Dynamic Hyperchaotic Key Generation Using Optical Orthogonal Frequency Division Multiplexing-based Visible Light Communication Networks

Mohammed Alresheedi
King Saud University
YAHYA AL-MOLIKI (yalmoliki@ksu.edu.sa)
King Saud University https://orcid.org/0000-0003-1778-8239
Yahya Al-Harthi
King Saud University
Ali Alqahtani
King Saud University

Research

Keywords: Confidentiality, hyperchaotic, key generation, optical orthogonal frequency division multiplexing, visible light communication

Posted Date: May 21st, 2021

DOI: https://doi.org/10.21203/rs.3.rs-499286/v1

Version of Record: A version of this preprint was published at IEEJ Transactions on Electrical and Electronic Engineering on February 8th, 2022. See the published version at https://doi.org/10.1002/tee.23557.

Dynamic Hyperchaotic Key Generation Using Optical Orthogonal Frequency Division Multiplexing-based Visible Light Communication Networks

Mohammed T. Alresheedi, Yahya M. Al-Moliki, Yahya Al-Harthi, and Ali H. Alqahtani

Abstract—This paper introduces an optical orthogonal frequency division multiplexing (OFDM)-based hyperchaotic key generation encryption approach that can improve confidentiality in visible light communication (VLC) networks. Using a hyperchaotic four-dimensional method, the bipolar real-valued OFDM signal can be used for constructing dynamic cypher keys modified at every frame over the communication time, resulting in a superior degree of protection against statistical and correlation attacks. In accordance with our findings, this approach decreases the ratio of peak-to-average power of the transmitted signal, and enhances the bit error rate efficiency and secrecy capacity of the OFDM-based VLC network, which improves confidentiality.

***Index Terms*— Confidentiality, hyperchaotic, key generation, optical orthogonal frequency division multiplexing, visible light communication**

1. INTRODUCTION

Physical-layer security is a powerful and inventive approach with respect to strengthening the confidentiality of communications and thus countering snooping [1]. In [2–4], authors suggest using physical-layer approaches for keyless protection strategies for visible light communication (VLC). However, to ensure effective implementation and confidentiality, these strategies require the snooper channel or physical location to be estimated during communication. Some reports suggest using key generation methods to improve the confidentiality of orthogonal frequency division multiplexing (OFDM)-based VLC networks [5–8]. These methods involve generating a secret key from the cyclic prefix (CP) of the OFDM signal. Theses keys are used for encoding the time-domain samples of the OFDM signal by utilizing a Hadamard product method until communication is complete.

Unfortunately, OFDM is vulnerable to clipping and signal compression non-linearities [9]. Two clipping types are possible in optical OFDM: positive and negative. For positive clipping, the positive part of the samples penetrating the non-linear area of the light-emitting diode is clipped, whereas, for negative clipping, the negative part of the samples is clipped for intensity modulation/direct detection technique. The encryption by random

sequence of the time-domain samples affects the sampling polarity and hence the clipping form (negative or positive) of each sample; it distorts the time-domain subcarriers during they are transmitted, thus deteriorating the optical OFDM performance.

This paper proposes a new hyperchaotic key generation approach using optical OFDM, referred to as hyperchaos-KG-OOFDM. We use the randomness character of the input information and the chaotic codes created via the hyperchaotic system to support VLC network confidentiality. The approach generates secret keys that are dependent on the polarity of the bipolar real-valued time-domain OFDM samples and chaotic schemes. In each frame, these secret sequences are modified, which results in a high degree of protection against statistical and correlation attacks. In comparison with [5–7], we recommend introducing phase encryption for frequency-domain subcarriers, rather than applying polarity encryption for the time-domain subcarriers. Since the encryption is executed prior to inverse fast Fourier transformation (IFFT), the OFDM signals are encrypted and transmitted without distortion. Furthermore, random sequence multiplication of the frequency-domain samples will render every in phase frequency-domain subcarrier out of phase. It decreases the ratio of peak-to-average power (PAPR) of the OFDM time-domain signals to enhance the OFDM method efficiency [10]. In contrast with [5–7], a channel coding method is proposed for secret keys produced by OFDM samples. By this way, the keys are safe as the signal is traveling through noisy channels.

2. METHOD

A four-dimensional (4D) hyperchaotic scheme is used to generate chaotic quantities for fourfold encryption, which can be obtained by the following equation [11]:

$$\begin{cases} x_{i,k} = a\left(-x_{i,k-1} + y_{i,k-1}\right) + y_{i,k-1}z_{i,k-1}u_{i,k-1} \\ y_{i,k} = b\left(x_{i,k-1} + y_{i,k-1}\right) - x_{i,k-1}z_{i,k-1}u_{i,k-1} \\ z_{i,k} = cy_{i,k-1} - u_{i,k-1} + dx_{i,k-1}y_{i,k-1}u_{i,k-1} \\ u_{i,k} = -eu_{i,k-1} + x_{i,k-1}y_{i,k-1}z_{i,k-1}, \end{cases} \quad (1)$$

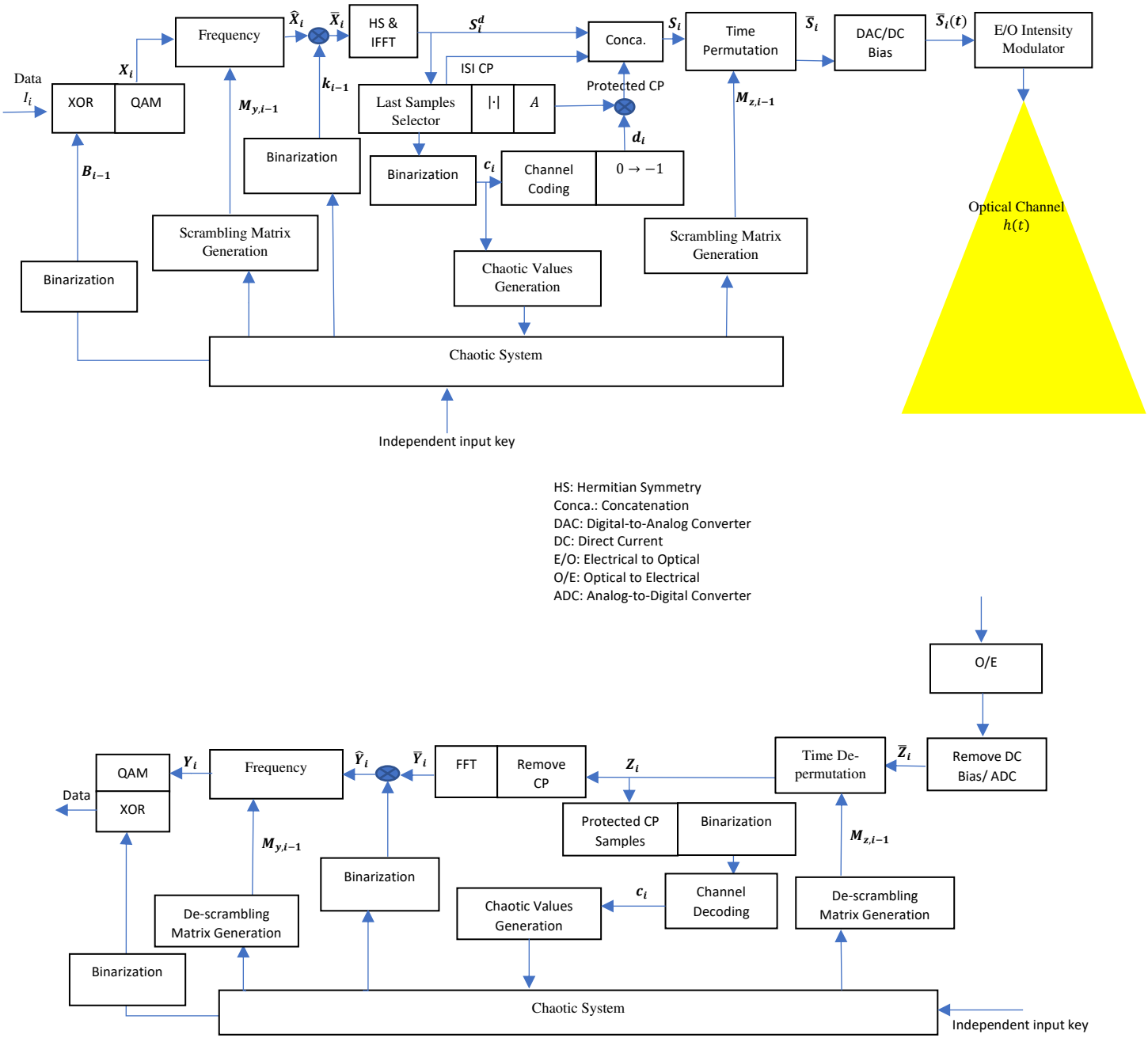

Fig. 1. Proposed hyperchaos-KG-OOFDM method.

where a, b, c, d, and e denote real parameters; $x_{i,k}$ is the k_{th} chaotic quantity of $\boldsymbol{x_i}$ at the i_{th} frame. In accordance with the Lyapunov exponent, the scheme indicates chaotic

features when $a = 35, b = 10, c = 80, d = 0.5$, and $e = 10$. The Runge–Kutta method can be applied to resolve (1) to get the chaos sequences $\boldsymbol{x_i}$, $\boldsymbol{y_i}$, $\boldsymbol{z_i}$, and $\boldsymbol{u_i}$ at each frame employing a 0.001s time step.

