IET Communications

Research Article

Blind recognition of alpha-stable random carrier signals by an eavesdropper in random communication systems

ISSN 1751-8628
Received on 10th September 2018
Revised 21st April 2019
Accepted on 28th May 2019
E-First on 23rd August 2019
doi: 10.1049/iet-com.2018.5884
www.ietdl.org

Areeb Ahmed[1] ✉, Ferit Acar Savaci[1]
[1]Department of Electrical and Electronic Engineering, Izmir Institute of Technology, Urla 35430, Izmir, Turkey
✉ *E-mail: areebahmed@iyte.com.tr*

Abstract: Invisibility of alpha-stable (α-stable) noise as carrier signals, in the presence of additive white Gaussian noise (AWGN) as channel noise, is a key factor to ensure covert transmission by employing random communication systems (RCSs). This study introduces a novel blind recognition method for an eavesdropper to detect the presence of real-valued symmetric and skewed α-stable random carrier signals in the presence of AWGN. The introduced method is based on the proposed random carrier signal recogniser (RCSR), which consists of fractional lower-order auto-covariance block, threshold control block and the random carrier signal recognition indicator. The proposed RCSR first detects the possible presence of α-stable random carrier signals and then recognises the impulsiveness and skewness parameters, exploited by the transmitter and the intended receiver, to extract covertly conveyed binary information. However, the determined covert range can be adopted to perform secure transmission by RCSs. The simulation results reflect the simplicity of the proposed method as it is capable of performing effectively in real time by utilising extremely less number of observed samples.

1 Introduction

Noise signal detection is a well-studied phenomenon due to its direct or indirect effect on all types of natural or manmade systems. Detection of noise like carrier signals by correlation method to establish secure communication systems started in the 1950's [1]. After the discovery of the first method to synchronise chaos in 1991 [2], many coherent and non-coherent signal detection schemes have been proposed to covertly convey the binary information by utilising noise like chaotic signals as information carriers [3, 4]; which then started a series of investigations related to the chaotic communication systems. However, chaotic communication systems, proposed till now, are only able to hide the information content in the channel, but the eavesdroppers are aware of the existence of communication. Because the security of chaotic communication systems is derived in this manner, many blind and semi-blind signal recognition techniques based on auto-correlation, generalised synchronisation, power analysis and signal filtering have been proposed to completely decode the information content hidden in the noise like chaotic carrier signals [5–7]. The worst part is that the user is never aware of the fact that the utilised carrier signals are being compromised. The drawbacks in noise like chaotic carrier based communication systems established the need to introduce some actual noise based communication systems. Since, using noise signals as a random carrier not only hides the communication content, but also makes the eavesdroppers unaware of its existence, an eavesdropper has no idea whether a meaningful message is being sent or not [8].

Alpha-stable noise, being the generalised version of the Gaussian noise, has the potential to be utilised as a random carrier as it can be invisible in the presence of additive white Gaussian noise (AWGN). The invisibility is more severe when the parameters of the transmitted α-stable random noise carrier are closer to the parameters of the Gaussian noise present in the channel and vice versa. However, detection and parameter estimation of α-stable random noise signals is considered to be a challenging problem in signal processing due to common characteristic properties of all heavy-tailed stable distributions which are (i) the non-existence of finite second or higher-order moments; (ii) relatively high probabilities of large deviations from the median [9]. Moreover, α-stable noise signal waveform contains no repetitions or periodicities, so the pulse length is also hidden, which makes it a natural candidate for secure communication. Therefore, many signal processing methods have been proposed in the past to estimate the related parameters of α-stable noise signals [10–13] or to model and estimate the number of α-stable distributions in mixture distributions [14, 15] but utilising them to perform covert transmission requires a priori knowledge of the utilised carrier signals. Therefore, the idea to use α-stable noise as a random carrier to covertly convey the binary information has an extra physical layer of security during transmission; which reduces the risk of eavesdropping.

This fact gave birth to symmetric and skewed α-stable random noise based binary communication systems, i.e. random communication systems (RCSs) [16, 17]. Different receiver design, signal detection and estimation schemes have also been utilised to increase the efficiency of RCSs; where it has also been analysed that RCSs can perform covert transmission in fading channels as well [18–20]. However, the most optimised model of RCS has been introduced recently followed by the first criterion to quantify the covertness of α-stable noise based communication systems where the effect of imperfect synchronisation on the performance of an eavesdropper has also been studied [21, 22]**.** All studies related to RCSs have already assumed perfect synchronisation; where no exact method was presented until the introduction of synchronised RCSs [23]. The security of RCSs is derived from the facts that (i) α-stable mixtures can be separated by the Bayesian techniques presented in [14, 15], but since the size of the cluster cannot be estimated therefore α-stable random noise signals are undetectable or invisible to an eavesdropper; (ii) the pulse length, i.e. duration of the carrier signal holding single binary information bit, needed for decoding is also hidden. These facts make it extremely difficult for an eavesdropper to blindly recognise and estimate the related parameter of α-stable carrier signals to retrieve the transmitted binary information.

In this paper, the first blind detection, recognition and data extraction method for α-stable carrier signals have been proposed and analysed from the perspective of an eavesdropper; where detection means to judge the possible presence of the carrier signals during real-time data reception in AWGN; signal recognition means to correctly recognise the associated parameters of *α*-stable carrier signals and data extraction means to extract the hidden binary information from the associated parameters by applying the hard decision rule. The technique related to detection in the proposed idea is inspired by the auto-correlation based blind recognition method for chaotic carrier signals [5]. Since the second and higher-order statistics do not exist for α-stable distributions, any auto-correlation based blind recognition method is not applicable for blind recognition of α-stable carrier signals. Therefore, in this paper, fractional lower-order covariance (FLOC) has been utilised to propose the first random carrier signal recogniser (RCSR) which follows the three-step procedure to detect and recognise α-stable carrier signals and then extract the hidden binary information in real time. In Section 2, paper, alpha-stable distributions, FLOC method and auto-correlation based blind recognition method for chaotic carrier signals have been briefly reviewed. In Section 3, the proposed three-step procedure based on the introduced fractional lower-order auto-covariance block (FLOACB), threshold control block (TCB) and random carrier signal recognition indicator (RCSRI) has been explained. The results are shown in Section 4, which is followed by conclusive remarks in Section 5.

2 Prior art

In this section, the utilised α-stable distribution and the method to correlate alpha-stable noise signals have been briefly explained. Later on, the auto-correlation based blind recognition method for chaotic carrier signals which have inspired us to propose the first blind recognition method for α-stable carrier signals has also been reviewed in this section.

2.1 Alpha-stable noise signals

Alpha-stable signals can be generated by utilising the characteristic function of α-stable noise 'X', i.e. $X \sim S_\alpha\,(\beta,\ \gamma, \mu)$, given in [24] as

$$\phi(\theta) = \begin{cases} \exp\left\{ \mathrm{j}\mu\theta - \gamma^\alpha |\theta|^\alpha \left(1 - \mathrm{j}\beta \operatorname{sign}(\theta) \tan\left(\frac{\alpha\pi}{2}\right)\right)\right\} & \text{if } \alpha \neq 1 \\ \exp\left\{ \mathrm{j}\mu\theta - \gamma|\theta| \left(1 + \mathrm{j}\beta\frac{2}{\pi} \operatorname{sign}(\theta) \ln\left(\frac{\alpha\pi}{2}\right)\right)\right\} & \text{if } \alpha = 1 \end{cases} \quad (1)$$

where $\alpha(0 < \alpha \leq 2)$ is the characteristic exponent, $\beta(-1 \leq \beta \leq 1)$ is the skewness parameter, $\gamma(\gamma \geq 0)$ is the dispersion parameter and $\mu \in R$ is the location parameter.

Remark 1: Gaussian distribution is the special case of α-stable distributions defined as $X \sim S_{\alpha=2}\,(\beta = 0, \gamma, \mu)$.

The second or higher-order moments do not exist for $\alpha < 2$. Moreover, the first-order moment does not exist as well for $\alpha \leq 1$ [24]. The procedure to generate α-stable signals has been adopted from [25].

