Eur. Phys. J. Plus (2017) **132**: 524
DOI 10.1140/epjp/i2017-11808-x

THE EUROPEAN
PHYSICAL JOURNAL PLUS

Regular Article

Audio signal encryption using chaotic Hénon map and lifting wavelet transforms*

Animesh Roy[a] and A.P. Misra[b]

Department of Mathematics, Siksha Bhavana, Visva-Bharati University, Santiniketan - 731 235, India

Received: 22 August 2017 / Revised: 26 November 2017
Published online: 18 December 2017 – © Società Italiana di Fisica / Springer-Verlag 2017

Abstract. We propose an audio signal encryption scheme based on the chaotic Hénon map. The scheme mainly comprises two phases: one is the preprocessing stage where the audio signal is transformed into data by the lifting wavelet scheme and the other in which the transformed data is encrypted by chaotic data set and hyperbolic functions. Furthermore, we use dynamic keys and consider the key space size to be large enough to resist any kind of cryptographic attacks. A statistical investigation is also made to test the security and the efficiency of the proposed scheme.

1 Introduction

Encryption of optical audio or video files and digital images received renewed interest in the processes of information hiding and information security in social networks, communications, Internet, such as in the segregation of the design decisions in computer programs that are like to change, thereby protecting other parts of the program from extensive modification if the design decision is changed, privacy protection, mobile or digital phones, tactical military systems to prevent transmitters being located, and many more. Both the information hiding techniques and cryptography have received much attention in recent times owing to the rapid developments of digital media and digital right management systems [1–9]. There are many different schemes for the encryption of multimedia data, like audio signal, of which adding noise is one. However, the encryption of an audio signal requires different transformation of maps from that of images and a strong level of security, so they are the subject of detailed cryptanalysis. Furthermore, in the advancement of security level, chaotic maps or dynamical systems play a vital role in the encryption process because of its ergodicity, randomness and sensitiveness to initial conditions [5,6]. The behavior of a dynamical system is predictable if the initial conditions are known, otherwise the system exhibits randomness. The latter can be used to induce confusion and diffusion in the plain text and thereby enabling the data transmission safely through insecure channels [1,2,5,6]. Thus, designing of a new encryption algorithm is very much required to secure audio files from any kind of attack for safe storing and transmission [7].

In this work, we propose a scheme that is used to encrypt an optical audio signal. Our starting point is to transform the audio signal into a data signal using the lifting wavelet scheme [10] instead of the fast Fourier transform. The latter is not well accepted in the context of cryptography. However, the lifting scheme has many advantages in constructing wavelets compared to the conventional wavelet transform techniques. A few techniques are demonstrated in sect. 2.2. On the other hand, optical or digital audio signals are usually a sequence of integers, and applying simply the wavelet transforms to them results in floating point numbers. In this way an efficient algorithm is required which converts integers into integers. The lifting scheme of wavelet transforms can fulfill the purpose for digital speech compression. Furthermore, we use the Hénon map [11] in our encryption scheme. Such a map has been extensively studied due to its low dimension (two-dimensional) and chaotic dynamics [1]. The properties of the map are also briefly discussed in sect. 2.1.

In the literature, several encryption schemes have been proposed. For example, Kordov and Bonchev [7] proposed an audio encryption algorithm based on a circle map. However, their scheme does not give any satisfactory decryption as it is not clear how one properly decrypts the encrypted audio by XOR operation. Belazi *et al.* [1] constructed

* Contribution to the Focus Point on "Systems and Security: Advanced Methods with Chaos and Complexity" edited by S. Banerjee.

[a] e-mail: aroyiitd@gmail.com

[b] e-mail: apmisra@gmail.com (corresponding author)

