By $t > \frac{1+2^{n/2+2}}{2^n-1}$, and $\mu(\mathbf{A}_{r_0}) \leq \frac{1+2^{n/2+2}}{2^n-1}$, we have $\mu(\mathbf{D}) > \mu(\mathbf{A}_{r_0})$.

Therefore, the theorem is proved in case of even $n$. Similarly, the same conclusion can be obtained in case of odd $n$. Thus, Theorem 4.2 is proved.

□

***Remark of Theorem 4.2*** For CS matrix, reducing the coherence leads to the reconstruction of original signal with higher accuracy. Theorem 4.2 demonstrates that reconstruction performance of the BSFDBC matrix is superior to its Gaussian and Bernoulli counterparts.

## 5. Simulation and Results

In this section, simulation experiments with sparse signals and image signals are given to investigate the performance of proposed BSFDBC matrices. Here, Gaussian and Bernoulli random matrices of same size are used for comparison. In Gaussian matrix construction, each element obeys standard normal distribution $N(0,1)$. In Bernoulli matrix construction, each element is 1 or -1 with equal probability.

For sparse signals, two types of BSFDBC matrices of size $(2^n-1)\times 2^{n+1}$ are generated with initial state $r_0$: (i) BSFDBC matrices of size $255\times 512$ for even $n$ and $n = 8$; (ii) BSFDBC matrices of size $127\times 256$ for odd $n$ and $n = 7$. The $k$-sparse $2^{n+1}\times 1$ original signal $\mathbf{x}$ is

generated by first selecting $k$ nonzero locations uniformly randomly among the total $2^{n+1}$ locations and then taking corresponding $k$ nonzero values by independent and identically distributed standard normal distribution $N(0,1)$. For each sparsity level $k$, 1000 experiments are averaged to obtain the corresponding result. Suppose $\mathbf{x}_R$ is the reconstructed signal from OMP. For noiseless signal recovery, if $\|\mathbf{x}-\mathbf{x}_R\|_2 < 10^{-6}$ satisfies in one experiment, this reconstruction experiment is claimed to be successful. The successful reconstruction probability equals the successful reconstruction times divided by 1000. For noisy signal recovery, additive Gaussian noise $\mathbf{e}$ is added to the original sparse signal $\mathbf{x}$, where the signal-to-noise ratio (SNR) can be set. Therefore, given a sensing matrix $\mathbf{A}$, we have the measurement vector $\mathbf{y} = \mathbf{A}(\mathbf{x}+\mathbf{e}) = \mathbf{A}\mathbf{x} + \mathbf{A}\mathbf{e}$, where $\mathbf{A}\mathbf{e}$ is the noise term. The reconstruction SNR is defined as

$$SNR(\mathbf{x}) = 20 \cdot \log_{10}\left(\frac{\|\mathbf{x}\|_2}{\|\mathbf{x}-\mathbf{x}_R\|_2}\right) dB. \tag{24}$$

For image signals $\mathbf{x}$ of size $m \times n$, the performance of BSFDBC matrix $\mathbf{A}_{r_0}$ is investigated in image reconstruction using the block CS algorithm. The image $\mathbf{I}$ is divided into smaller subimage set $\{\mathbf{I}_l \,|\, l = 1,2,\cdots,N\}$ of equal size. For each subimage $\mathbf{I}_l$, the sparse vector $\mathbf{d}_l$ is obtained by the vectorized version of $\mathbf{s}_l$, which is the two-dimensional Daubechies 9/7 discrete wavelet transform (DWT) of $\mathbf{I}_l$. By using all the wavelet coefficients of $\mathbf{d}_l$, the dimensionality of the reconstruction problem can be determined. A down-sampling for $\mathbf{d}_l$ is implemented to get the compressed measurements $\mathbf{y}_l = \mathbf{A}_{r_0}\mathbf{d}_l$. For image reconstruction, OMP algorithm is used to recover $\mathbf{d}_l$ (and consequently $\mathbf{I}_l$) from the reduced vector $\mathbf{y}_l$. Considering the tradeoff among reconstruction quality, hardware implementation and recovery time, the block size are selected to be $32 \times 16$ and $32 \times 32$, which correspond to two types of BSFDBC matrices. Let $\mathbf{x}_R$ be the reconstructed image. The peak signal-to-noise ratio (PSNR) is defined as