2.2 Fractional lower-order covariance

FLOC is the method to correlate α-stable signals. The FLOC between G pairs of observations $\{x_m[1], \ldots, x_m[G]\}$ for α-stable random noise signals $X_m = 1, 2$ is defined in [10] as

$$\boldsymbol{R_d}[\boldsymbol{k}] \triangleq E\{(x_1[i])^a \cdot (x_2[i+k])^b\} \quad (2)$$

for $0 \leq a < \alpha/2$ and $0 \leq b < \alpha/2$.

The estimated FLOC represented interchangeably by '$\hat{\boldsymbol{R}}_{\boldsymbol{d}}[\boldsymbol{k}]$' or '$\hat{\boldsymbol{R}}_{X_1X_2}[\boldsymbol{k}]$' is computed in [10] as

$$\hat{\boldsymbol{R}}_{\boldsymbol{d}}[\boldsymbol{k}] = \hat{\boldsymbol{R}}_{X_1X_2}[\boldsymbol{k}] = \frac{\sum_{i=L_1+1}^{L_2} \left|x_1[i]\right|^a \cdot \left|x_2[i+k]\right|^b \cdot \operatorname{sign}(x_1[i] \cdot x_2[i+k])}{L_2 - L_1} \quad (3)$$

where $L_1 = \max\{0, -k\}, L_2 = \min\{G - k, G\}$.

2.3 Blind recognition of chaotic carrier signals by auto-correlation function

Chaotic carrier signals do not possess the capability to become invisible in AWGN hence their existence can always be revealed by an eavesdropper. This weak link resulted in many signal processing techniques which can retrieve the information from chaotic carrier signals [5–7]; where auto-correlation based blind recognition technique is one of the first and simplest among them [5]. The first step of the method is to recognise the type of specific system used to generate noise like chaotic carrier signals. It can be done after producing a thumbprint of the utilised chaotic system in the following ways: (i) by finding the specific strange chaotic attractor from the signal iteration plot; which is a plot of a signal with a delayed version of itself (see Figs. 1 and 2 in [5]); (ii) or by plotting the auto-correlation function of the time series; where every chaotic system has a unique auto-correlation plot (see Fig. 3 in [5]). Then the comparison of the produced thumbprint with already compiled a library of plots can recognise the type of the utilised chaotic system.

After the recognition of the specific chaotic system, in the second step, the eavesdropper can extract the hidden binary information by generating the mimicked inverse system. The parameters of the inverse system can then be optimised to minimise the output and thus separate the chaotic signal and underlying binary information (see Fig. 9 in [5]). Although there are advanced techniques available in [6, 7], the simple two-step signal processing technique given in [5] is sufficient for an eavesdropper to bring down the security of chaotic communication systems.

3 Blind recognition of α-stable carrier signals by fractional lower-order auto-covariance

In comparison to the two-step, i.e. recognition and extraction method, discussed above for blind recognition of chaotic carrier signals, α-stable carrier signals require one extra step which is to first detect the possible presence of α-stable carrier signals in the channel. Afterwards, the type or associated parameter of α-stable carrier signals should be recognised, which should be followed by the extraction of the binary information as the last step. Following the above-prepared guidelines, blind recognition technique for α-stable carrier signals has been explained in this section. The three steps, i.e. detection, recognition and extraction by an eavesdropper, can be achieved by the proposed RCSR. Before discussing the system model, two important concepts, utilised to establish the RCSR, have been given in Sections 3.1 and 3.2.

3.1 FLOAC of α-stable noise signals

The FLOAC of α-stable random noise signal X can be defined as

$$\boldsymbol{R_d}[\boldsymbol{k}] \triangleq E\{(x[i])^a \cdot (x[i+k])^b\} \quad (4)$$

for $0 \leq a < \alpha/2$ and $0 \leq \beta < \alpha/2$.

Similarly, the estimated FLOAC of X can be computed as

$$\hat{\boldsymbol{R}}_{\boldsymbol{d}}[\boldsymbol{k}] = \hat{\boldsymbol{R}}_{\boldsymbol{XX}}[\boldsymbol{k}] = \frac{\sum_{i=L_1+1}^{L_2} |x[i]|^a \cdot |x[i+k]|^b \cdot \operatorname{sign}(x[i] \cdot x[i+k])}{L_2 - L_1} \quad (5)$$

The non-delayed FLOAC value, i.e. $\hat{\boldsymbol{R}}_{\boldsymbol{d}}[0]$ or $\hat{\boldsymbol{R}}_{\boldsymbol{XX}}[0]$, of α-stable random noise signal X has significant importance. It has played a key role in establishing pilot-assisted synchronisation for RCSs as it provides the capability to differentiate between the requisite pilot symbol and all other non-requisite pilot symbols by accurately separating the estimated value $\hat{\boldsymbol{R}}_{\boldsymbol{d}}[0]$ and all other estimated $\hat{\boldsymbol{R}}_{\boldsymbol{d}}[\boldsymbol{k}]$ due to the presence of a large difference between them [23]. Moreover, it has also been shown in [26] that the value $\hat{\boldsymbol{R}}_{\boldsymbol{d}}[0]$ of α-stable random noise signal X varies as the associated impulsiveness and skewness parameter of the utilised X are varied.

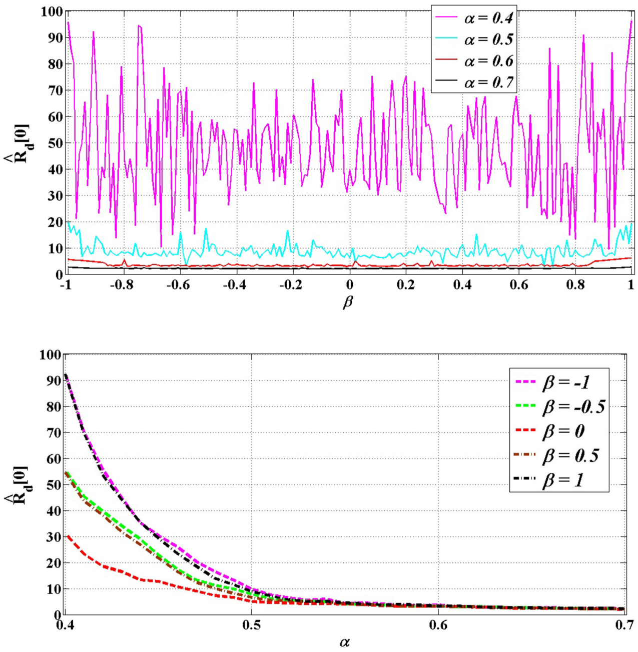

Fig. 1 *Non-delayed FLOAC '$\hat{\boldsymbol{R}}_d[0]$ or $\hat{\boldsymbol{R}}_{XX}[0]$' of x $X \sim S_{0.4 \le \alpha \le 0.7}$ ($-1 \le \beta \le 1$, $\gamma = 1$, $\mu = 0$); for different α's (top), for different β's (bottom)*

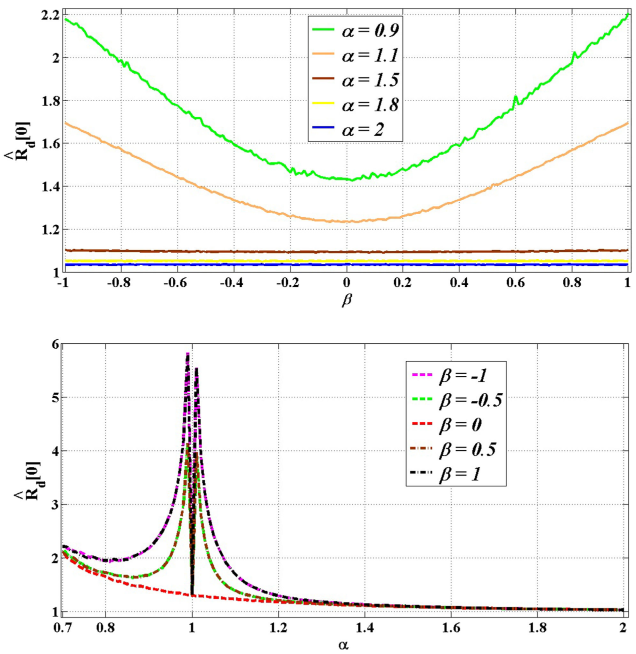

Fig. 2 *Non-delayed FLOAC '$\hat{\boldsymbol{R}}_d[0]$ or $\hat{\boldsymbol{R}}_{XX}[0]$' of $X \sim S_{0.7 \le \alpha \le 2}$ ($-1 \le \beta \le 1$, $\gamma = 1$, $\mu = 0$); for different α's (top), for different β's (bottom)*

The detailed analysis related to non-delayed FLOAC has been presented in Figs. 1 and 2; where it has been observed that $\hat{\boldsymbol{R}}_d[0]$ increases (decreases) if X has been generated with smaller α (larger α), i.e. high impulsiveness (low impulsiveness), and larger $|\beta|$ (smaller absolute β), i.e. β heavily skewed either towards right or left (β not skewed). These observations related to FLOAC of α-stable noise signal X, in [23, 26], have helped to optimise the detection process of synchronised RCSs [27].