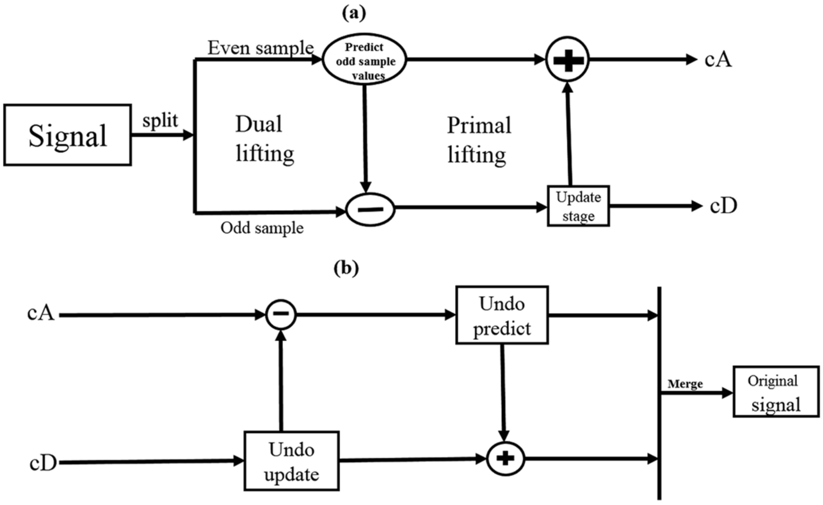


Fig. 1. An illustration of the forward (panel (a)) and the inverse (panel (b)) lifting schemes.

a chaos-based partial image encryption scheme based on linear fractional and lifting wavelet transforms. However, a chaos-based audio signal encryption scheme using the lifting wavelet scheme has not been reported before.

The manuscript is organized as follows: Some preliminary concepts of the Hénon map and the lifting scheme are briefly discussed in sect. 2. Section 3 presents the proposed scheme comprising the lifting scheme for audio signals, the generation of chaotic data for encryption and decryption and the key representation for encryption and decryption. Furthermore, a security analysis is carried out in sect. 4. Finally, the results are concluded in sect. 5.

2 Some preliminaries

The proposed encryption and decryption scheme of audio signals is based on the Hénon map and the lifting wavelet scheme. These are briefly discussed in the following two subsects. 2.1 and 2.2.

2.1 Hénon's map

The Hénon map is described as [11]

$$\begin{aligned} x_{n+1} &= 1 - \alpha x_n^2 + y_n, \\ y_{n+1} &= \beta y_n, \end{aligned} \tag{1}$$

where α (> 0) and β (> 0) are bifurcation parameters. The Hénon map (1) has quadratic nonlinearity and strange attractors as its chaotic solutions. The model was proposed by Michel Hénon as a simplified model of the Poincaré map which appears from a solution of the Lorenz equations. Furthermore, the parameter β is a measure of the rate of area contraction which is independent of x_n and y_n. Note that, for $\beta = 0$, eq. (1) reduces to the map which exhibits period doubling route to chaos.

In our scheme the solution of eq. (1) will be taken as computational tools instead of an illustration of the physical dynamics. The chaotic data set, obtained from eq. (1) for some particular values of α and β, are used to generate key vectors with sine and cosine hyperbolic functions for encryption.

2.2 Lifting wavelet scheme

The lifting scheme, as introduced by Sweldens [10], is a simple construction of second-generation wavelets, as well as wavelets that are not necessarily translates or dilates of one fixed function in the spatial domain and has the capability of time-frequency localization. It is faster, efficient and requires low-power applications, less memory space and, in contrast to the traditional wavelet transforms, it does not require any complex mathematical calculation and does not have any quantization error.

The lifting scheme is composed of three phases: Split/Merge, Prediction and Update. The details are illustrated in fig. 1:

- Split: The input data signal is split up into odd and even sample values.
- Predict: The even samples are used to predict the odd samples.
- Update: The even samples are obtained by a linear combination of the set to be obtained from the predict step.

3 The proposed scheme

In this section we systematically demonstrate the lifting wavelet scheme applied to an audio signal, to obtain the chaotic data set from the Hénon map (1) and its application for the generation of key vectors in the encryption and decryption processes.

3.1 Lifting scheme for audio signals

We itemize the lifting scheme as follows. The details for the encryption and decryption are illustrated in fig. 1.

Step 1: Read the audio file and store as data in the form $[y, f_s] = \text{audioread}(\texttt{sample.mp3})$, where f_s (in hertz) is the frequency and y is the size of the signal.
Step 2: Take the z-transform of the signal data vector y as

$$f(z) = \sum_i y_i z^{-i}, \tag{2}$$

where i denotes the length of the vector. This representation is called the poly-phase representation of the signal data.
Step 3: The audio signal data vector is split up into disjoint components. A common way to do this is to extract the even and odd poly-phase components. The z-transform of the even poly-phase component is

$$f_e(z) = \sum_i y_{2i} z^{-i}. \tag{3}$$

The z-transform of the odd poly-phase component is

$$f_o(z) = \sum_i y_{2i+1} z^{-i}. \tag{4}$$

Next, we write the z-transform of the input signal as the sum of dilated versions of the z-transforms of the poly-phase components:

$$f(z) = f_e(z^2) + z^{-1} f_o(z^2). \tag{5}$$

This is known as the lazy wavelet or splitting stage.
Step 4: This step is the predict phase in which the odd poly-phase components are predicted from a linear combination of the set of the even poly-phase components. This predict phase ensures polynomial cancellation in high pass. The set of odd poly-phase components is then replaced by the difference between the odd poly-phase components and the predicted values. The predict operation is also referred to as the dual lifting step.