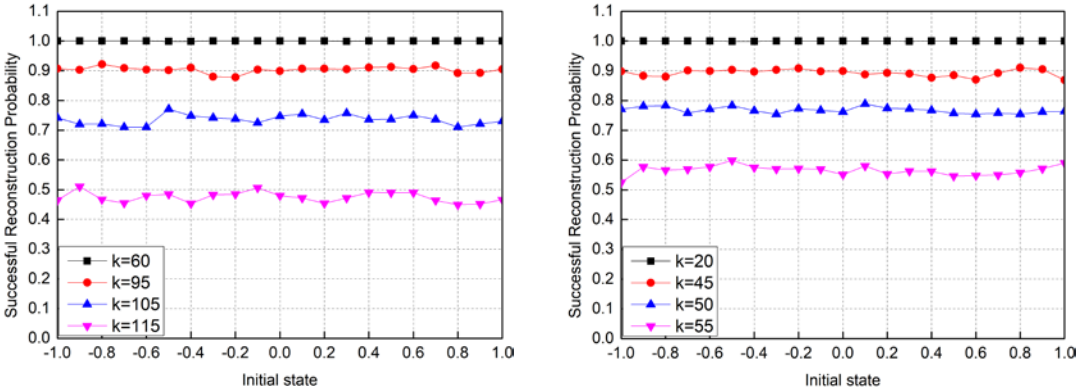
$$PSNR(\mathbf{x}) = 10 \cdot \log_{10}\left(\frac{255^2}{\|\mathbf{x}-\mathbf{x}_R\|_2^2/(m \cdot n)}\right) dB. \tag{25}$$

Note that if the original image $\mathbf{x}$ is a three-dimensional color image, the signal $\mathbf{x}$ is first converted to be a two-dimensional grayscale image signal $\mathbf{x}^F$ by concatenating its R, G, B components in column extension form and then the resulting signal $\mathbf{x}^F$ and corresponding reconstruction signal $\mathbf{x}_R^F$ are applied to calculate $PSNR(\mathbf{x})$.

### 5.1 BSFDBC in Different Initial States

For matrices of size $255 \times 512$, **Fig. 1(a)** presents the successful reconstruction probability of noiseless $k$ -sparse $512 \times 1$ signals under different initial states $r_0$, where $k \in \{60,95,105,115\}$, and $-1 \le r_0 \le 1$. For matrices of size $127 \times 256$, **Fig. 1(b)** presents the successful reconstruction probability of noiseless $k$ -sparse $256 \times 1$ signals under different initial states $r_0$, where $k \in \{20,45,50,55\}$, and $-1 \le r_0 \le 1$.

**Fig. 1** shows that for all values of sparsity level, the initial state of the BSFDBC has limited influence on the recovery accuracy. For instance, for matrices of size $255\times512$, the associated successful reconstruction probabilities at sparsity 105 vary in a limited range $[0.71,0.757]$. This result is due to the insensitivity of coherence of BSFDBC matrix to its initial state.




**(a)** **(b)**

**Fig. 1.** The successful reconstruction probability versus initial state for noiseless sparse signals where sparsity level varies. **(a)** The matrices of size $255\times512$, **(b)** The matrices of size $127\times256$