3.2 Compiled library of FLOAC matrix

Since, it has been observed in Figs. 1 and 2 that every different value of α and β results in a different and unique value of $\hat{\boldsymbol{R}}_d[0]$, therefore, they can be referred to as $\hat{\boldsymbol{R}}_d[0]_{\alpha\beta}$ or $\hat{\boldsymbol{R}}_{XX}[0]_{\alpha\beta}$. By utilising all possible combinations of α and β, a complete compiled library of $\hat{\boldsymbol{R}}_d[0]_{\alpha\beta}$ has been developed in the form of FLOAC matrix denoted by '$\boldsymbol{F}$' which is defined below:

$$\boldsymbol{F} \triangleq \begin{array}{c} \\ \boldsymbol{\alpha}_1 \\ \vdots \\ \boldsymbol{\alpha}_u \end{array} \begin{array}{c} \begin{array}{ccc} \boldsymbol{\beta}_1 & \cdots & \boldsymbol{\beta}_v \end{array} \\ \left[\begin{array}{ccc} a_{11} & \cdots & a_{1v} \\ \vdots & \ddots & \vdots \\ a_{u1} & \cdots & a_{uv} \end{array}\right]_{u \times v} \end{array} \tag{6}$$

for

$$a_{ij} \triangleq \boldsymbol{R}_d[0]_{\alpha_i \beta_j} \tag{7}$$

where

$$\alpha_i \triangleq i \cdot \Delta\alpha \tag{8}$$

for $i = 1, 2, \dots, u$ and

$$\Delta\alpha \triangleq \frac{2}{u} \tag{9}$$

similarly

$$\beta_j \triangleq \{(j-1) \cdot \Delta\beta\} - 1 \tag{10}$$

for $j = 1, 2, \dots, v$ and

$$\Delta\beta \triangleq \frac{2}{v-1} \tag{11}$$

The complexity and accuracy of the proposed FLOAC matrix '$\boldsymbol{F}$' are directly proportional to its dimensions, i.e. the chosen values of u and v. In this paper, the $\boldsymbol{F}$generated from $u = 20$ and $v = 21$ has been utilised which has also been given in Tables 1 and 2.

3.3 RCS model

The generalised system model of α-stable noise-based RCSs has been considered to evaluate the performance of the proposed blind recognition method for α-stable random carrier signals. The model includes RCSR and its sub-parts, i.e. FLOACB, TCB and RCSRI; where the considered transmitter and the channel noise have been explained first.

3.3.1 Considered transmitter and channel noise: The generalised α-stable noise signal generator has been used as a transmitter where different values of the impulsiveness parameter 'α' and the skewness parameter 'β' can be used to generate α-stable carrier signals which contain covertly conveyed binary information. The transmitter sends α-stable random noise signals X_m where the utilised pulse length 'N', i.e. number of noise samples representing one binary information bit, contains $N = 2000$ samples $\{x_{11}, x_{12}, \dots, x_{1N}\}$. The pulse length N is assumed to be pre-known only to the transmitter and to the intended receiver in RCSs. Since, it has been shown in [22] that if an eavesdropper is aware of the exact pulse length then it is possible to detect and recognise α-stable carrier signals in the presence of AWGN as well as extract the underlying hidden binary information by one of the signal recognition techniques proposed in [10–13]. However, there is no method available which can perform blind recognition, i.e. detection, recognition and extraction, of the α-stable carrier if the pulse length is not known (see Fig. 3).

The AWGN has been considered as the channel noise 'N_G' which can be defined as

$$N_G \sim S_{\alpha=2}(\beta = 0, \gamma_N = 1, \mu = 0) \tag{12}$$

3.3.2 Random carrier signal recogniser: The proposed RCSR requires no a priori knowledge of the α-stable random carrier

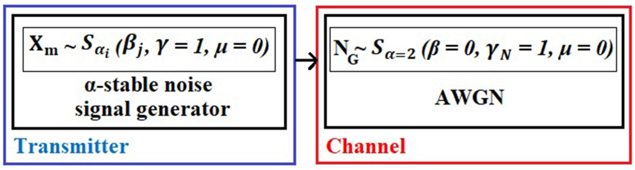

Fig. 3 *System model of the considered transmitter and the channel*

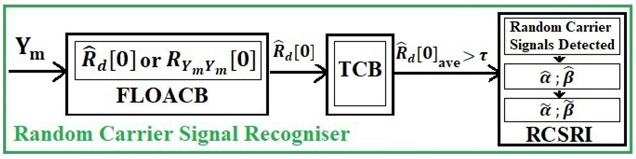

Fig. 4 *Block diagram of the RCSR*

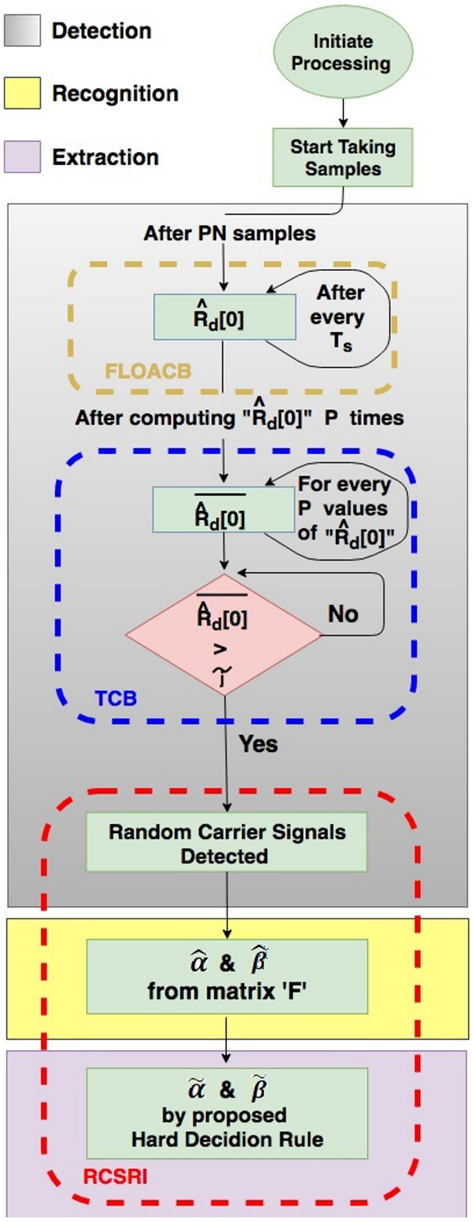

Fig. 5 *Process flow diagram of the RCSR*

signals utilised by the transmitter and the intended receiver for covert transmission. However, in this study, it is assumed that the eavesdropper is perfectly synchronised with the transmitter as a best-case scenario generally followed in [16–23] for implementing RCSs. The RCSR consists of FLOACB, TCB and RCSRI. The α-stable random carrier signals are detected by the combined efforts of FLOACB and TCB. The RCSRI recognises the impulsiveness and the skewness parameters by utilising the introduced compiled library of non-delayed FLOAC values, i.e. FLOAC matrix $\boldsymbol{F}$ in (6), followed by extracting the hidden binary information by using the proposed hard decision rule (see Fig. 4).

The RCSR receives the sequence '$\boldsymbol{Y_m}$' as

$$\boldsymbol{Y_m} = \begin{cases} \boldsymbol{X_m} + N_G, & \text{if random carrier signals are present} \\ N_G, & \text{if random carrier signals are absent} \end{cases} \quad (13)$$

where $\boldsymbol{Y_m}$ is the mixture of α-stable random carrier signals with the AWGN 'N_G' present in the channel, if there is the presence of information bearing α-stable random carrier signals in the channel at that specific time instant, otherwise $\boldsymbol{Y_m}$ is only N_G in the channel. The channel state information is assumed to be known to the RCSR.