$$\text{Let } \alpha_i \longleftarrow y_{2i} \quad \text{and} \quad \beta_i \longleftarrow y_{2i-1} \ldots \text{ (split)}$$
$$\beta_i \longleftarrow \beta_i - \frac{1}{2}(\alpha_i + \alpha_{i+1}) \ldots \text{ (predict)}.$$

Step 5: This step is the update phase in which the even poly-phase components are obtained by a linear combination of the set to be obtained from the predict step. This step is also referred to as the primal lifting step and it ensures preservation of moments in low pass.

$$\alpha_i \longleftarrow \alpha_i + \frac{1}{4}(\beta_{i-1} + \beta_i) \ldots \text{ (update)}.$$

In practice, a normalization is done for both the primal and the dual lifting processes.

This is how we transform the audio signal into a data vector by lifting the scheme of wavelet transforms. The next stage will be the encryption and decryption scheme to be discussed later. However, after the decryption process, the transformed data set is to be recovered in the form of audio signal with the help of inverse lifting scheme stated below:

- Inverse primal lifting: $\alpha_i \longleftarrow \alpha_i - \frac{1}{4}(\beta_{i-1} + \beta_i)$.
- Inverse dual lifting: $\beta_i \longleftarrow \beta_i + \frac{1}{2}(\alpha_i + \alpha_{i+1})$.
- Merge: $\alpha_i \longrightarrow y_{2i}$ and $\beta_i \longrightarrow y_{2i-1}$.

This transformation gives more fruitful values than the fast Fourier transformation and it estimates the high pick audio signal for the recover section from the original data set transmitted by the sender.

3.2 Generation of chaotic data for encryption and decryption

We generate chaotic data set from eq. (1) for a particular set of values of the parameters α and β, *e.g.*, $\alpha = 1.4$ and $\beta = 0.3$, together with the initial condition $x_0 = 0.01$, $y_0 = 0.003$. The chaotic data set so obtained are then arranged as vectors according to the size of the audio data set in the following process:

- $l \longleftarrow$ length(audioread(`sample.mp3`)).
- When l is even, then

$$\begin{aligned} &Y_{k_1} \longleftarrow \text{uint8}\left([\cos(\phi/i)y(k_1) + \sin(\phi/i)y(k_1+1)] \times 10^9\right),\\ \text{for}\quad &k_1 = 1,2,\ldots,\frac{l}{2};\quad i = 1,2,\ldots,l \text{ and } 0 \leq \phi \leq \pi/2;\\ &Y_{k_2} \longleftarrow \text{uint8}\left([\sin(\phi/i)y(k_2) - \cos(\phi/i)y(k_2+1)] \times 10^9\right),\\ \text{for}\quad &k_2 = \frac{l}{2},\ \frac{l}{2}+1,\ \frac{l}{2}+2,\ldots,l-1;\quad i = 1,2,\ldots,l \text{ and } 0 \leq \phi \leq \pi/2. \end{aligned}$$

- When l is odd, then

$$\begin{aligned} &Y_{k_1} \longleftarrow \text{uint8}\left([\cos(\phi/i)y(k_1) + \sin(\phi/i)y(k_1+1)] \times 10^9\right),\\ \text{for}\quad &k_1 = 1,2,\ldots,\left[\frac{l}{2}\right];\quad i = 1,2,\ldots,l \text{ and } 0 \leq \phi \leq \pi/2;\\ &Y_{k_2} \longleftarrow \text{uint8}\left([\sin(\phi/i)y(k_2) - \cos(\phi/i)y(k_2+1)] \times 10^9\right),\\ \text{for}\quad &k_2 = \left[\frac{l}{2}\right]+1,\ \left[\frac{l}{2}\right]+2,\ldots,l-1;\quad i = 1,2,\ldots,l \text{ and } 0 \leq \phi \leq \pi/2. \end{aligned}$$