### 5.2 Key Sensitivity of BSFDBC

As described in Section 3, the BSFDBC matrix $\mathbf{A}_{r_0}$ is constructed based on BSF and Chebyshev chaotic sequence with secret key $r_0=0.8$. The matrix $\mathbf{A}_{r_0}$ can be used as encryption key for cryptography, which implies that encryption occurs implicitly in the data sampling stage. As for the signal recovery, consider the matrix $\mathbf{A}_{r_0}$ generated by the right key $r_0=0.8$ and $\mathbf{A}_{r_1}$ generated by the wrong key $r_1$. The test image is the "liftingbody" of size $512\times512$ shown in **Fig. 2(a)**, where the block size is selected to be $32\times16$. **Fig. 2(b)** and **Fig. 2(c)** are the decrypted image with wrong keys $r_1=0.3$ and $r_1=$-$0.8$, respectively. **Fig. 2(d)** is the decrypted image with right key $r_0=0.8$. The according reconstruction PSNR for **Fig. 2(b)**, **Fig. 2(c)** and **Fig. 2(d)** are 2.01dB, 2.14dB and 36.48dB, respectively. Obviously, the encrypted image cannot be decrypted correctly with wrong key $r_1$. **Fig. 3** presents the reconstruction PSNR for the "liftingbody" decrypted with different key $r_1$, where $-1\le r_1\le1$.

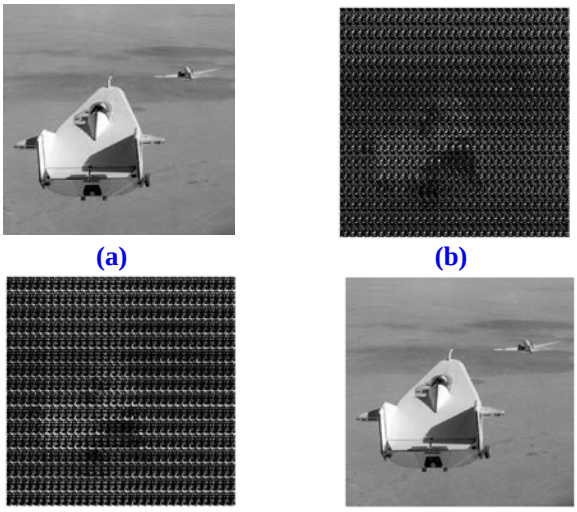



**Fig. 2.** Performance of BSFDBC for "liftingbody". **(a)** Original image, **(b)** Decrypted image with wrong key 0.3, **(c)** Decrypted image with wrong key -0.8, **(d)** Decrypted image with right key 0.8

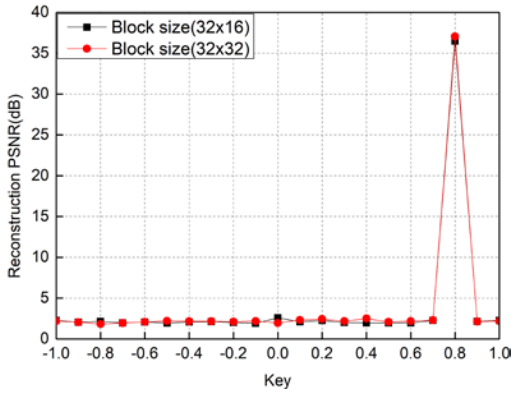



**Fig. 3.** The reconstruction PSNR for the "liftingbody" decrypted with different key

**Fig. 3** shows that the image signal cannot be decrypted correctly with wrong key $r_1 \neq r_0$. Therefore, the BSFDBC $\mathbf{A}_{r_0}$ is sensitive to the secret key $r_0$ and data security can be ensured effectively.

### 5.3 BSFDBC for Sparse Signals

Without loss of generality, the initial state of BSFDBC matrix is set to be 0.8 in this section and later one.

***Example 1:*** For matrices of size $255\times512$, **Fig. 4(a)** presents the successful reconstruction probability of noiseless $k$-sparse $512\times1$ signals under different sparsity levels, where $30\le k\le150$. For matrices of size $127\times256$, **Fig. 4(b)** presents the successful reconstruction probability of noiseless $k$-sparse $256\times1$ signals under different sparsity levels, where $10\le k\le80$.