An outline of the proposed method has also been explained in the form of process flow graph in Fig. 5. It illustrates all the steps, beginning from the time instant of process initialisation, which is related to α-stable random carrier signals detection, recognition and extraction steps carried out by FLOACB, TCB and RCSRI.

FLOACB: Some part of the first step, i.e. detection by an eavesdropper, has been performed by the proposed FLOACB. The FLOACB starts computing the estimated $\hat{\boldsymbol{R}}_{\boldsymbol{d}}[0]$ or $\hat{\boldsymbol{R}}_{\boldsymbol{Y_mY_m}}[0]$ exactly after accepting N_a samples from the time instant of initialisation, i.e. receiving the first sample of $\boldsymbol{Y_m}$, and this process is then repeated after every T_s duration, i.e. duration between the consecutive samples of $\boldsymbol{Y_m}$; where N_a is the assumed pulse length assumed by an eavesdropper to extract single binary information bit whereas N is the actual pulse length utilised by both the transmitter and the intended receiver. All the methods introduced in the literature whether related to the recognition of α-stable random carrier signals [10–12] or to the RCSs [16–23] has utilised pulse length greater than 500 as it is difficult to utilise pulse length 'N' less than 500 if accurate estimation of the involved α or β is required. However, the eavesdropper has assumed N_a being equal to 100, 200 and 300 as the proposed method does not need an accurate estimation of α and β, it rather depends on the computed intervals of these associated parameters which can be found by utilising the proposed hard decision rule given in the sequel.

TCB: The remaining part of the first step, i.e. detection by an eavesdropper, has been performed by the proposed TCB. Since, the FLOACB starts sending consecutive $\hat{\boldsymbol{R}}_{\boldsymbol{d}}[0]$ values to TCB exactly after accepting N_a samples from the time instant of initialisation, therefore, the TCB also starts computing the average non-delayed FLOAC value, i.e. $\hat{\boldsymbol{R}}_{\boldsymbol{d}}[0]_{\text{ave}}$, according to the criterion defined below:

$$\hat{\boldsymbol{R}}_{\boldsymbol{d}}[0]_{\text{ave}} = \frac{1}{N_a}\sum_{i=1}^{N_a} \hat{\boldsymbol{R}}_{\boldsymbol{d}}[0](i) \quad (14)$$

where $\hat{\boldsymbol{R}}_{\boldsymbol{d}}[0](\boldsymbol{i})$ is the ith $\hat{\boldsymbol{R}}_{\boldsymbol{d}}[0]$ value sent by the FLOACB to TCB and N_a is arbitrarily chosen the value of the unknown pulse length. The process of computing $\hat{\boldsymbol{R}}_{\boldsymbol{d}}[0]_{\text{ave}}$ is continuously repeated for every new N_a values of $\hat{\boldsymbol{R}}_{\boldsymbol{d}}[0]$ received by the TCB.

RCSRI: If for pre-selected threshold 'τ', $\hat{\boldsymbol{R}}_{\boldsymbol{d}}[0]_{\text{ave}} > \tau$ is achieved at some time instant, then the information bearing α-stable carrier signals are considered as detected and the Y_m is forwarded to RCSRI for the remaining steps, i.e. recognition and extraction by an eavesdropper; where τ can be chosen as any $\boldsymbol{a_{ij}} = \boldsymbol{R_d}[0]_{\alpha_i\beta_j}$ from the pre-known compiled library of non-delayed FLOAC values, i.e. FLOAC matrix '$\boldsymbol{F}$', given in Tables 1 and 2 in order to detect specifically those transmitted α-stable carrier signals which have been generated by utilising $\alpha(0 < \alpha < \alpha_i)$ and $\beta(-1 \le \beta_j < j)$ or $(\beta_j \le j \le 1)$. The threshold $\tau = 1.1$ has been chosen from the $\boldsymbol{F}$ given in Tables 1 and 2, which has been used throughout this paper as the targeted α-stable carrier signals are

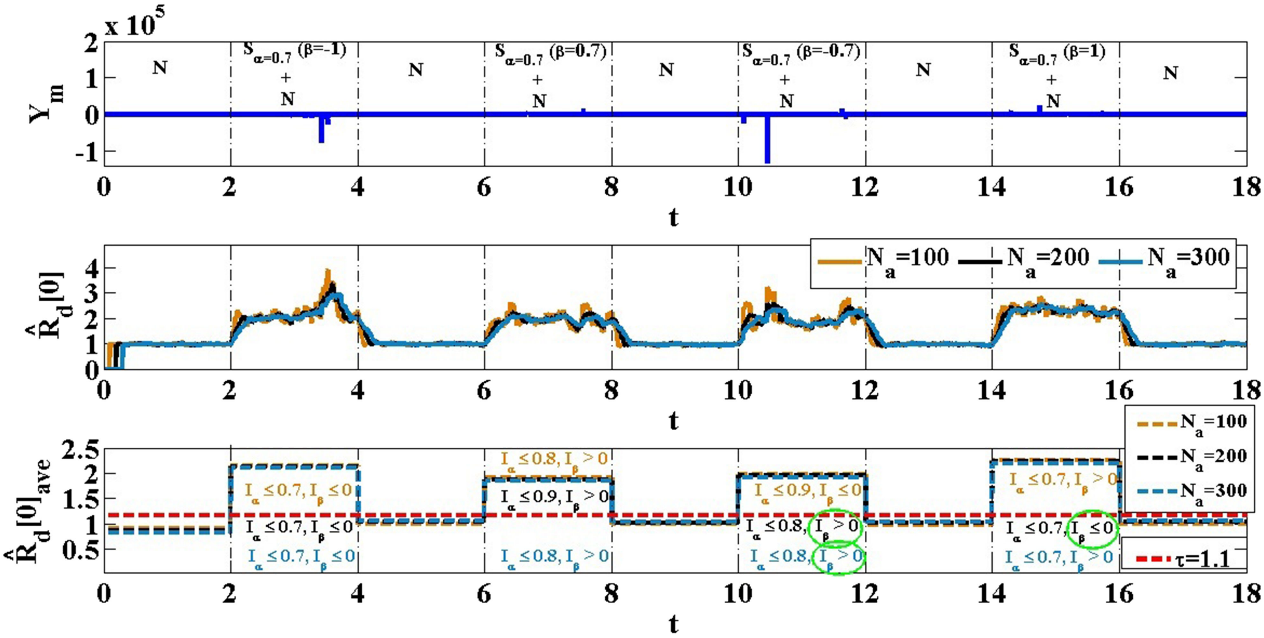

Fig. 6 *Blind recognition of* $S_{=0.7}$ *(β = − 1),* $S_{\alpha=0.7}$ *(β = 0.7),* $S_{\alpha=0.7}$ *(β = −0.7) and* $S_{\alpha=0.7}$ *(β = 1) with different '*$\boldsymbol{N_a}$*'; where* $\boldsymbol{\tau}$ = 1.1

those which have been generated by utilising $\alpha(0 < \alpha < 1.5)$ and $\beta(-1 \le \beta \le 1)$.

Computing the characteristic exponent ($\hat{\alpha}$) *and the impulsiveness parameter* ($\hat{\beta}$): In the second step, recognition by an eavesdropper has been performed by the RCSRI. It first compares the value $\hat{\boldsymbol{R}}_{\boldsymbol{d}}[0]_{\text{ave}} > \tau$ with all the elements of the FLOAC matrix '$\boldsymbol{F}$' and selects the closest one. For example, $\boldsymbol{a}_{34} = \hat{\boldsymbol{R}}_{\boldsymbol{d}}[0]_{\alpha_3\beta_4}$ enables the RCSRI to declare $\hat{\alpha}$ as α_3 and $\hat{\beta}$ as β_4 from the associated element a_{34} of $\boldsymbol{F}$ according to (7).