  Here, $[x]$ denotes the greatest integer $\leq x$.
- The vector $[Y_{k_1}, Y_{k_2}]$ is the well organized chaotic vector which helps key vectors hide in itself and thereby ensuring the encryption process more secured.
  We note that in the calculation of Y_{k_1} and Y_{k_2} for each k_1 and k_2, both i and ϕ vary in the ranges $i = 1,2,\ldots,l$ and $0 \leq \phi \leq \pi/2$, respectively. The sin and cos functions in the square brackets are considered to arrange the chaotic data in a bounded region. Also, those functions are multiplied by 10^9 so as to generate the chaotic data set (with suitable initial conditions) upto nine decimal places. Thus, it may be hard to predict the key values even if one tries with different initial conditions to generate the chaotic data set. Furthermore, the function *uint*8 is used to generate values multiples of 0–255. Thus, any change in the decimal places results into a huge change in the key values.

3.3 Key representation for encryption and decryption

The initial conditions, used to generate chaos, play a vital role in the formation of key points which are sent confidentially to the receiver section. Since the size of the initial condition is small, we form the key matrix in such a way that it is hidden in the chaotic medium. Thus, for the encryption process, we propose two algorithms: one is the key matrix representation and the other is to hide the matrix in the chaotic medium. For decryption we, however, reverse the process to recover the key matrix.

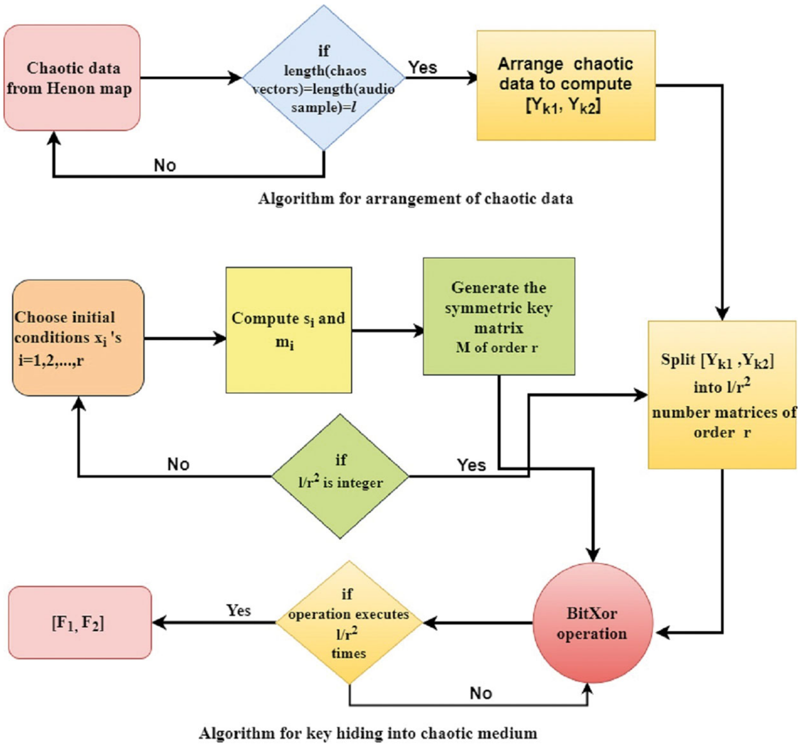
Algorithm for key matrix representation: Let x_0^i, $i = 1,2,\ldots,r$ denote the initial condition which exhibits chaos in eq. (1). The following process may be followed to generate the key matrix.

- Define $s_i = (x_0^i + l)/(2^{16} + l)$ and $m_i = \text{uint8}(\text{mod}(s_i \times 10^{16}, 1))$ for $i = 1,2,\ldots,r$.
- Then the symmetric key matrix, which will be hidden in the chaotic medium, is represented as

$$M = \begin{bmatrix} m_1\ m_2\ m_3\ \ldots\ \ m_r \\ m_2\ m_3\ m_4\ \ldots\ \ m_1 \\ \ldots\ \ldots\ \ldots\ \ldots\ \ \ldots \\ m_r\ m_1\ m_2\ \ldots\ m_{r-1} \end{bmatrix}. \tag{6}$$

In the expression of s_i, the factor 2^{16} is considered to make it much smaller than the unity, and is such that no recurrence decimal representation of s_i occurs. Also, in the definition of m_i, s_i is multiplied by 10^{16} in order to retain the corresponding values up to 16 significant digits (for security reason). Here, mod$(x, 1)$ denotes the binary value 0 or 1.