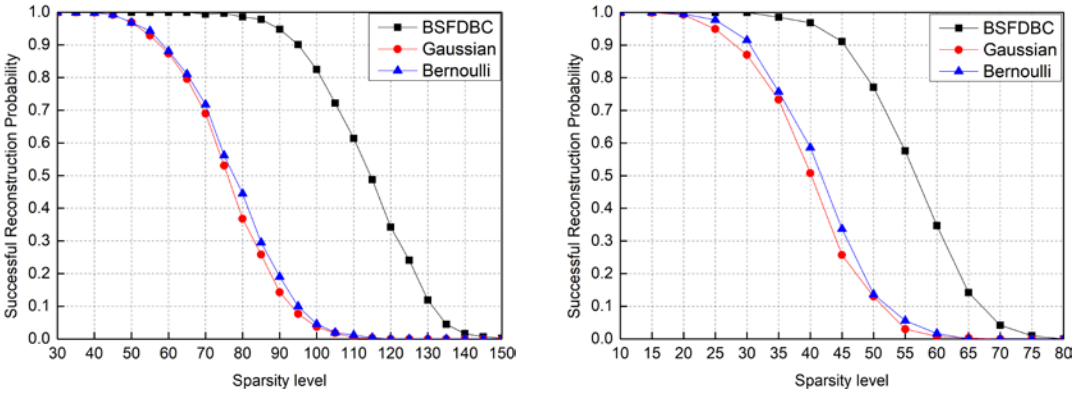



**Fig. 4.** The successful reconstruction probability versus sparsity level for noiseless sparse signals. **(a)** The matrices of size $255\times512$, **(b)** The matrices of size $127\times256$

**Fig. 4** shows that the reconstruction performance of BSFDBC matrix is superior to its Gaussian and Bernoulli counterparts. For instance, for the BSFDBC, Gaussian and Bernoulli matrices of size $255\times512$, the associated successful reconstruction probabilities at sparsity 70 are 0.994, 0.69, and 0.718, respectively. This result is due to the smaller coherence provided by BSFDBC matrix than the other two.

***Example 2:*** In this example, the 30dB noise level is added to the original sparse signal. For matrices of size $255\times512$, **Fig. 5(a)** presents the reconstruction SNR of noisy $k$-sparse $512\times1$ signals under different sparsity levels, where $30\le k\le150$. For matrices of size $127\times256$, **Fig. 5(b)** presents the reconstruction SNR of noisy $k$-sparse $256\times1$ signals under different sparsity levels, where $10\le k\le80$ .

**Fig. 5** shows that for all values of sparsity level, the BSFDBC matrix has more SNR than the Gaussian and Bernoulli matrices. For instance, for the BSFDBC, Gaussian and Bernoulli matrices of size $255\times512$, the associated reconstruction SNRs at sparsity 70 are 32.98 dB, 31.34 dB and 31.34 dB, respectively. This is because that the BSFDBC matrix has smaller coherence than the other two, which is more conducive to signal recovery.

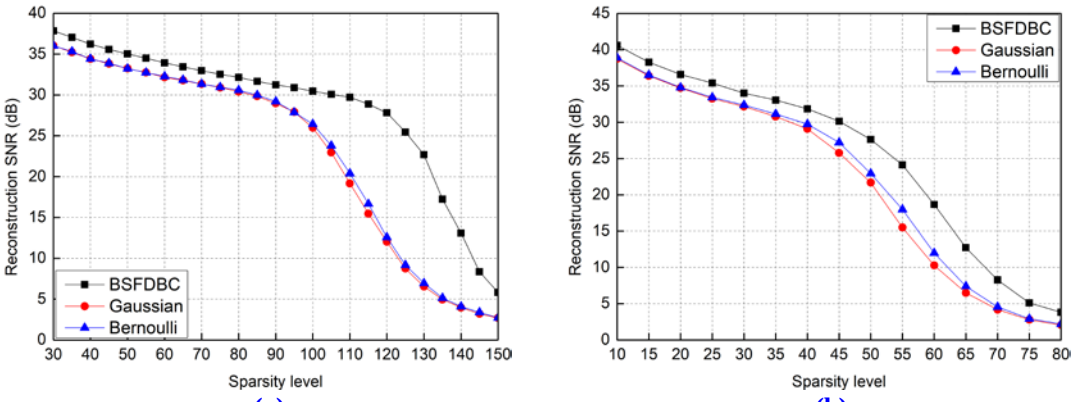



**Fig. 5.** The reconstruction SNR versus sparsity level for noisy sparse signals with SNR of 30 dB. **(a)** The matrices of size $255\times512$, **(b)** The matrices of size $127\times256$