Following iteration at some initial stage, digital chaotic quantities can be produced after iteration with uniform distribution. For example, let $\boldsymbol{D_{x,i}}$ be the digitized chaos sequence of $\boldsymbol{x_i}$, which can be expressed as follows [12]:

$$D_{x,i,k} = mod\big(Extract\big(x_{i,k}, \mathrm{m}, \mathrm{n}, \mathrm{p}\big), M\big), \tag{2}$$

where $D_{x,i,k}$ is the k_{th} chaotic quantity of $\boldsymbol{D_{x,i}}$, the function $Extract(x_i, \mathrm{m}, \mathrm{n}, \mathrm{p})$ yields an integer that is obtained from the $\mathrm{m_{th}}, \mathrm{n_{th}}$, and $\mathrm{p_{th}}$ digits in the decimal portion of $x_{i,k}$, $mod(\cdot,\cdot)$ is the modulo operation, and *M* denotes the largest quantity value, which, in our approach, is 256. The other digitalized sequences $\boldsymbol{D_{y,i}}$, $\boldsymbol{D_{z,i}}$, and $\boldsymbol{D_{u,i}}$ can be obtained in a similar way.

In our proposed method, the CP samples of time-domain signals are served to dynamically update the hyperchaotic quantities produced through the chaotic approach at the beginning of every frame throughout the entire session. For example, if $x_{i,1}$ is the chaotic quantity generated by the chaotic scheme and $x_{i,cp}$ is the chaotic quantity generated from the CP samples at the i_{th} frame, then the first quantity $D_{x,i,1}$ can be obtained at the i_{th} frame as follows:

$$D_{x,i,1} = mod\left(Extract\left(\frac{x_{i,1} + x_{i,cp}}{2}, \mathrm{m}, \mathrm{n}, \mathrm{p}\right), M\right). \tag{3}$$

The remaining iterated quantities of $\boldsymbol{D_{x,i}}$, $\{D_{x,i,2}, D_{x,i,3}, \ldots \ldots\}$ are generated from $\boldsymbol{x_i}$ by the chaotic scheme using (1) and (2). The hyperchaotic quantities produced by the chaos system are extremely sensitive to initial quantities ($\sim 1 \times 10^{-15}$) and have a powerful randomness feature [12] that ensures high protection against vicious intrusions.

Fig. 1 shows the proposed hyperchaos-KG-OOFDM method. This approach uses four key stages to implement chaotic encryption. The first stage is binary data XOR encryption, which is described by the $\boldsymbol{D_{x,i}}$ sequence. The second stage consists of the permuted frequency-domain OFDM symbol, which is described by the $\boldsymbol{D_{y,i}}$ sequence. The third stage is defined by the $\boldsymbol{D_{z,i}}$ sequence; it consists of the phase encryption of frequency-domain symbols. The final stage is described by the $\boldsymbol{D_{u,i}}$ sequence; it consists of the permutation of the time-domain OFDM samples. The encryption technique is explained below.

The first sequence $\boldsymbol{D_{x,i}}$ is used for the XOR encryption of binary data. A confidential key $\boldsymbol{B_i}$ is extracted from $\boldsymbol{D_{x,i}}$ using the binarization process as follows:

$$B_{i,k} = \begin{cases} 0 \; for \; D_{x,i,k} \leq \dfrac{M}{4} \\ 1 \; for \; D_{x,i,k} > \dfrac{M}{4}, \end{cases} \quad 1 \leq k \leq L \tag{4}$$

where $B_{i,k}$ is the k_{th} element of $\boldsymbol{B_i}$, and L is the length of the data frame. This key is used for XOR binary data operation.

The second sequence $\boldsymbol{D_{y,i}}$ is used to permutate the frequency-domain OFDM symbol, as illustrated in Fig. 1. A $\boldsymbol{M_{y,i}}$ scrambling matrix is created in line with the order of digital values in $\boldsymbol{D_{y,i.}}$ Supposing $\boldsymbol{r_{y,i}}$ is a permuted vector with a length of $\frac{N_f}{2}$, where N_f denotes the frequency-domain subcarrier number, then the vector can be expressed as follows:

$$\boldsymbol{r_{y,i}} = \left[D_{y,i,1}, D_{y,i,2}, \ldots, D_{y,i,\frac{N_f}{2}} \right]^T. \tag{5}$$

Letting $\boldsymbol{r}_{\boldsymbol{y,i}}^{S}$ be the ascending ordered sequence of $\boldsymbol{r}_{\boldsymbol{y,i}}$, then a $\frac{N_f}{2} \times \frac{N_f}{2}$ matrix $\boldsymbol{E}_{\boldsymbol{y,i}}$ is obtained as follows:

$$\boldsymbol{E}_{\boldsymbol{y,i}} = \boldsymbol{I}\left(\boldsymbol{r}_{\boldsymbol{y,i}}^{S}\left[\boldsymbol{r}_{\boldsymbol{y,i}}^{-1}\right]^{T}\right), \tag{6}$$

where $\boldsymbol{r}_{\boldsymbol{y,i}}^{-1} = \left[\frac{1}{D_{y,i,1}}, \frac{1}{D_{y,i,2}}, \ldots, \frac{1}{D_{y,i,\frac{N_f}{2}}}\right]^{T}$; $\boldsymbol{I}(\cdot)$ can be obtained as follows:

$$\boldsymbol{I}(\boldsymbol{Y}) = \boldsymbol{Z} \rightarrow Z_{m,n} = \begin{cases} 1 \; for \; Y_{m,n} = 1 \\ 0 \text{ else,} \end{cases} \tag{7}$$

where $\boldsymbol{Y}$ and $\boldsymbol{Z}$ are the input and output matrices of $\boldsymbol{I}$. The $N_f \times N_f$ scrambling matrix can be evaluated as follows:

$$\boldsymbol{M}_{\boldsymbol{y,i}} = \begin{bmatrix} \boldsymbol{E}_{\boldsymbol{y,i}} & \boldsymbol{0} \\ \boldsymbol{0} & \boldsymbol{E}_{\boldsymbol{y,i}}^{r} \end{bmatrix}, \tag{8}$$

where $\boldsymbol{E}_{\boldsymbol{y,i}}^{r}$ represents the rotation process of $\boldsymbol{E}_{\boldsymbol{y,i}}$, which can be expressed as follows:

$$\boldsymbol{E}_{\boldsymbol{y,i}}^{\boldsymbol{r}} = \boldsymbol{r}\boldsymbol{E}_{\boldsymbol{y,i}}\boldsymbol{r}, \tag{9}$$

where $\boldsymbol{r}$ is a $\frac{N_f}{2} \times \frac{N_f}{2}$ anti-diagonal matrix, which can be expressed as follows:

$$\boldsymbol{r} = \begin{bmatrix} & & 1 \\ & \vdots & \\ 1 & & \end{bmatrix}. \tag{10}$$