Algorithm for key hiding in chaotic medium: We construct a chaotic set of vectors which are used to hide the key points in it and help encrypt the audio signal.


Chaotic data from Henon map
if length(chaos vectors)=length(audio sample)=l
Yes
No
Arrange chaotic data to compute [Yk1, Yk2]
Choose initial conditions xi 's i=1,2,...,r
Compute si and mi
Generate the symmetric key matrix M of order r
Split [Yk1 ,Yk2] into l/r2 number matrices of order r
No
if l/r2 is integer
Yes
[F1, F2]
Yes
if operation executes l/r2 times
No
BitXor operation

Algorithm for arrangement of chaotic data

Algorithm for key hiding into chaotic medium

Fig. 2. Flow charts for the arrangement of chaotic data (upper part) and key hiding in chaotic medium (lower part).

- Form a set of l/r^2 number of square matrices of size r from the vectors $[Y_{k_1}, Y_{k_2}]$ obtained in sect. 3.2 as

$$[Y_{k1}, Y_{k2}] \longrightarrow B_{r\times r\times \frac{l}{r^2}}.$$

- Do bit-level operation between each matrix of order $r \times r$ and the matrix M:

$$B'_{r\times r\times i} \longleftarrow B_{r\times r\times i} \oplus M_{r\times r}, \quad \text{for } i = 1, 2, \ldots, \frac{l}{r^2}; \qquad [F_1, F_2] \longleftarrow B'_{r\times r\times \frac{l}{r^2}},$$

  where F_1 and F_2 contain $\frac{l}{2}$ number of elements.
- Repeat the previous step until l/r^2 number of matrices is formed. This step is the mixing part where the key matrix M is being hidden in the chaos sequence.
- Next, we split up the matrix into vectors as $[Y_{k_1}, Y_{k_2}]$ and the new vectors are set as $[F_1, F_2]$.

In our proposed algorithm of encryption and decryption we use hyperbolic functions with $[F_1, F_2]$ and function is chosen in such a way that decryption be the reverse process of encryption. The purpose of taking hyperbolic function is that these functions are not periodic (fig. 2).

3.4 Audio encryption process

The algorithm for encryption is as follows:

- Read the audio data, *e.g.*, in the format (.mp3 or .wav, etc.) as $X \longleftarrow$ audioread(`sample.mp3`).
- Apply the lifting scheme on X to get the two samples corresponding to odd (cA) and even (cD) values, *i.e.*, $[cA, cD] \longleftarrow \mathrm{LWT}(X)$.
- Redefine cA and cD by means of hyperbolic functions for a particular value of θ in $0 < \frac{\theta}{l} \le \frac{\pi}{4}$ as
  $cA'(i) = cA(i)\left(\cosh\left(\frac{\theta}{l}\right) - \sinh\left(\frac{\theta}{l}\right)\right) + F_1(i)\left(\cosh\left(\frac{\theta}{l}\right) + \sinh\left(\frac{\theta}{l}\right)\right)$,
  $cD'(i) = cD(i)\left(\cosh\left(\frac{\theta}{l}\right) - \sinh\left(\frac{\theta}{l}\right)\right) + F_2(i)\left(\cosh\left(\frac{\theta}{l}\right) + \sinh\left(\frac{\theta}{l}\right)\right)$,
  where $i = 1, 2, 3, \ldots, \frac{l}{2}$. In order to make the arguments of the hyperbolic functions random for a particular value of θ, we have considered θ/l instead of simply θ, as different audio file has different lengths l. Such a choice of these aperiodic hyperbolic functions gives much better encryption and decryption in the interval $0 < \frac{\theta}{l} \le \frac{\pi}{4}$ for a particular value of θ. We will later see that for $\theta/l \gg 1$, the corresponding noise level so increases that it is almost impossible for hackers to recover the original signal data.
- Apply the inverse wavelet transform to get the encrypted audio as encrypted audio $(X') \longleftarrow \mathrm{ILWT}([cA'\ cD'])$;

The encrypted signal is sent to the receiver section for decryption and to recover the original audio signal.