Computing the interval of characteristic exponent ($\hat{\alpha}$) *and impulsiveness parameter* ($\hat{\beta}$): In RCSs [13–20, 23], binary shift keying is performed by transmitting two different α-stable noise carrier signals by either modulating the impulsiveness parameter 'α', i.e. $X_1 \sim S_{\alpha_1}(\beta, \gamma, \mu)$ as '0' and $X_2 \sim S_{\alpha_2}(\beta, \gamma, \mu)$ as '1', or by modulating the skewness parameter 'β', i.e. $X_1 \sim S_\alpha(\beta_1, \gamma, \mu)$ as '0' and $X_2 \sim S_\alpha(\beta_2, \gamma, \mu)$ as '1', where $\beta_2 = -\beta_1$. The difference $\Delta\alpha$, i.e. $\alpha_2 - \alpha_1$, in symmetric α-stable (SαS) noise-based RCS and $\Delta\beta$, i.e. $\beta_2 - \beta_1$, in skewed α-stable (SkαS) noise-based RCS are always kept large to minimise the error in the extraction of binary information bits '0' and '1' at the intended receiver side as the extraction strictly depends upon the accurate estimation of $\hat{\alpha}_1$, $\hat{\alpha}_2$ or $\hat{\beta}_1$, $\hat{\beta}_2$. Since, instead of exact estimation, the proposed method selects $\hat{\alpha}$ and $\hat{\beta}$ from $\boldsymbol{F}$, therefore, a separate hard decision rule is also proposed to determine the interval of the selected $\hat{\alpha}$ and $\hat{\beta}$ which are referred as I_α and I_β which are computed according to the criteria defined as

$$I_\alpha = \begin{cases} I_\alpha \ge \hat{\alpha}, & \text{if} \quad \hat{\alpha} \ge \alpha_\tau \\ I_\alpha \le \hat{\alpha}, & \text{if} \quad \hat{\alpha} < \alpha_\tau \end{cases} \tag{15}$$

$$I_\beta = \begin{cases} I_\beta > \beta_\tau, & \text{if} \quad \hat{\beta} > \beta_\tau \\ I_\beta \le \beta_\tau, & \text{if} \quad \hat{\beta} \le \beta_\tau \end{cases} \tag{16}$$

where fixed thresholds $\alpha_\tau(\alpha_1 < \alpha_\tau < \alpha_2)$ and $\beta_\tau(\beta_1 \le \beta_\tau \le \beta_2)$ are used to take a hard decision for retrieving binary information bits '0' and '1' as a third step, i.e. extraction by an eavesdropper. The thresholds $\alpha_\tau = 1$ and $\beta_\tau = 0$ has been used throughout the paper.

4 Simulation results

The proposed blind recognition method has been tested on 12 different types of α-stable carrier signals which have been generated from the possible combination of chosen three different impulsiveness parameters, i.e. $\alpha = 0.7$, 1.1 and 1.5, and four skewness parameters, i.e. $\beta = -1$, 0.7, −0.7, 1. To label the intensity of the α-stable carrier signals, i.e. $X \sim S_\alpha$ $(\beta, \gamma = 0.5, \mu)$ contaminated by the AWGN, i.e. $N \sim S_{\alpha=2}$ $(\beta = 0,\ \gamma_N = 1,\ \mu = 0)$, mixed signal-to-noise ratio (MSNR) defined in [12] as

$$\text{MSNR}_{\text{dB}} = 10\log\frac{\gamma}{\gamma_N} \tag{17}$$

equals to −3 dB has been used where the location parameter μ has been kept to 0. Since $\gamma = 0.5$ and $\mu = 0$ have been used throughout to generate X, therefore, the notation $X \sim S_\alpha(\beta)$ has been used in Figs. 6–8 for clarity.

In Fig. 6, the received sequence $\boldsymbol{Y_m}$ contains AWGN 'N_G' alone as well as N_G added with four different types of α-stable carrier signals, i.e. $S_{\alpha=0.7}$ $(\beta = -1)$, $S_{\alpha=0.7}$ $(\beta = 0.7)$, $S_{\alpha=0.7}$ $(\beta = -0.7)$ and $S_{\alpha=0.7}$ $(\beta = 1)$. The α-stable carrier signals have been generated by utilising the same impulsiveness parameter, i.e. $\alpha = 0.7$, in combination with four different skewness parameters, i.e. $\beta = -1$, 0.7, −0.7, 1. It can be seen that the whole received sequence $\boldsymbol{Y_m}$ looks like AWGN in the real-time, which reminds the capability of α-stable carrier signals to become invisible in the presence of AWGN. As the presence or the absence of the information carrying α-stable carrier signals in the received signal '$\boldsymbol{Y_m}$' is a priori unknown, therefore the blind recognition can be considered impossible.

However, as it is shown in Fig. 7 that the computed $\hat{\boldsymbol{R}}_{\boldsymbol{d}}[0]$ according to the proposed method confirms the presence of α-stable carrier signals in $\boldsymbol{Y_m}$. Moreover, the intervals of the present α-stable carrier signals have also been correctly detected in real time. The accuracy of the detection is more or less the same for the three utilised values of N_a. Similarly, the computed $\hat{\boldsymbol{R}}_{\boldsymbol{d}}[0]_{\text{ave}}$ has provided an enhanced view of the detected α-stable carrier signals in $\boldsymbol{Y_m}$. It should be noted that the computed $\hat{\boldsymbol{R}}_{\boldsymbol{d}}[0]_{\text{ave}}$ during the interval of detected $S_{\alpha=0.7}$ $(\beta = -1)$ and $S_{\alpha=0.7}$ $(\beta = 1)$ is higher than the $S_{\alpha=0.7}$ $(\beta = 0.7)$ and $S_{\alpha=0.7}$ $(\beta = -0.7)$ which follows the pattern obtained in Figs. 1 and 2. The determined intervals of I_α and I_β have also been shown in Fig. 7 where all the I_α have been correctly determined which proves the capability of the proposed method to extract the binary information in SαS noise based RCSs by utilising

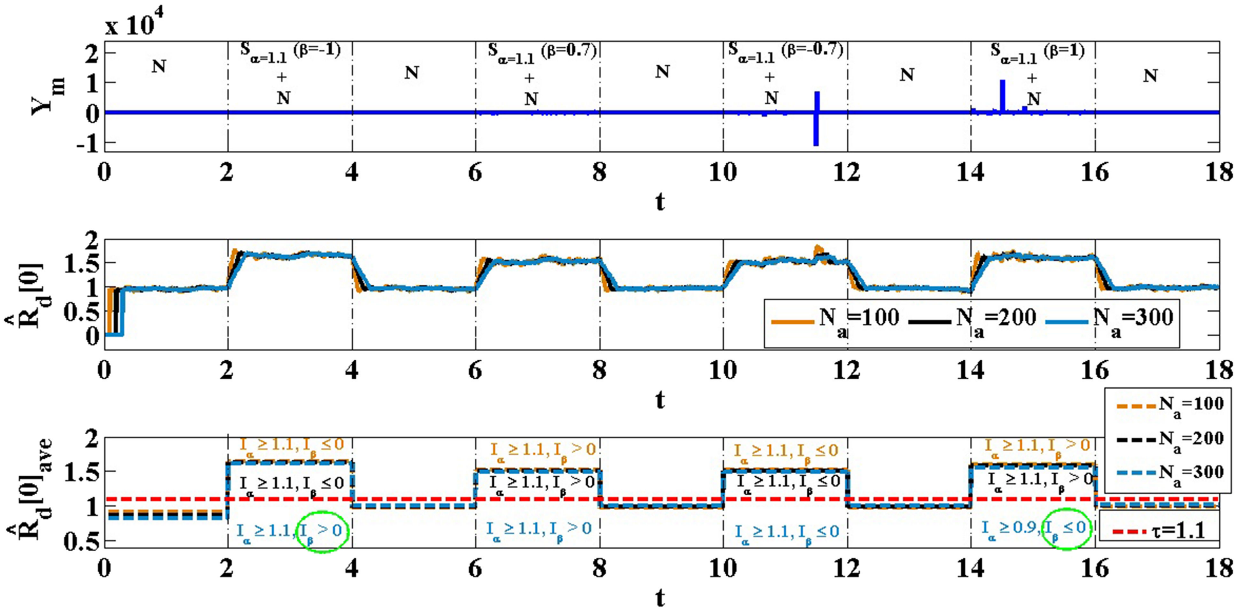

Fig. 7 *Blind recognition of $S_{=1.1}$ ($\beta = -1$), $S_{\alpha=1.1}$ ($\beta = 0.7$), $S_{\alpha=1.1}$ ($\beta = -0.7$) and $S_{\alpha=1.1}$ ($\beta = 1$) with different 'N_a'; where $\tau = 1.1$*