The scrambling matrix $\boldsymbol{M_{y,i}}$ holds a value of 1 in each row and column; the remaining values are zeroes. Once the scrambling matrix has been generated, a frequency-domain OFDM symbol permutation is applied:

$$\widehat{\boldsymbol{X}}_{\boldsymbol{i}} = \boldsymbol{M}_{\boldsymbol{y,i-1}}\boldsymbol{X}_{\boldsymbol{i}}, \tag{11}$$

where $M_{y,i-1}$ is the scrambling matrix generated from $\boldsymbol{D_{y,i-1}}$ at the frame with index $(i-1)_{\text{th}}$; $\widehat{\boldsymbol{X}}_{\boldsymbol{i}}$ denotes the permuted frequency-domain OFDM symbol. For the phase encryption of $\widehat{\boldsymbol{X}}_{\boldsymbol{i}}$, the third sequence $\boldsymbol{D_{z,i}}$ is utilized. By using binary operation, a secret key $\boldsymbol{k_i}$ is obtained from $\boldsymbol{D_{z,i}}$ as follows:

$$k_{i,\kappa} = \begin{cases} -1 \; for \; D_{z,i,k} \leq \dfrac{M}{4} \\ +1 \; for \; D_{z,i,k} > \dfrac{M}{4}, \end{cases} \quad 1 \leq k \leq N_f \tag{12}$$

where $k_{i,\kappa}$ is the κ_{th} element of $\boldsymbol{k_i}$. The key is used for the phase encryption of the frequency-domain OFDM symbol as follows:

$$\overline{\boldsymbol{X}}_{\boldsymbol{i}} = \widehat{\boldsymbol{X}}_{\boldsymbol{i}} .* \boldsymbol{k_{i-1}}, \tag{13}$$

where $\boldsymbol{k_{i-1}}$ denotes the secret key created from $\boldsymbol{D_{z,i-1}}$ at the $(i-1)_{\text{th}}$ frame, $*$ denotes the Hadamard product operation, and $\overline{\boldsymbol{X}}_{\boldsymbol{i}}$ denotes the encoded OFDM symbol.

In our method, we let $\boldsymbol{S_i^d}$ represent the present real bipolar OFDM samples during communication at the IFFT operation output. This signal is generated when Hermitian symmetry is applied to the frequency-domain subcarrier. The CP samples $\boldsymbol{S_i^c}$ are appended to $\boldsymbol{S_i^d}$ to produce the whole OFDM samples $\boldsymbol{S_i}$. From the last few samples of $\boldsymbol{S_i^d}$, the samples $\boldsymbol{S_i^c}$ can be generated as follows:

$$\boldsymbol{S_i^c} = \left[\underbrace{S^d_{i,(N_d-l_I)}, \ldots, S^d_{i,N_d}}_{\text{ISI CP Samples}}, \underbrace{A_i.* d_{i,1}, A_i.* d_{i,2}, \ldots, A_i.* d_{i,l_p}}_{\text{Protected CP Samples}}\right], \tag{14}$$

$$A_i = \frac{1}{l_I} \sum_{j=N_d-l_I}^{N_d} \left|S^d_{i,j}\right|, \tag{15}$$

where N_d denotes the amount of time-domain subcarriers, $S^d_{i,k}$ denotes the k_{th} sample of $\boldsymbol{S_i^d}$ at the i_{th} frame, (l_I, l_p) indicates ISI and protected CP sample lengths respectively, A_i denotes the mean of the absolute values for the latter few chosen samples of $\boldsymbol{S_i^d}$ (which is considerably above the channel noise due to the illumination requirement [5]), and $d_{i,k}$ is the k_{th} vector element of $\boldsymbol{d_i}$, where $\boldsymbol{d_i}$ is generated from the last few samples of $\boldsymbol{S_i^d}$ after channel coding as well as binary operation (as shown in Fig. 1). The first segment of $\boldsymbol{S_i^c}$ is used for ISI mitigation, whereas the second segment includes the primary key $\boldsymbol{c_i}$, which can be produced from the last few samples of $\boldsymbol{S_i^d}$ as follows:

$$c_{i,k} = \begin{cases} -1 \; for \; S^d_{i,k} \leq 0 \\ +1 \; for \; S^d_{i,k} \geq 0, \end{cases} \quad N_d - Rl_p \leq k \leq N_d \tag{16}$$

where $c_{i,k}$ is the k_{th} element of $\boldsymbol{c_i}$; R denotes the code rate of channel encoder, which encodes $\boldsymbol{c_i}$. The key $\boldsymbol{c_i}$ at the i_{th} frame is used to update the chaotic quantities of the hyperchaotic approach. When the total OFDM signal $\boldsymbol{S_i}$ is produced from $\boldsymbol{S_i^c}$ and $\boldsymbol{S_i^d}$, the fourth sequence $\boldsymbol{D_{u,i}}$ is used to permutate OFDM samples at the time domain. By letting the total number of time-domain subcarriers equal $N = (N_d + l_I + l_p)$, according to the order of the digital values in $\boldsymbol{D_{u,i}}$, a $N \times N$ scrambling matrix $\boldsymbol{M_{u,i}}$ can be generated, and, as such, time-domain OFDM symbols permutation can be implemented as follows:

$$\overline{\boldsymbol{S}}_{\boldsymbol{i}} = M_{u,i-1}\boldsymbol{S}_{\boldsymbol{i}}, \tag{17}$$

where $M_{u,i-1}$ is the scrambling matrix generated from $\boldsymbol{D}_{\boldsymbol{u,i-1}}$ during the $(i-1)_{\text{th}}$ frame; $\overline{\boldsymbol{S}}_{\boldsymbol{i}}$ denotes the permuted time-domain OFDM samples. The input data is randomly used to produce dynamic cypher keys. Using (17), to detect the current signal $\boldsymbol{S}_{\boldsymbol{i}}$, Eavesdropper requires knowing $\boldsymbol{S}_{\boldsymbol{i-1}}$ to generate $\boldsymbol{M}_{\boldsymbol{u,i-1}}$ (which was used for $\boldsymbol{S}_{\boldsymbol{i}}$ encryption); therefore, the entire historic OFDM signals are mandatory for recovering the successive signal. In contrast to the methods in [13-16] that produce static chaotic keys with statistical features that are useful for vicious nodes, the proposed approach produces dynamic cypher keys that are related to random input data that can disrupt such statistic types, and, therefore, it ensures high statistical attack protection.

In this context, we presume that the initial key used for generating the initial hyperchaotic values to encrypt the first frame throughout the session will be securely shuffled between the receiver and the transmitter during the connection installation process. In [7], the authors implemented a chaotic protocol to generate a key by utilizing position-sensitive and real-valued channel state information of the VLC channel.

The received signal is provided at the receiving node as follows:

$$\overline{\boldsymbol{Z}}_{\boldsymbol{i}} = \boldsymbol{h} \otimes (r \cdot \overline{\boldsymbol{S}}_{\boldsymbol{i}}) + \boldsymbol{n}, \tag{18}$$

where r is the responsivity of the photodetector, $\boldsymbol{n}$ denotes the shot and thermal noises (modeled as an AWGN process), $\otimes$ denotes convolution, and $\boldsymbol{h}$ denotes the impulse response of the channel . Note that the optical channel's time-domain impulse response has been obtained by [17]. In line-of-sight channel scenario, a common scenario, the channel DC gain $h(0)$ from the transmitter to the receiver is given as:

$$h(0) = \frac{(m+1)A_{pd}}{2\pi \mathrm{D}^2} cos^m(\emptyset)\cos(\varphi), \tag{19}$$

where m denotes the order of Lambertian emission, A_{pd} is the physical area of the detector, D denotes the Euclidean distance between the receiver and transmitter, and $\emptyset$ and φ denote the radiance and incident angles, respectively. We presume that the effect of multi-path fading is eliminated with the zero-forcing (ZF) equalizer [5]; the sampled filter output can be obtained after equalization as follows:

$$\overline{\boldsymbol{Z}}_{\boldsymbol{i}} = r \cdot \overline{\boldsymbol{S}}_{\boldsymbol{i}} + \boldsymbol{h}^{-\mathbf{1}} \otimes \boldsymbol{J} + \boldsymbol{h}^{-\mathbf{1}} \otimes \boldsymbol{n}. \tag{20}$$