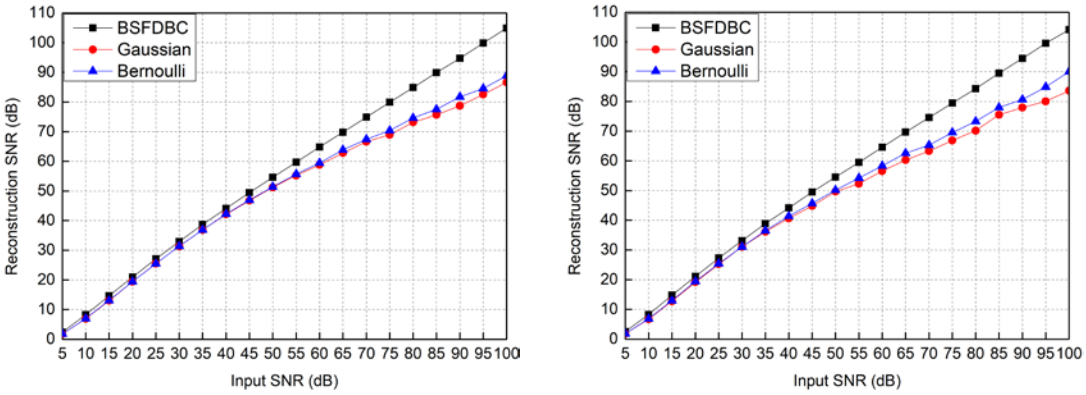



**Fig. 6.** The reconstruction SNR versus input SNR for noisy sparse signals. **(a)** The matrices of size $255\times512$, **(b)** The matrices of size $127\times256$

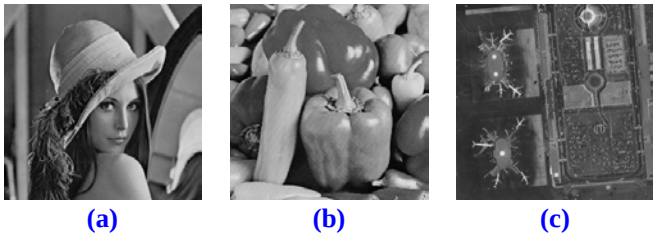
***Example 3:*** In this example, the sparsity level of original signal is fixed and its noise level varies. For matrices of size $255\times512$, **Fig. 6(a)** presents the reconstruction SNR of noisy 70-sparse $512\times1$ signals under different noise levels. For matrices of size $127\times256$, **Fig. 6(b)** presents the reconstruction SNR of noisy 35-sparse $256\times1$ signals under different noise levels.

**Fig. 6** shows that the BSFDBC matrix gives higher reconstruction SNR than the corresponding Gaussian and Bernoulli matrices in different noise levels. Here, we provide some experiment results via the BSFDBC, Gaussian and Bernoulli matrices of size $255\times512$. When the input SNR is 50dB, the associated reconstruction SNRs are 54.62 dB, 51.25 dB and 51.41 dB, respectively.

From above three examples, it can be found that the BSFDBC matrices give better recovery performance than their Gaussian and Bernoulli counterparts in noiseless and noisy scenarios.

### 5.4 BSFDBC for Image Signals

As shown in **Fig. 7**, the test images include three grayscale images and three color images. The three grayscale images are "lena" of size $256\times256$, "peppers" of size $256\times256$ and "airport" of size $1024\times1024$, while the three color images are "Earth" of size $512\times512\times3$, "airplane" of size $512\times512\times3$ and "bone" of size $675\times653\times3$. **Table 1** presents the reconstruction PSNR for different test images with block size $32\times16$ and $32\times32$.