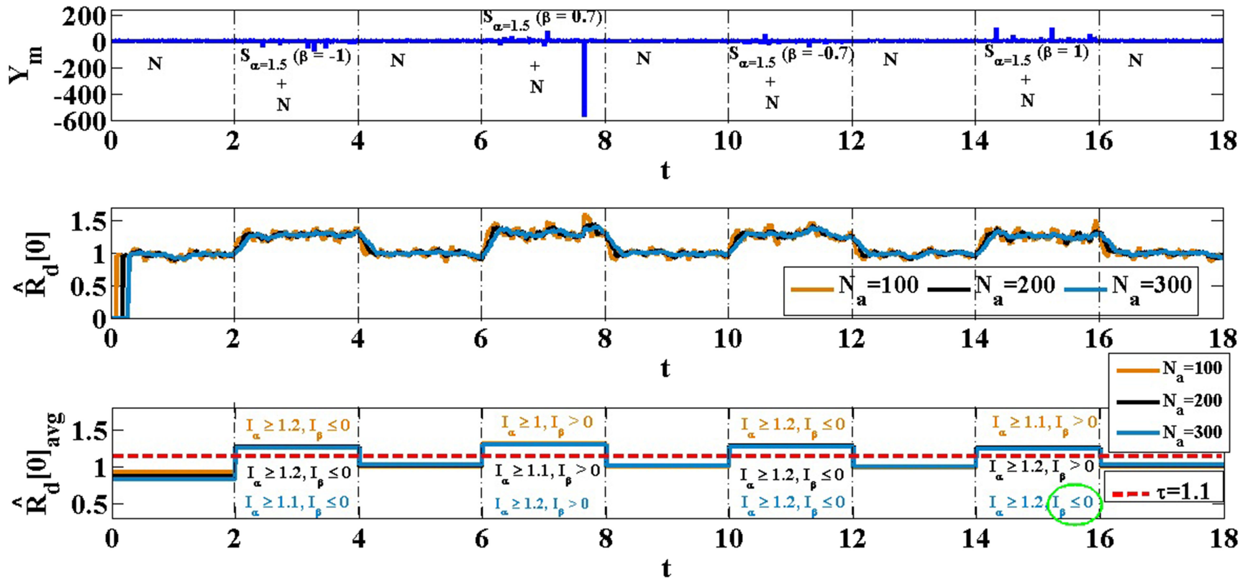

Fig. 8 *Blind recognition of $S_{=1.5}$ ($\beta = -1$), $S_{\alpha=1.5}$ ($\beta = 0.7$), $S_{\alpha=1.5}$ ($\beta = -0.7$) and $S_{\alpha=1.5}$ ($\beta = 1$) with different 'N_a'; where $\tau = 1.1$*

any value of N_a. However, 3 I_β out of 12, highlighted in a green ellipse in Fig. 7, are found as incorrect, therefore extraction of the binary information in SkαS noise-based RCSs can be carried out by utilising the lesser value of N_a, i.e. $N_a = 100$.

The result for the received sequence $\boldsymbol{Y_m}$ containing α-stable carrier signals, i.e. $S_{\alpha=1.1}$ ($\beta = -1$), $S_{\alpha=1.1}$ ($\beta = 0.7$), $S_{\alpha=1.1}$ ($\beta = -0.7$) and $S_{\alpha=1.1}$ ($\beta = 1$), generated with higher α, i.e. $\alpha = 1.1$, and previously used β have been shown in Fig. 8. Similarly, $\boldsymbol{Y_m}$ containing α-stable carrier signals generated with much higher α, i.e. $\alpha = 1.5$, and previously used β, i.e. $S_{\alpha=1.5}$ ($\beta = -1$), $S_{\alpha=1.5}$ ($\beta = 0.7$), $S_{\alpha=1.5}$ ($\beta = -0.7$) and $S_{\alpha=1.5}$ ($\beta = 1$) have been shown in Fig. 8. It can be seen that all the I_α in Figs. 7 and 8 have also been correctly determined where the error in I_β has been reduced to one when the transmitted α-stable carrier signals are generated with $\alpha = 1.5$. It has to be considered that the above results are obtained by utilising $\boldsymbol{F}$ generated from $u = 20$ and $v = 21$; where much better results are expected if much higher order $\boldsymbol{F}$ has been used by choosing values of u and v.

4.1 Covertness range for α-stable noise-based RCSs

It can be seen in Figs. 7 and 8 that there is a difference in the value of $\hat{\boldsymbol{R}}_d[0]_{\text{ave}}$ during the presence of α-stable carrier signals in comparison to the value of $\hat{\boldsymbol{R}}_d[0]_{\text{ave}}$ during the absence of α-stable carrier signals. This difference enables the RCSR to differentiate between information carrying α-stable carrier signals and the AWGN. However, this difference, which is due to the difference between the members of $\boldsymbol{F}$, i.e. $\boldsymbol{a_{ij}} = \boldsymbol{R_d}[0]_{\alpha_i\beta_j}$, in (9), starts to decrease when α of the transmitted α-stable carrier signals starts to increase and vice versa. Moreover, this difference starts to decrease drastically for $\alpha > 1.5$ (see Tables 1 and 2); hence, detection of α-stable carrier signals, generated with $\alpha > 1.5$, is extremely difficult. This is the reason that the threshold 'τ' equals to 1.1 from Tables 1 and 2, which corresponds to $\boldsymbol{R_d}[0]_{\alpha=1.5,\ -1\le\beta\le1}$ has been chosen to perform the blind recognition of those α-stable carrier signals which have been generated with $\alpha \le 1.5$ and $-1 \le \beta \le 1$.

Therefore, to establish secure communication by employing RCSs with $\alpha > 1.5$ and the lesser absolute β should be utilised while generating α-stable carrier signals. These intervals for α and β can be said as covertness range for α-stable noise-based RCSs; where choosing α and β under this range will ensure cover transmission by employing RCSs. However, further investigations should be done to optimise the proposed method to blindly recognise α-stable carrier signals in the covertness range as well. Moreover, Cramer-Rao lower bounds would be derived for the performance of the proposed algorithm in the future as it has been done in [28].

5 Conclusion

A three-step procedure for the blind recognition of α-stable random carrier signals has been introduced. The proposed method has been analysed from the perspective of an eavesdropper who has no a priori knowledge of the utilised α-stable carrier signals. It has been concluded from the simulations that the RCSs utilising α-stable carrier signals generated with smaller α (highly impulsive) and larger absolute β (heavily skewed towards the right or left) are prone to the proposed method. The only way to perform secure transmission, by utilising α-stable noise-based RCSs, is to use the related parameters of the α-stable carrier signals, i.e. α and β, according to the proposed covertness range given in the simulation results.

It is shown that the α-stable carrier signals can no longer be considered invisible as (i) detecting their presence in AWGN is now possible from the proposed method; (ii) their associated parameters, i.e. α and β, can also be recognised; (iii) extraction of the binary information hidden in the utilised α or β can also be carried out by determining intervals I_α and I_β using the proposed hard decision rule. However, further strength can be added to the proposed blind recognition method if more precise intervals of the determined I_α and I_β can be found by utilising larger values of u and v which might result in enhanced accuracy for an eavesdropper. Similarly, detecting α-stable carrier signals in the introduced covertness range and the performance of an imperfectly synchronised eavesdropper while utilising the proposed technique are the concerns of ongoing study.

6 Acknowledgments

The authors wish to acknowledge all the comments and suggestions made by the reviewers, which has improved the technical content of the paper, as well as clarity in its presentation.