The component $\boldsymbol{h}^{-\mathbf{1}} \otimes \boldsymbol{n}$ has a significant effect only on the beginning of $\overline{\boldsymbol{Z}}_{\boldsymbol{i}}$, which can be extracted by eliminating the CP samples of ISI [5]. After obtaining $\overline{\boldsymbol{Z}}_{\boldsymbol{i}}$, the samples are de-permuted by $\boldsymbol{M}_{\boldsymbol{u},\boldsymbol{i}-\mathbf{1}}$ produced by $\boldsymbol{D}_{\boldsymbol{u},\boldsymbol{i}-\mathbf{1}}$ at $(i-1)_{\text{th}}$ frame as follows:

$$\boldsymbol{Z}_{\boldsymbol{i}} = \boldsymbol{M}_{\boldsymbol{u},\boldsymbol{i}-\mathbf{1}} \overline{\boldsymbol{Z}}_{\boldsymbol{i}}, \tag{21}$$

where $\boldsymbol{Z}_{\boldsymbol{i}}$ denotes the de-permuted OFDM signal received at the i_{th} frame. This signal contains $\boldsymbol{Z}_{\boldsymbol{i}}^{\boldsymbol{d}}$, which is the OFDM data signal, as well as $\boldsymbol{Z}_{\boldsymbol{i}}^{\boldsymbol{c}}$, which is the CP signal. The protected CP samples of $\boldsymbol{Z}_{\boldsymbol{i}}^{\boldsymbol{c}}$ are used for generating the primary key $\boldsymbol{c}_{\boldsymbol{i}}$ to update the quantities for the chaotic approach, as illustrated in Fig. 1. These quantities are maintained at a legitimate receiver to generate the chaos sequences $\boldsymbol{D}_{\boldsymbol{x},\boldsymbol{i}}, \boldsymbol{D}_{\boldsymbol{y},\boldsymbol{i}}, \boldsymbol{D}_{\boldsymbol{z},\boldsymbol{i}}$, and $\boldsymbol{D}_{\boldsymbol{u},\boldsymbol{i}}$, which are used to decrypt the received OFDM signal during the $(i+1)_{\text{th}}$ frame. After the creation of the secret quantities, $\boldsymbol{Z}_{\boldsymbol{i}}^{\boldsymbol{c}}$ is eliminated, and, to produce the phase-scrambled signal $\overline{\boldsymbol{Y}}_{\boldsymbol{i}}$, $\boldsymbol{Z}_{\boldsymbol{i}}^{\boldsymbol{d}}$ is added to the IFFT, which is the receiving form of $\overline{\boldsymbol{X}}_{\boldsymbol{i}}$. The signal is de-scrambled by $\boldsymbol{k}_{\boldsymbol{i}-\mathbf{1}}$, which is generated from $\boldsymbol{D}_{\boldsymbol{z},\boldsymbol{i}-\mathbf{1}}$ using a binarization operation at the $(i-1)_{\text{th}}$ frame, as follows:

$$\widehat{\boldsymbol{Y}}_{\boldsymbol{i}} = \overline{\boldsymbol{Y}}_{\boldsymbol{i}} .* \boldsymbol{k}_{\boldsymbol{i}-\mathbf{1}}, \tag{22}$$

where $\widehat{\boldsymbol{Y}}_{\boldsymbol{i}}$ denotes the phase-encryption output, the receiving form of $\widehat{\boldsymbol{X}}_{\boldsymbol{i}}$. After obtaining $\widehat{\boldsymbol{Y}}_{\boldsymbol{i}}$, the symbols are de-permuted by $\boldsymbol{M}_{\boldsymbol{y},\boldsymbol{i-1}}$ produced by $\boldsymbol{D}_{\boldsymbol{y},\boldsymbol{i-1}}$ at the $(i-1)_{\text{th}}$ frame as follows:

$$\boldsymbol{Y}_{\boldsymbol{i}} = \boldsymbol{M}_{\boldsymbol{y},\boldsymbol{i-1}}\widehat{\boldsymbol{Y}}_{\boldsymbol{i}}, \tag{23}$$

where $\boldsymbol{Y}_{\boldsymbol{i}}$ denotes the de-permuted frequency-domain OFDM signal, the receiving form of $\boldsymbol{X}_{\boldsymbol{i}}$. The QAM demodulator is finally applied, after that, an XOR decryption operation by the key $\boldsymbol{B}_{\boldsymbol{i-1}}$, defined by the sequence $\boldsymbol{D}_{\boldsymbol{x},\boldsymbol{i-1}}$, can be applied to $\boldsymbol{Y}_{\boldsymbol{i}}$ to recover the data.

By obtaining the mutual information L between the data sent by the legitimate transmitter U^T and the data recovered by the snooper V^S, the security of our approach can be quantitatively assessed supposing that every transmitted bit has an equal probability of being zero or one. This can be described as follows [18]:

$$\begin{aligned} L &= I(V^S; U^T) \\ &= H(V^S) - H(V^S|U^T), \\ &= 1 + P_s log_2 P_s + (1-P_s)\log_2(1-P_s), \end{aligned} \tag{24}$$

where P_s denotes the snooper bit error rate (BER); H denotes the process of entropy. Consequently, we can obtain the data secrecy capacity C_d as follows:

$$\begin{aligned} C_d &= \max\left[I(U^T; V^r) - I(U^T; V^S)\right] \\ &\geq H(V^r) - H(V^r|U^T) - \left(H(V^S) - H(V^S|U^T)\right) \\ &= P_r\log_2 P_r + (1-P_r)\log_2(1-P_r) - P_s\log_2 P_s - (1-P_s)\log_2(1-P_s), \end{aligned} \tag{25}$$

where V^r denotes the data retrieved by the legitimate receiver; P_r indicates the legitimate receiver's BER.

3. RESULTS AND DISSCUSSION

We performed Monte Carlo simulation to develop our hyperchaos-KG-OOFDM

approach depicted in Fig.1. We utilized 64-QAM as a modulation scheme, $N_d = 512$, and $\boldsymbol{l_I} = \boldsymbol{l_p} = \frac{\boldsymbol{N_d}}{\boldsymbol{8}}$. The BER simulation is shown in Fig. 2 along with C_d and the key-mismatch rate (KMR) performances of the proposed hyperchaos-KG-OOFDM (conducted using the proposed phase-encryption process as well as polarity encryption, which was used by [5–7]). The findings have been compared with traditional optical OFDM, i.e., DCO-OFDM [19], with no key generation and encryption operations. In the simulation, a transmitter at $(2.5, 2.5, 3)$ with a $70\,°$ half-power semi-angle and 1-W power was used. A legitimate receiver with a $85\,°$ half-angle field of view at $(1.5, 1.5, 0)$ was utilized. As Fig. 2 reveals, the KMR and BER performances of phase-encryption hyperchaos-KG-OOFDM are superior to those of polarity encryption hyperchaos-KG-OOFDM due to distortion in the polarity encryption of the OFDM subcarriers. Moreover, the BER output of hyperchaos-KG-OOFDM with phase encryption is superior to that of standard optical OFDM. In essence, the addition of scrambling enables our method to enhance the efficiency of BER optical OFDM systems in addition to providing security support. For secrecy performance, hyperchaos-KG-OOFDM has comparable performance for both polarity encryption and phase encryption; secrecy capacity is not supported by conventional optical OFDM. Fig. 2 also indicates the snooper performance, which is located at $(3, 3, 0)$. The hidden keys were unknown to the snoopers, and they could not retrieve the data.

The time-domain OFDM $\boldsymbol{S_i}$ PAPR has been calculated by [10]:

$$PAPR_i = \frac{max_{k=1,\ldots,\ell N_s}|S_{ik}|^2}{\frac{1}{\ell N_s}\sum_{k=1}^{\ell N_s}|S_{ik}|^2} = \frac{\|\boldsymbol{S_i}\|_\infty^2}{\frac{1}{\ell N_s}\|\boldsymbol{S_i}\|_2^2}, \tag{26}$$

where ℓ denotes the oversampling factor, which is 10 in this work. According to (26), when the frequency-domain OFDM subcarriers are in phase (or relatively in phase), higher peaks can be observed in the time-domain OFDM samples. If the original input data consists of images, then a number of correlation pixels will exist in the images. After encoding and modulation, it is likely that some resulting subcarriers will be in phase or

relatively in phase in the frequency-domain OFDM symbols. Accordingly, higher PAPR values exist for the time-domain signals produced by traditional optical OFDM systems. The phase encryption in the suggested approach reduces the probability of in phase and relatively in phase symbols in the frequency-domain OFDM subcarrier. as a result, it decreases the PAPR of the time-domain OFDM signal and improve the OFDM device efficiency. Fig. 3 compares the hyperchaos-KG-OOFDM with traditional optical OOFDM, from which it is evident that the proposed method improves the PAPR signal efficiency.

To investigate the sensitivity of our chaotic scheme, Fig. 4 shows the BER as a function of the difference between two chaotic quantities, i.e. x_1 and x_2. As depicted, the encrypted data cannot be detected when the difference value is more than 10^{-15}. This indicates the high-security support by the method.