**(d)** **(e)** **(f)**

**Fig. 7.** Test images. **(a)** Lena, **(b)** Peppers, **(c)** Airport, **(d)** Earth, **(e)** Airplane, **(f)** Bone

**Table 1.** The reconstruction PSNR (dB) for different test images with block size $32\times16$ and $32\times32$

| **Matrices** | **BSFDBC** | | **Gaussian** | | **Bernoulli** | |
|---|---|---|---|---|---|---|
| Block size | $32\times16$ | $32\times32$ | $32\times16$ | $32\times32$ | $32\times16$ | $32\times32$ |
| Lena | 27.87 | 28.28 | 26.40 | 27.34 | 26.43 | 27.36 |
| Peppers | 29.35 | 30.18 | 28.28 | 29.01 | 28.28 | 28.95 |
| Airport | 26.84 | 27.17 | 26.00 | 26.24 | 25.96 | 26.29 |
| Earth | 30.56 | 30.84 | 29.73 | 30.01 | 29.71 | 29.97 |
| Airplane | 31.34 | 31.85 | 30.03 | 30.62 | 30.15 | 30.76 |
| Bone | 31.02 | 32.12 | 29.88 | 31.19 | 29.48 | 31.39 |

From **Table 1**, it is observed that for all test images, the BSFDBC matrix has more reconstruction PSNR than the Gaussian and Bernoulli matrices. In addition, the reconstruction PSNR increases as the block size.

Simulation experiments with sparse signals and image signals show that the reconstruction performance of BSFDBC matrices is superior to their Gaussian and Bernoulli counterparts, which is coincide with the conclusion of Theorem 4.2. Consequently, inspired from BSF and Chebyshev chaotic sequence, the designed BSFDBC matrices possess the characteristics of easy hardware implementation, good sensing performance and good cryptographic property. These characteristics can make the proposed matrices applied to practical CS applications, such as sparse signal restore, image block CS and image encryption.

## 6. Conclusion

On the basis of BSF and Chebyshev chaotic sequence, this paper constructs a class of deterministic bipolar measurement matrices named BSFDBC and gives related example. The coherence of proposed BSFDBC matrices is investigated and derived theoretically to be smaller than the corresponding Gaussian and Bernoulli random matrices. Simulation experiments with sparse signals and image signals show that the proposed BSFDBC matrix is sensitive to its initial state, has limited influence on the recovery accuracy in different initial states and it outperforms its Gaussian and Bernoulli counterparts in recovery accuracy. The BSFDBC matrices possess the characteristics of easy hardware implementation, good sensing performance and good cryptographic property, which is conducive to practical CS.

## References


[1] Emmanuel J. Candès, Justin Romberg and Terence Tao, "Robust uncertainty principles: exact signal reconstruction from highly incomplete frequency information," *IEEE Transactions on Information Theory*, vol. 52, no. 2, pp. 489-509, February, 2006. Article (CrossRef Link)

[2] David L. Donoho, "Compressed sensing," *IEEE Transactions on Information Theory*, vol. 52, no. 4, pp. 1289-1306, April, 2006. Article (CrossRef Link)

[3] Shuai Liu, Weiling Bai, Gaocheng Liu, Wenhui Li and Hari M. Srivastava, "Parallel fractal compression method for big video data," *Complexity*, vol. 2018, pp. 1-16, October, 2018. Article (CrossRef Link)

[4] Gaocheng Liu, Shuai Liu, Khan Muhammad, Arun Kumar Sangaiah and Faiyaz Doctor, "Object tracking in vary lighting conditions for fog based intelligent surveillance of public spaces," *IEEE Access*, vol. 6, pp. 29283-29296, May, 2018. Article (CrossRef Link)

[5] Zheng Pan, Shuai Liu, Arun Kumar Sangaiah and Khan Muhammad, "Visual attention feature (VAF): a novel strategy for visual tracking based on cloud platform in intelligent surveillance systems," *Journal of Parallel and Distributed Computing*, vol. 120, pp. 182-194, October, 2018. Article (CrossRef Link)

[6] Emmanuel J. Candès and Terence Tao, "Decoding by linear programming," *IEEE Transactions on Information Theory*, vol. 51, no. 12, pp. 4203-4215, December, 2005. Article (CrossRef Link)

[7] Scott Shaobing Chen, David L. Donoho and Michael A. Saunders, "Atomic decomposition by basis pursuit," *SIAM Journal on Scientific Computing*, vol. 20, no. 1, pp. 33-61, August, 1998. Article (CrossRef Link)