7 References

[1] Basore, B.L.: 'Noise-like signals and their detection by correlation'. PhD Thesis, MIT, Cambridge, MA, 1952

[2] Pecora, L.M., Carroll, T.L.: 'Synchronization in chaotic systems', *Phys. Rev. Lett.*, 1990, **64**, (8), pp. 821–823

[3] Oppenheim, A.V., Wornell, G.W., Isabelle, S.H., *et al.*: 'Signal processing in the context of chaotic signals'. Acoustics, Speech, and Signal Processing (ICASSP), San Francisco, CA, USA, 1992, pp. 117–120

[4] Dedieu, H., Kennedy, M.P., Hasler, M.: 'Chaos shift keying: modulation and demodulation of a chaotic carrier using self-synchronizing Chua's circuits', *IEEE Trans. Circ. Syst. II, Anal. Digit. Sig. Process.*, 1993, **40**, (10), pp. 634–642

[5] Sobhy, M.I, Shehata, A.-E.R.: 'Methods of attacking chaotic encryption and countermeasures'. Proc. IEEE Int. Conf. Acoustics Speech Signal Process (ICASSP '01), Salt Lake City, UT, USA, 2001, pp. 1001–1004

[6] Gonzalo, A., Montoya, F., Romera, M., *et al.*: 'Breaking parameter modulated chaotic secure communication system', *Chaos, Solitons Fractals*, 2004, **21**, pp. 783–787

[7] Gonzalo, A., Montoya, F., Romera, M., *et al.*: 'Breaking two secure communication systems based on chaotic masking', *IEEE Trans. Circuits Syst. II, Express Briefs*, 2004, **51**, (10), pp. 505–506

[8] Gu, C., Cao, X.: 'Research on information hiding technology'. Proc. Int. Conf. Consumer Electronics, Communications and Networks (CECNet), Three Gorges, China, 2012, pp. 2035–2037

[9] Nikias, C.L., Shao, M.: '*Signal processing with alpha-stable distributions and applications*' (Wiley, New York, 1995)

[10] Ma, X., Nikias, C.L.: 'Joint estimation of time delay and frequency delay in impulsive noise using fractional lower order statistics', *IEEE Trans. Signal Process.*, 1996, **44**, (11), pp. 2669–2687

[11] Tsihrintzis, G.A., Nikias, C.L.: 'Fast estimation of the parameters of alpha-stable impulsive interference', *IEEE Trans. Signal Process.*, 1996, **44**, (6), pp. 1492–1503

[12] Kuruoğlu, E.E.: 'Density parameter estimation of skewed alpha-stable distributions', *IEEE Trans. Signal Process.*, 2001, **49**, (10), pp. 2192–2201

[13] Kannan, N., Ravishanker, N.: 'High resolution estimation for sub-Gaussian stable signals in a linear array model', *IET Signal Process.*, 2007, **1**, (1), pp. 35–42

[14] Casarin, R.: 'Bayesian inference for mixtures of stable distributions'. Working paper No. 0428, CEREMADE, University Paris IX, 2004

[15] Diego, S.G., Kuruoglu, E.E., Diego, P.R.: 'Finite mixture of α-stable distributions', *Digit. Signal Process.*, 2009, **19**, (2), pp. 250–264

[16] Cek, M.E., Savaci, F.A.: 'Stable non-Gaussian noise parameter modulation in digital communication', *IET Electron. Lett.*, 2009, **45**, (24), pp. 1256–1257

[17] Cek, M.E.: 'Covert communication using skewed α-stable distributions', *IET Electron. Lett.*, 2015, **51**, (1), pp. 116–118

[18] Cek, M.E.: 'M-ary alpha-stable noise modulation in spread-spectrum communication', *Fluct. Noise Lett.*, 2015, **14**, (3), 1550022

[19] Xu, Z.J., Wang, K., Gong, Y., *et al.*: 'Structure and performance analysis of an SαS-based digital modulation system', *IET Commun.*, 2016, **10**, (11), pp. 1329–1339

[20] Xu, Z.J., Wang, K., Gong, Y., *et al.*: 'A covert digital communication system based on joint normal distribution', *IET Commun.*, 2017, **11**, (8), pp. 1282–1290

[21] Ahmed, A., Savaci, F.A.: 'Random communication system based on skewed alpha-stable levy noise shift keying', *Fluct. Noise Lett.*, 2017, **16**, (3), 1750024

[22] Ahmed, A., Savaci, F.A.: 'Measure of covertness based on the imperfect synchronization of an eavesdropper in random communication systems'. 10th Int. Conf. on Electrical and Electronic Engineering (ELECO), Turkey, November 2017, pp. 638–641

[23] Ahmed, A., Savaci, F.A.: 'Synchronisation of alpha-stable levy noise-based random communication system', *IET Commun.*, 2018, **12**, (3), pp. 276–282

[24] Samorodnitsky, G., Taqqu, M.S.: '*Stable non-Gaussian random processes*' (Chapman & Hall/CRC, New York, USA, 1994)

[25] Janicki, A., Weron, A.: '*Simulation and chaotic behaviour of a-stable stochastic processes*' (Marcel Dekker, New York, USA, 1994)

[26] Ahmed, A., Savaci, F.A.: 'Structure and performance evaluation of fractional lower-order covariance method in alpha-stable noise environments', *Recent Adv. Electr. Electron. Eng.*, 2019, **12**, (1), pp. 40–44

[27] Ahmed, A., Savaci, F.A.: 'On optimizing fractional lower order covariance based synchronization method for random communication systems'. 26th IEEE Signal Processing and Communications Applications Conf. (SIU), Turkey, May 2018

[28] Hameed, F., Dobre, O.A., Popescu, D.C., *et al.*: 'On the likelihood-based approach to modulation classification', *IEEE Trans. Wirel. Commun.*, 2019, **8**, (12), pp. 5884–5892

8 Appendix

See Tables 1 and 2.

Table 1 (Part 1) ***F*** for $U = 20$, $V = 21$ and $\Delta\alpha = \Delta\beta = 0.001$

F	$\hat{\beta} = \beta_1 = -1$	$\hat{\beta} = \beta_2 = -0.9$	$\hat{\beta} = \beta_3 = -0.8$	$\hat{\beta} = \beta_4 = -0.7$	$\hat{\beta} = \beta_5 = -0.6$
$\hat{\alpha} = \alpha_1 = 0.1$	1.80×10^{21}	2.82×10^{22}	8.85×10^{24}	4.09×10^{20}	2.98×10^{27}
$\hat{\alpha} = \alpha_2 = 0.2$	6.33×10^{9}	1.42×10^{9}	5.31×10^{9}	5.83×10^{9}	5.92×10^{8}
$\hat{\alpha} = \alpha_3 = 0.3$	3848	19392	2×10^{6}	3×10^{6}	6933.73
$\hat{\alpha} = \alpha_4 = 0.4$	51.8	150	46.4	708	1107
$\hat{\alpha} = \alpha_5 = 0.5$	7.06	7.07	7.43	6.96	8.13
$\hat{\alpha} = \alpha_6 = 0.6$	3.23	3.14	3.1	2.97	3.23
$\hat{\alpha} = \alpha_7 = 0.7$	2.33	2.16	2.36	2.13	2.13
$\hat{\alpha} = \alpha_8 = 0.8$	1.97	1.93	1.83	1.79	1.78
$\hat{\alpha} = \alpha_9 = 0.9$	2.19	2.08	1.98	1.87	1.77
$\hat{\alpha} = \alpha_{10} = 1$	1.33	1.32	1.31	1.32	1.31
$\hat{\alpha} = \alpha_{11} = 1.1$	1.69	1.63	1.57	1.51	1.44
$\hat{\alpha} = \alpha_{12} = 1.2$	1.3	1.28	1.26	1.24	1.23
$\hat{\alpha} = \alpha_{13} = 1.3$	1.18	1.18	1.17	1.16	1.16
$\hat{\alpha} = \alpha_{14} = 1.4$	1.14	1.13	1.12	1.12	1.12
$\hat{\alpha} = \alpha_{15} = 1.5$	1.1	1.1	1.1	1.1	1.1
$\hat{\alpha} = \alpha_{16} = 1.6$	1.08	1.08	1.08	1.08	1.08
$\hat{\alpha} = \alpha_{17} = 1.7$	1.06	1.06	1.06	1.06	1.06
$\hat{\alpha} = \alpha_{18} = 1.8$	1.05	1.05	1.05	1.05	1.05
$\hat{\alpha} = \alpha_{19} = 1.9$	1.04	1.04	1.04	1.04	1.04
$\hat{\alpha} = \alpha_{20} = 2$	1.03	1.03	1.03	1.03	1.03