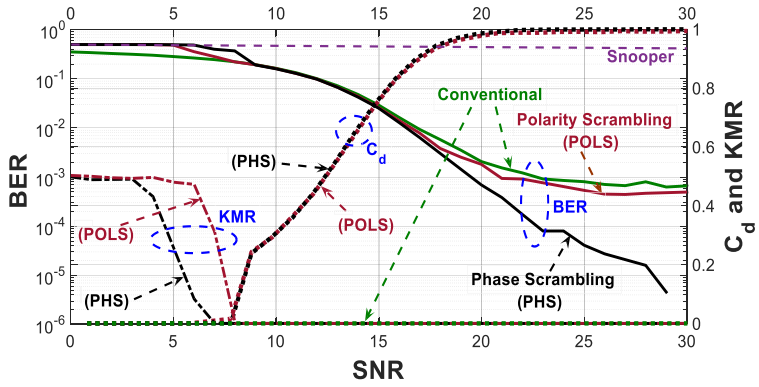

Fig. 2. Performance of the optical OFDM methods.

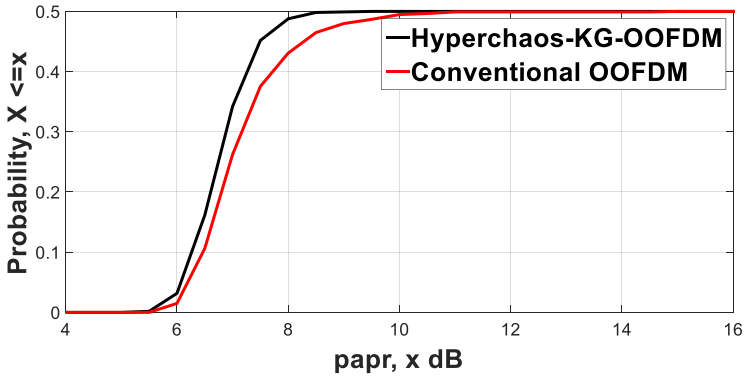

Fig. 3. PAPR of the optical OFDM methods.

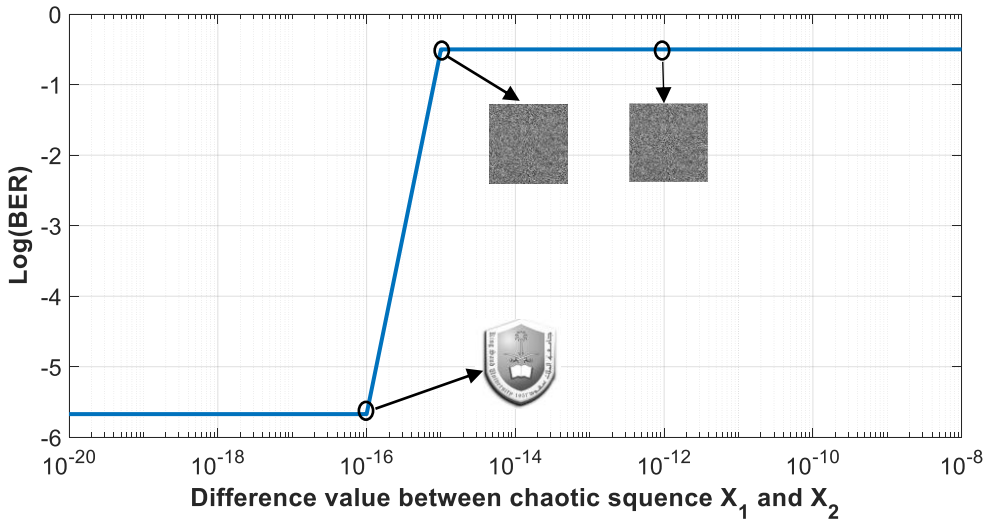

Fig. 4. Correlation matrix of the primary keys.

To investigate the statistical feature of the proposed method, Fig. 5 gives The histograms and Welch's power spectral densities of the clear and encrypted data. From Fig. 5, the redundancy in the clear image is hidden in the pixel distribution of the encrypted image and there is no clue about the clear image. Also, from the figure, the fluctuant power spectrum of the clear image is destroyed in the case of the encrypted image. Thus, our method provides the capability against statistical attacks.

Figure 6 shows the matrix of normalized correlation for the 318 primary dynamic keys retrieved throughout the whole communication time. A peak correlation can only be seen among the identical keys, and a minimal correlation was demonstrated among the different keys. Throughout the whole session, our approach produced uncorrelated keys and, consequently, extremely different chaotic quantities that are modified for each frame. Our approach, therefore, offers a high degree of confidentiality against statistical and correlation attacks.

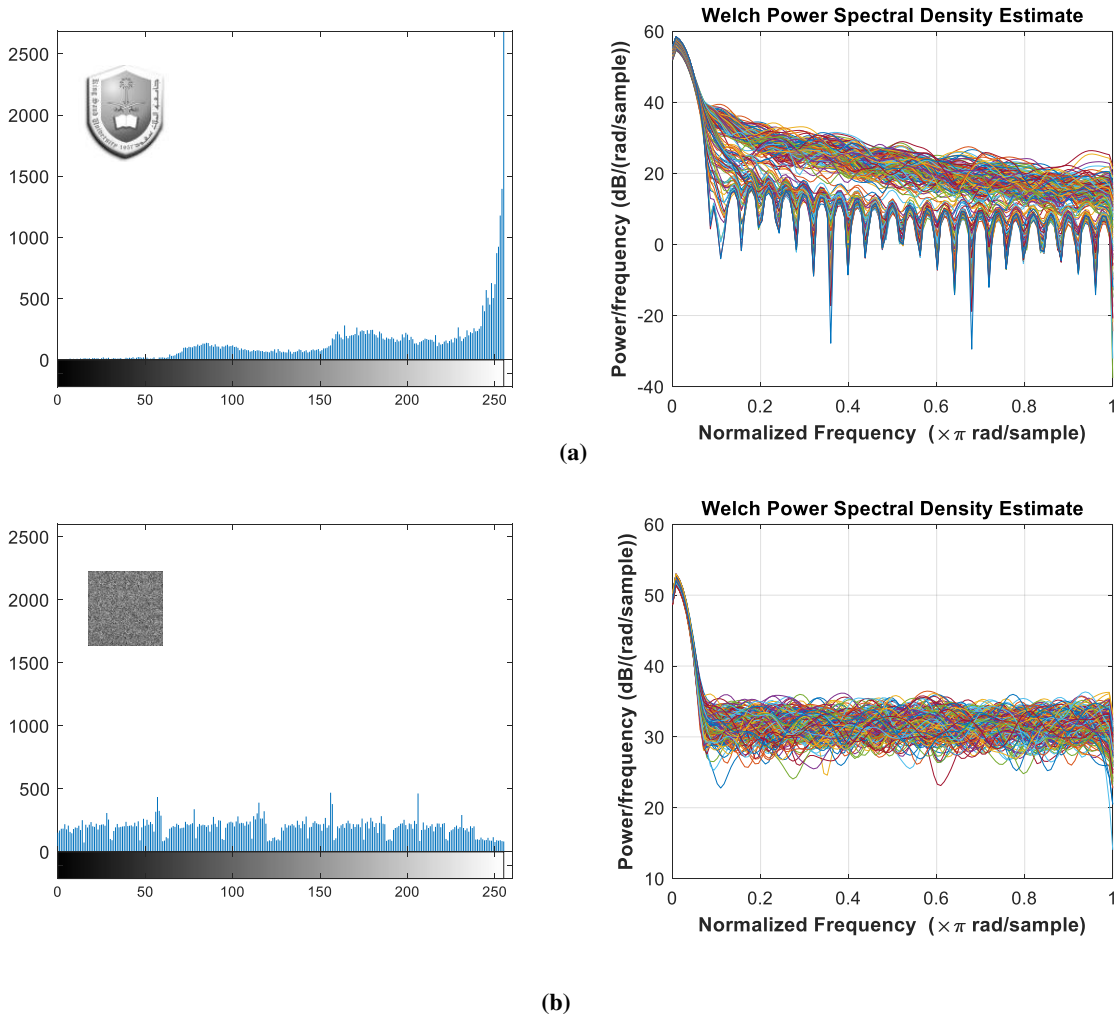

Fig. 5. Histograms and Welch's power spectral density. (a) Clear and (b) encrypted image

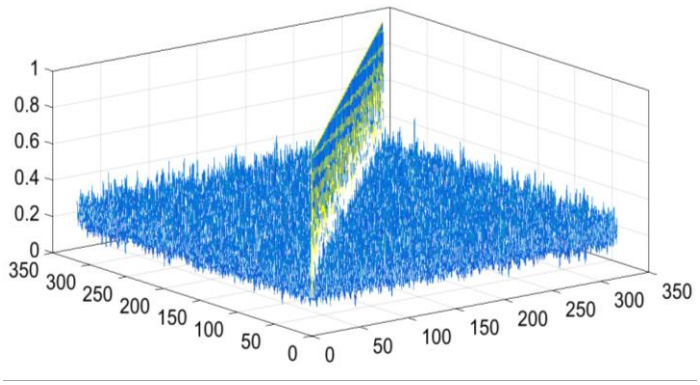

Figure 6. Correlation matrix of the primary keys.