[8] Joel A. Tropp, "Greed is good: Algorithmic results for sparse approximation," *IEEE Transactions on Information Theory*, vol. 50, no. 10, pp. 2231-2242, October, 2004. Article (CrossRef Link)

[9] R. Ramu Naidu, Phanindra Jampana and C. S. Sastry, "Deterministic compressed sensing matrices: construction via Euler Squares and applications," *IEEE Transactions on Signal Processing*, vol. 64, no. 14, pp. 3566-3575, July, 2016. Article (CrossRef Link)

[10] R. Ramu Naidu and Chandra R. Murthy, "Construction of binary sensing matrices using extremal set theory," *IEEE Signal Processing Letters*, vol. 24, no. 2, pp. 211-215, February, 2017. Article (CrossRef Link)

[11] Pradip Sasmal, R. Ramu Naidu, Challa S. Sastry and Phanindra Jampana, "Composition of binary compressed sensing matrices," *IEEE Signal Processing Letters*, vol. 23, no.8, pp. 1096-1100, August, 2016. Article (CrossRef Link)

[12] Shuxing Li and Gennian Ge, "Deterministic sensing matrices arising from near orthogonal systems," *IEEE Transactions on Information Theory*, vol. 60, no. 4, pp. 2291-2302, April, 2014. Article (CrossRef Link)

[13] Jun Zhang, Guojun Han and Yi Fang, "Deterministic construction of compressed sensing matrices from protograph LDPC codes," *IEEE Signal Processing Letters*, vol. 22, no. 11, pp. 1960-1964, November, 2015. Article (CrossRef Link)

[14] Mohammad Fardad, Sayed Masoud Sayedi and Ehsan Yazdian, "A low-complexity hardware for deterministic compressive sensing reconstruction," *IEEE Transactions on Circuits and Systems I: Regular Papers*, vol. 65, no. 10, pp. 3349-3361, October, 2018. Article (CrossRef Link)

[15] Jin-Wei Jhang and Yuan-hao Huang, "A high-SNR projection-based atom selection OMP processor for compressive sensing," *IEEE Transactions on Very Large Scale Integration (VLSI) Systems*, vol. 24, no. 12, pp. 3477-3488, December, 2016. Article (CrossRef Link)

[16] Hongping Gan, Zhi Li, Jian Li, Xi Wang and Zhengfu Cheng, "Compressive sensing using chaotic sequence based on chebyshev map," *Nonlinear Dynamics*, vol. 78, no. 4, pp. 2429-2438, December, 2014. Article (CrossRef Link)

[17] Juan Castorena and Charles D. Creusere, "The restricted isometry property for banded random matrices," *IEEE Transactions on Signal Processing*, vol. 62, no. 19, pp. 5073-5084, October, 2014. Article (CrossRef Link)