F	$\hat{\beta} = \beta_6 = -0.5$	$\hat{\beta} = \beta_7 = -0.4$	$\hat{\beta} = \beta_8 = -0.3$	$\hat{\beta} = \beta_9 = -0.2$	$\hat{\beta} = \beta_{10} = -0.1$
$\hat{\alpha} = \alpha_1 = 0.1$	4.95×10^{25}	2.21×10^{23}	1.71×10^{22}	6.92×10^{28}	3.45×10^{21}
$\hat{\alpha} = \alpha_2 = 0.2$	2.7×10^{7}	1.02×10^{8}	6.4×10^{7}	8.5×10^{7}	1.15×10^{8}
$\hat{\alpha} = \alpha_3 = 0.3$	3465.04	4645.865	1159.76	1923.45	5557.67
$\hat{\alpha} = \alpha_4 = 0.4$	861	51	43	91.5	35.2
$\hat{\alpha} = \alpha_5 = 0.5$	6.1	9.26	9.7	11.9	8.17
$\hat{\alpha} = \alpha_6 = 0.6$	3.5	3.21	3.86	3.03	3.17
$\hat{\alpha} = \alpha_7 = 0.7$	2.14	2.24	2.2	2.04	2.06
$\hat{\alpha} = \alpha_8 = 0.8$	1.73	1.7	1.68	1.63	1.72
$\hat{\alpha} = \alpha_9 = 0.9$	1.69	1.62	1.51	1.47	1.45
$\hat{\alpha} = \alpha_{10} = 1$	1.31	1.31	1.31	1.31	1.31
$\hat{\alpha} = \alpha_{11} = 1.1$	1.39	1.34	1.29	1.26	1.24
$\hat{\alpha} = \alpha_{12} = 1.2$	1.21	1.2	1.19	1.19	1.18
$\hat{\alpha} = \alpha_{13} = 1.3$	1.15	1.15	1.15	1.15	1.14
$\hat{\alpha} = \alpha_{14} = 1.4$	1.12	1.12	1.12	1.11	1.12
$\hat{\alpha} = \alpha_{15} = 1.5$	1.1	1.09	1.09	1.09	1.09
$\hat{\alpha} = \alpha_{16} = 1.6$	1.08	1.08	1.08	1.07	1.08
$\hat{\alpha} = \alpha_{17} = 1.7$	1.06	1.06	1.06	1.06	1.06
$\hat{\alpha} = \alpha_{18} = 1.8$	1.05	1.05	1.05	1.05	1.05
$\hat{\alpha} = \alpha_{19} = 1.9$	1.04	1.04	1.04	1.04	1.0
$\hat{\alpha} = \alpha_{20} = 2$	1.03	1.03	1.03	1.04	1.03

Table 2 (Part 2) ***F*** for $U = 20$, $V = 21$ and $\Delta\alpha = \Delta\beta = 0.1$

F	$\hat{\beta} = \beta_{11} = 0$	$\hat{\beta} = \beta_{12} = 0.1$	$\hat{\beta} = \beta_{13} = 0.2$	$\hat{\beta} = \beta_{14} = 0.3$	$\hat{\beta} = \beta_{15} = 0.4$	$\hat{\beta} = \beta_{16} = 0.5$
$\hat{\alpha} = \alpha_1 = 0.1$	2.46×10^{26}	2.77×10^{23}	2.40×10^{22}	2.93×10^{23}	4.10×10^{26}	2.00×10^{21}
$\hat{\alpha} = \alpha_2 = 0.2$	7×10^7	5.2×10^7	2.2×10^7	1.5×10^7	2.92×10^9	1.72×10^{10}
$\hat{\alpha} = \alpha_3 = 0.3$	8865.1	246,631.4	241,912.4	11,251.7	2225.7	10,518.7
$\hat{\alpha} = \alpha_4 = 0.4$	62.4	118.7	170.4	349.8	389.02	63.8
$\hat{\alpha} = \alpha_5 = 0.5$	7.53	11.1	9.35	7.79	9.62	8.16
$\hat{\alpha} = \alpha_6 = 0.6$	3.07	3.21	3.37	4.4	3.23	3.15
$\hat{\alpha} = \alpha_7 = 0.7$	2.09	2.15	2.03	2.02	2.22	2.07
$\hat{\alpha} = \alpha_8 = 0.8$	1.62	1.64	1.66	1.69	1.72	1.73
$\hat{\alpha} = \alpha_9 = 0.9$	1.43	1.45	1.47	1.53	1.6	1.69
$\hat{\alpha} = \alpha_{10} = 1$	1.31	1.32	1.31	1.31	1.31	1.31
$\hat{\alpha} = \alpha_{11} = 1.1$	1.23	1.24	1.26	1.3	1.33	1.38
$\hat{\alpha} = \alpha_{12} = 1.2$	1.17	1.18	1.19	1.2	1.2	1.21
$\hat{\alpha} = \alpha_{13} = 1.3$	1.14	1.14	1.15	1.15	1.15	1.15
$\hat{\alpha} = \alpha_{14} = 1.4$	1.11	1.11	1.12	1.12	1.12	1.12
$\hat{\alpha} = \alpha_{15} = 1.5$	1.09	1.09	1.09	1.09	1.09	1.1
$\hat{\alpha} = \alpha_{16} = 1.6$	1.07	1.08	1.07	1.08	1.08	1.08
$\hat{\alpha} = \alpha_{17} = 1.7$	1.06	1.06	1.06	1.06	1.06	1.06
$\hat{\alpha} = \alpha_{18} = 1.8$	1.05	1.05	1.05	1.05	1.05	1.05
$\hat{\alpha} = \alpha_{19} = 1.9$	1.04	1.04	1.04	1.04	1.04	1.04
$\hat{\alpha} = \alpha_{20} = 2$	1.03	1.04	1.03	1.03	1.03	1.03

F	$\hat{\beta} = \beta_{17} = 0.6$	$\hat{\beta} = \beta_{18} = 0.7$	$\hat{\beta} = \beta_{19} = 0.8$	$\hat{\beta} = \beta_{20} = 0.9$	$\hat{\beta} = \beta_{21} = 1$
$\hat{\alpha} = \alpha_1 = 0.1$	7.18×10^{20}	3.96×10^{19}	1.67×10^{22}	1.37×10^{21}	1.62×10^{25}
$\hat{\alpha} = \alpha_2 = 0.2$	4.5×10^7	1.19×10^8	8.73×10^8	1.9×10^9	1.67×10^{10}
$\hat{\alpha} = \alpha_3 = 0.3$	2065.8	3280.4	6972.1	76,381.8	1249.5
$\hat{\alpha} = \alpha_4 = 0.4$	60.8	60.6	60.9	74.8	91.2
$\hat{\alpha} = \alpha_5 = 0.5$	7.35	8.87	7.59	7.45	6.39
$\hat{\alpha} = \alpha_6 = 0.6$	3.54	4.66	3.33	3.27	3.27
$\hat{\alpha} = \alpha_7 = 0.7$	2.07	2.16	2.19	2.17	2.21
$\hat{\alpha} = \alpha_8 = 0.8$	1.76	1.8	1.84	1.9	1.94
$\hat{\alpha} = \alpha_9 = 0.9$	1.77	1.88	1.98	2.09	2.19
$\hat{\alpha} = \alpha_{10} = 1$	1.31	1.32	1.32	1.32	1.32
$\hat{\alpha} = \alpha_{11} = 1.1$	1.44	1.5	1.57	1.63	1.7
$\hat{\alpha} = \alpha_{12} = 1.2$	1.23	1.24	1.26	1.28	1.3
$\hat{\alpha} = \alpha_{13} = 1.3$	1.16	1.16	1.17	1.18	1.19
$\hat{\alpha} = \alpha_{14} = 1.4$	1.12	1.12	1.13	1.13	1.13
$\hat{\alpha} = \alpha_{15} = 1.5$	1.1	1.1	1.1	1.1	1.1
$\hat{\alpha} = \alpha_{16} = 1.6$	1.08	1.08	1.08	1.08	1.08
$\hat{\alpha} = \alpha_{17} = 1.7$	1.06	1.06	1.06	1.06	1.06
$\hat{\alpha} = \alpha_{18} = 1.8$	1.05	1.05	1.05	1.05	1.05
$\hat{\alpha} = \alpha_{19} = 1.9$	1.04	1.04	1.04	1.04	1.04
$\hat{\alpha} = \alpha_{20} = 2$	1.03	1.03	1.03	1.03	1.03