4. CONCLUSION

In this paper, we proposed a hyperchaos-KG-OOFDM approach to enhance the confidentiality of VLC systems. With the aid of a hyperchaotic 4D method, real bipolar OFDM samples were utilized to generate dynamic cypher keys that are altered at each frame, thereby ensuring a high degree of protection to counter statistical and correlation attacks. Besides confidentiality support, our approach also decreases the PAPR and improves the secrecy capacity and BER efficiency of OFDM-based VLC networks.

Abbreviations

VLC: Visible light communication; OFDM: orthogonal frequency division multiplexing; CP: cyclic prefix; KG-OOFDM: key generation based optical orthogonal frequency division multiplexing; IFFT: inverse fast Fourier transformation; PAPR: peak-to-average power; 4D: four-dimensional; HS: Hermitian Symmetry; Conca.: Concatenation; DAC: Digital-to-Analog Converter; DC: Direct Current; E/O: Electrical to Optical; O/E: Optical to Electrical; ADC: Analog-to-Digital Converter; mod: modulo operation; ISI: Inter-symbol interference; AWGN: Additive white gaussian noise; DC: Direct current; ZF: zero-forcing; QAM: Quadrature amplitude modulation; BER: bit error rate; KMR: key-mismatch rate.

ACKNOWLEDGMENT

The authors would like to thank Deanship of Scientific Research (DSR) in King Saud University for funding and supporting this research through the initiative of Graduate Students Research (GSR) Support.

Authors' contributions

All authors made contributions in all parts of the manuscript. All authors read and approved the final manuscript.

Funding

This research was partially funded by Deanship of Scientific Research (DSR) in King Saud University for funding and supporting this research through the initiative of Graduate Students Research (GSR) Support.

Availability of data and materials

Not available online.

Declarations

Ethics approval and consent to participate

Not applicable.

Consent for publication

Not applicable.

Competing interests

The authors declare that they have no competing interests.

References

[1] J. M. Hamamreh et al., "Classifications and applications of physical layer security techniques for confidentiality: A comprehensive survey," IEEE Commun. Surv. Tutorials, vol. 21, no. 2, pp. 1773-1828, 2019.

[2] A. Mostafa and L. Lampe, "Optimal and robust beamforming for secure transmission in MISO visible-light communication links," IEEE Trans. Signal Process., vol. 64, no. 24, pp. 6501-6516, 2016.

[3] T. V. Pham et al., “Artificial-noise-aided precoding design for multi-user visible light communication channels,” IEEE Access, vol. 7, pp. 3767-3777, 2019.

[4] S. Cho et al., “Enhancement of physical layer security with simultaneous beamforming and jamming for visible light communication systems,” IEEE Trans.Inform.Forensic. Secur., vol. 14, no. 10, pp. 2633-2648, 2019.

[5] Y. M. Al-Moliki et al., “Robust key generation from optical OFDM signal in indoor VLC networks,” IEEE Photon. Technol. Lett., vol. 28, no. 22, pp. 2629-2632, 2016.

[6] Y. M. Al-Moliki et al., “Secret key generation protocol for optical OFDM systems in indoor VLC networks,” IEEE Photon. J., vol. 9, no. 2, pp. 1-15, 2017.

[7] Y. M. Al-Moliki et al., “Chaos-based physical-layer encryption for OFDM-based VLC schemes with robustness against Known/chosen plaintext attacks,” IET Optoelectron., vol. 13, no. 3, pp. 124-133, 2018.

[8] Y. M. Al-Moliki, M. T. Alresheedi and Y. Al-Harthi, "Improving Availability and Confidentiality via Hyperchaotic Baseband Frequency Hopping Based on Optical OFDM in VLC Networks," in IEEE Access, vol. 8, pp. 125013-125028, 2020

[9] T. Rouphael, “Common digital modulation methods” in RF and Digital Signal Processing for Software-Defined Radio. Australia: Newnes, 2009, pp. 25-85, ch. 3.

[10] Y. Wang et al., “Optimized signal distortion for PAPR reduction of OFDM signals with IFFT/FFT complexity via ADMM approaches,” IEEE Trans. Signal Process., vol. 67, no. 2, pp. 399-414, 2019.

[11] M. Cheng et al., “Security-enhanced OFDM-PON using hybrid chaotic system,” IEEE Photon. Technol. Lett., vol. 27, no. 3, pp. 326-329, 2015.

[12] X. Hu et al., “Chaos-based partial transmit sequence technique for physical layer security in OFDM-PON,” IEEE Photon. Technol. Lett., vol. 27, no. 23, pp. 2429-2432, 2015.

[13] Z. Wang and W. Qiu, ‘‘Secure image transmission over DFT-precoded OFDM-VLC systems based on chebyshev chaos scrambling,’’ Opt. Commun., vol. 397, pp. 84–90, Aug. 2017.

[14] Z. Wang, F. Chen, W. Qiu, S. Chen, and D. Ren, ‘‘A two layer chaotic encryption scheme of secure image transmission for DCT precoded OFDM-VLC transmission,’’ Opt. Commun., vol. 410, pp. 94–101, Mar. 2018.

[15] M. Gao, C. Li, and Z. Xu, ‘‘Performance enhancement of LED-based indoor OFDM-VLC system using digital chaotic scheme,’’ Opt. Commun., vol. 439, pp. 21–26, May 2019.

[16] Z. Wang, Z. Wang, and S. Chen, ‘‘Encrypted image transmission in OFDMbased VLC systems using symbol scrambling and chaotic DFT precoding,’’ Opt. Commun., vol. 431, pp. 229–237, Jan. 2019.

[17] J. R. Barry et al., “Simulation of multipath impulse response for indoor wireless optical channels,”, IEEE J. Select. Areas Commun., vol. 11, no. 3, 367-379, 1993.

[18] H. Li et al., “Dynamic subcarrier coordinate interleaving for eavesdropping prevention in OFDM systems,” IEEE Commun. Lett., vol. 18, no. 6, pp. 1059-1062, 2014.

[19] S. D. Dissanayake and J. Armstrong, “Comparison of ACO-OFDM, DCO-OFDM and ADO-OFDM in IM/DD systems,” J. Lightwave Technol., vol. 31, no. 7, pp. 1063-1072, 2013.