[18] Hongping Gan, Song Xiao and Yimin Zhao, "A novel secure data transmission scheme using chaotic compressed sensing," *IEEE Access*, vol. 6, pp. 4587-4598, February, 2018. Article (CrossRef Link)
[19] Mahsa Lotfi and Mathukumalli Vidyasagar, "A fast noniterative algorithm for compressive sensing using binary measurement matrices," *IEEE Transactions on Signal Processing*, vol. 66, no. 15, pp. 4079-4089, May, 2018. Article (CrossRef Link)
[20] Li Zeng, Xiongwei Zhang, Liang Chen, Tieyong Cao and Jibin Yang, "Deterministic construction of toeplitzed structurally chaotic matrix for compressed sensing," *Circuits, Systems, and Signal Processing*, vol. 34, no. 3, pp. 797-813, March, 2015. Article (CrossRef Link)
[21] Hongping Gan, Song Xiao, Yimin Zhao and Xiao Xue, "Construction of efficient and structural chaotic sensing matrix for compressive sensing," *Signal Processing: Image Communication*, vol. 68, pp. 129-137, October, 2018. Article (CrossRef Link)
[22] Hongping Gan, Song Xiao and Yimin Zhao, "A large class of chaotic sensing matrices for compressed sensing," *Signal Processing*, vol. 149, pp. 193-203, August, 2018. Article (CrossRef Link)
[23] Guohua Zhang, Rudolf Mathar and Quan Zhou, "Deterministic bipolar measurement matrices with flexible sizes from Legendre sequence," *Electronics Letters*, vol. 52, no. 11, pp. 928-930, May, 2016. Article (CrossRef Link)
[24] Gang Wang, Min-Yao Niu and Fang-Wei Fu, "Deterministic constructions of compressed sensing matrices based on optimal codebooks and codes," *Applied Mathematics and Computation*, vol. 343, pp. 128-136, February, 2019. Article (CrossRef Link)
[25] Weizhi Lu, Tao Dai and Shu-Tao Xia, "Binary matrices for compressed sensing," *IEEE Transactions on Signal Processing*, vol. 66, no. 1, pp. 77-85, January, 2018. Article (CrossRef Link)
[26] Liu Haiqiang, Yin Jihang, Hua Gang, Yin Hongsheng and Zhu Aichun, "Deterministic construction of measurement matrices based on Bose balanced incomplete block designs," *IEEE Access*, vol. 6, pp. 21710-21718, April, 2018. Article (CrossRef Link)
[27] Tian Shujuan, Fan Xiaoping, Li Zhetao, Pan Tian, Choi Youngjune and Sekiya Hiroo, "Orthogonal-gradient measurement matrix construction algorithm," *Chinese Journal of Electronics*, vol. 25, no. 1, pp. 81-87, January, 2016. Article (CrossRef Link)
[28] Haiyang Liu, Hao Zhang and Lianrong Ma, "On the spark of binary LDPC measurement matrices from complete protographs," *IEEE Signal Processing Letters*, vol. 24, no. 11, pp. 1616-1620, November, 2017. Article (CrossRef Link)
[29] Jue Wang, Zhaoyang Zhang, Xianbin Wang, Hong Wang and Chunxu Jiao, "A low-complexity reconstruction algorithm for compressed sensing using Reed-Muller sequences," in *Proc. of IEEE Int. Conf. on Communications*, pp. 1-6, May 20-24, 2018. Article (CrossRef Link)
[30] Sung-Hsien Hsieh, Chun-Shien Lu and Soo-Chang Pei, "Compressive sensing matrix design for fast encoding and decoding via sparse FFT," *IEEE Signal Processing Letters*, vol. 25, no. 4, pp. 591-595, April, 2018. Article (CrossRef Link)
[31] Nam Yul Yu and Guang Gong, "A new binary sequence family with low correlation and large size," *IEEE Transactions on Information Theory*, vol. 52, no. 4, pp. 1624-1636, April, 2006. Article (CrossRef Link)
[32] Yan Tang, Guonian Lv and Kuixi Yin, "Deterministic sensing matrices based on multidimensional pseudo-random sequences," *Circuits, Systems, and Signal Processing*, vol. 33, no. 5, pp. 1597-1610, May, 2014. Article (CrossRef Link)
[33] Jarvis Haupt, Waheed U. Bajwa, Gil Raz and Robert Nowak, "Toeplitz compressed sensing matrices with applications to sparse channel estimation," *IEEE Transactions on Information Theory*, vol. 56, no. 11, pp. 5862-5875, November, 2010. Article (CrossRef Link)

**Cunbo Lu** is currently a postdoctoral researcher of Beijing Institute of Applied Physics and Computational Mathematics. He received his Bachelor degree from PLA Information Engineering University, Zhengzhou, China and his Ph.D. degree from Xidian University, Xi'an, China. His research interests include network coding, wireless network, image processing and compressed sensing.

**Wengu Chen** received the Ph.D. degree from Beijing Normal University in 1996 in mathematics. He is currently a professor of Beijing Institute of Applied Physics and Computational Mathematics. His research interests include harmonic analysis, channel coding, and compressive sensing.

**Haibo Xu** received the Ph.D. degree from Graduate School of China Academy of Engineering physics. He is currently a professor of Beijing Institute of Applied Physics and Computational Mathematics. His research interests include radiation imaging and image processing.