Figures

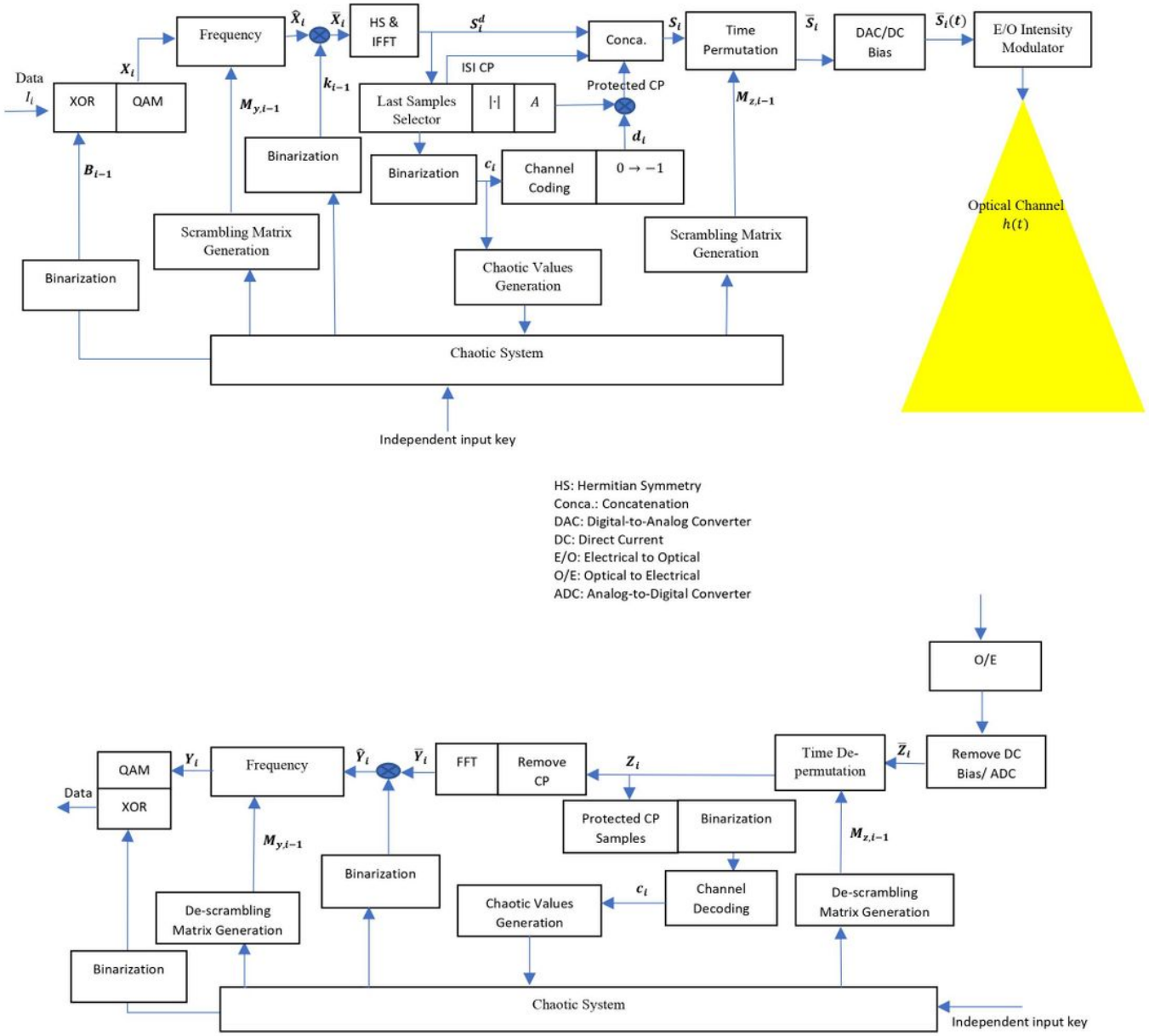

Figure 1

Proposed hyperchaos-KG-OOFDM method

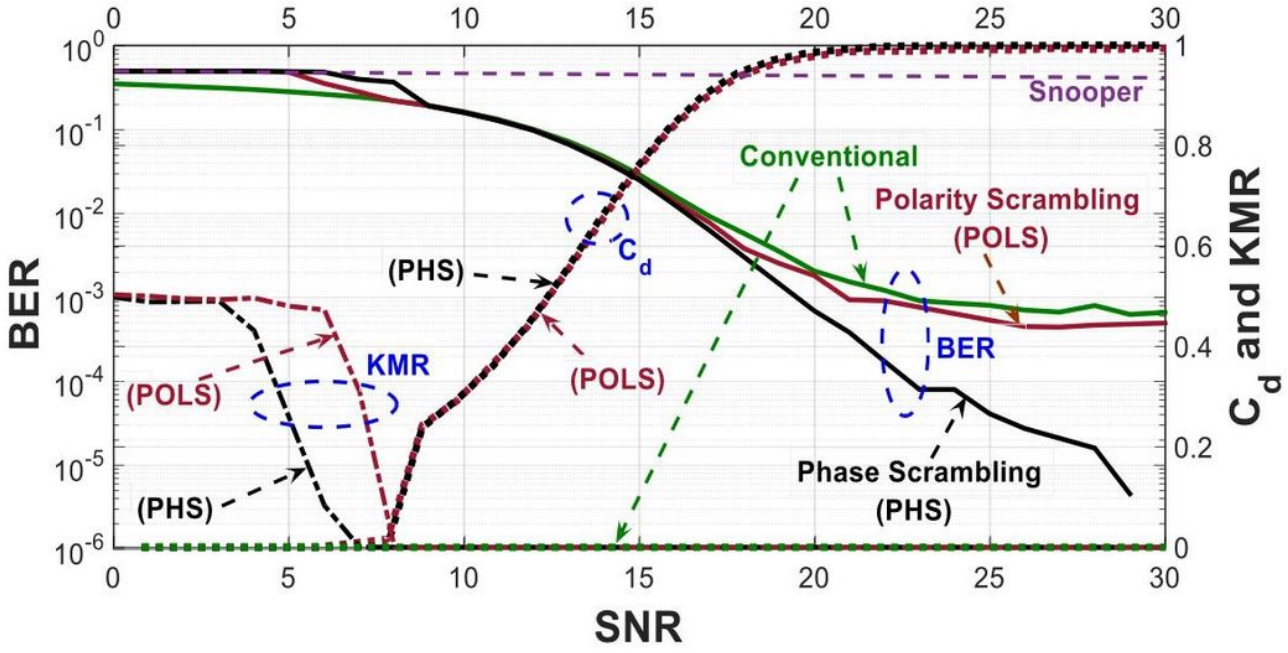

Figure 2

Performance of the optical OFDM methods.

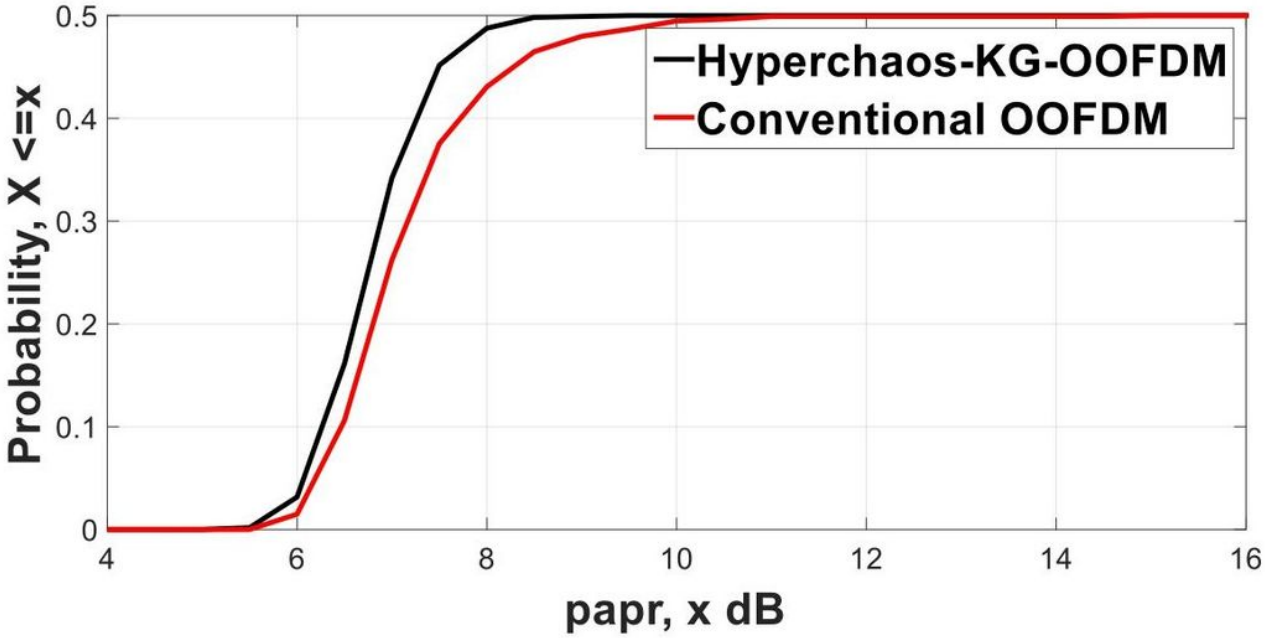

Figure 3

PAPR of the optical OFDM methods.

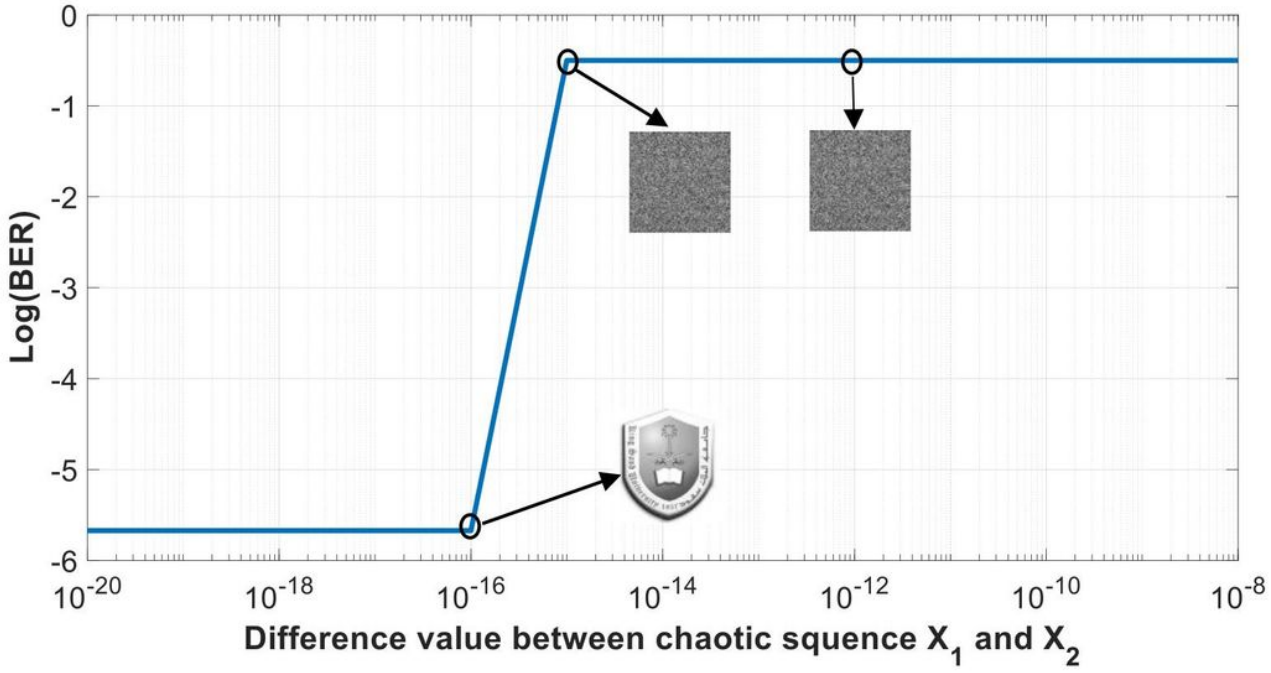

Figure 4

Correlation matrix of the primary keys.

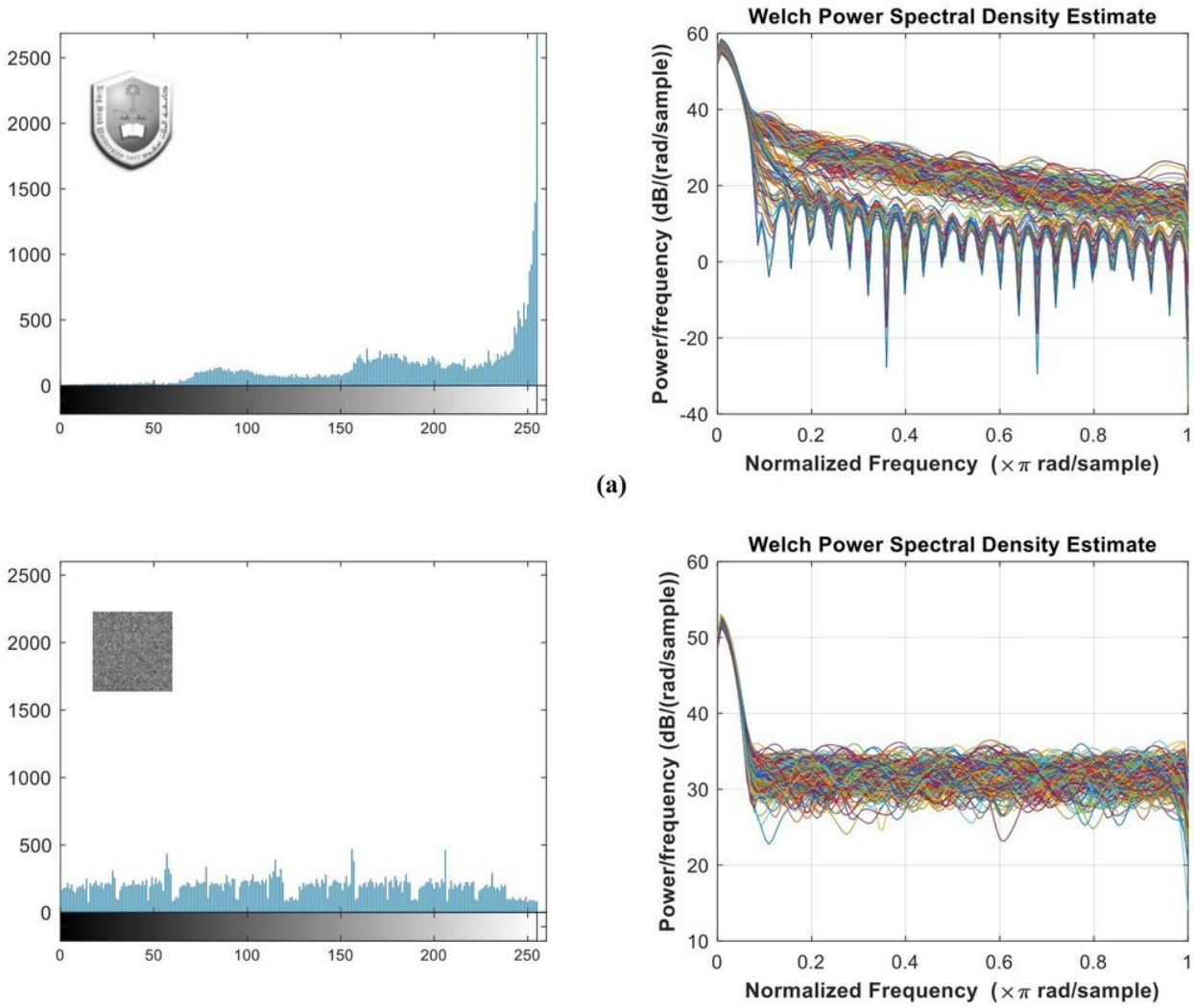

Figure 5

Histograms and Welch's power spectral density. (a) Clear and (b) encrypted image

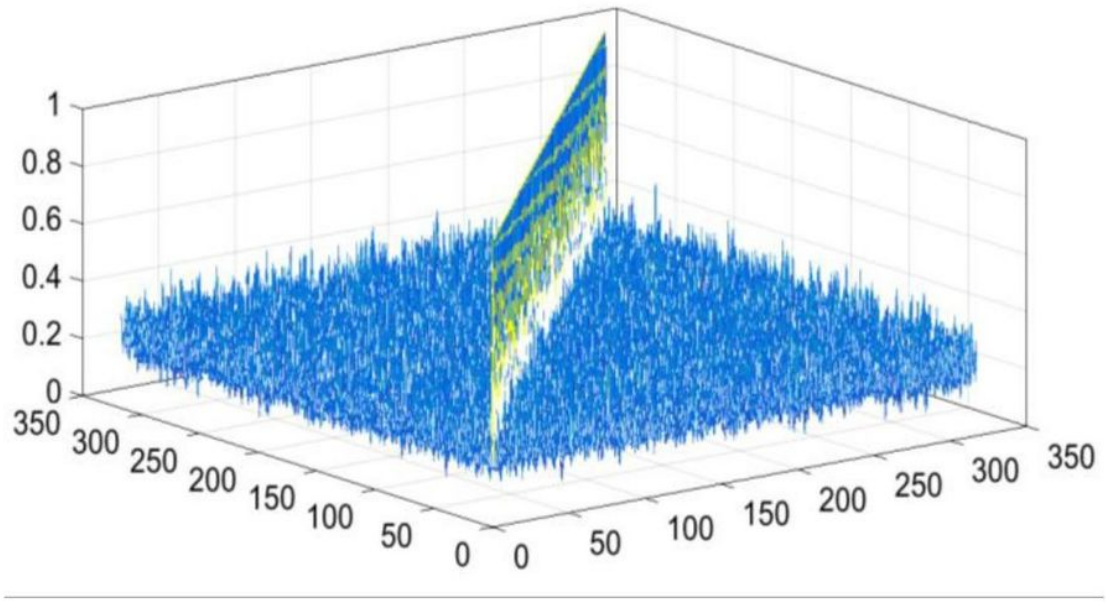

Figure 6

Correlation matrix of the primary keys.