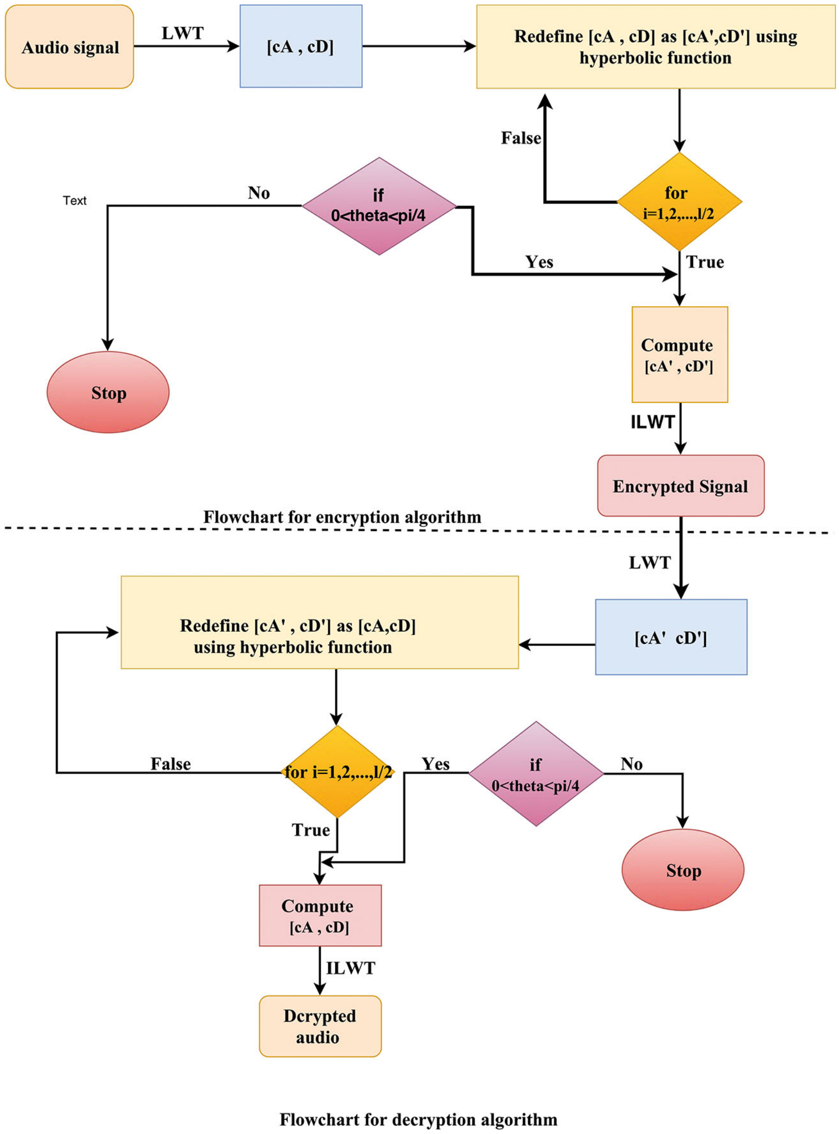


Fig. 3. Flow charts for encryption (upper part) and decryption (lower part) of an audio signal as separated by the dashed line.

3.5 Audio decryption process

The decryption process is the reverse of the encryption process:

- Read the encrypted data *i.e.*, $Y \longleftarrow \text{audioread}(X')$.
- $[cA', cD'] \longleftarrow \text{LWT}(Y)$;
- $cA(i) = cA'(i)\left(\cosh\left(\frac{\theta}{l}\right) + \sinh\left(\frac{\theta}{l}\right)\right) - F_1(i)\left(\cosh\left(\frac{\theta}{l}\right) + \sinh\left(\frac{\theta}{l}\right)\right)^2$
  $cD(i) = cD'(i)\left(\cosh\left(\frac{\theta}{l}\right) + \sinh\left(\frac{\theta}{l}\right)\right) - F_2(i)\left(\cosh\left(\frac{\theta}{l}\right) + \sinh\left(\frac{\theta}{l}\right)\right)^2$,
  for $i = 1, 2, 3, \ldots, \frac{l}{2}$ and for a particular value of θ in $0 < \frac{\theta}{l} \leq \frac{\pi}{4}$. Note that the expressions for $cA(i)$ and $cD(i)$ are obtained by multiplying the expressions of $cA'(i)$ and $cD'(i)$ as in the third item in sect. 3.4 by $\cosh(\frac{\theta}{l}) + \sinh(\frac{\theta}{l})$ and noting that $\cosh^2(\frac{\theta}{l}) - \sinh^2(\frac{\theta}{l}) = 1$.
- Decrypt the audio signal as $(X) \longleftarrow \text{ILWT}([cA, cD])$.

See fig. 3.

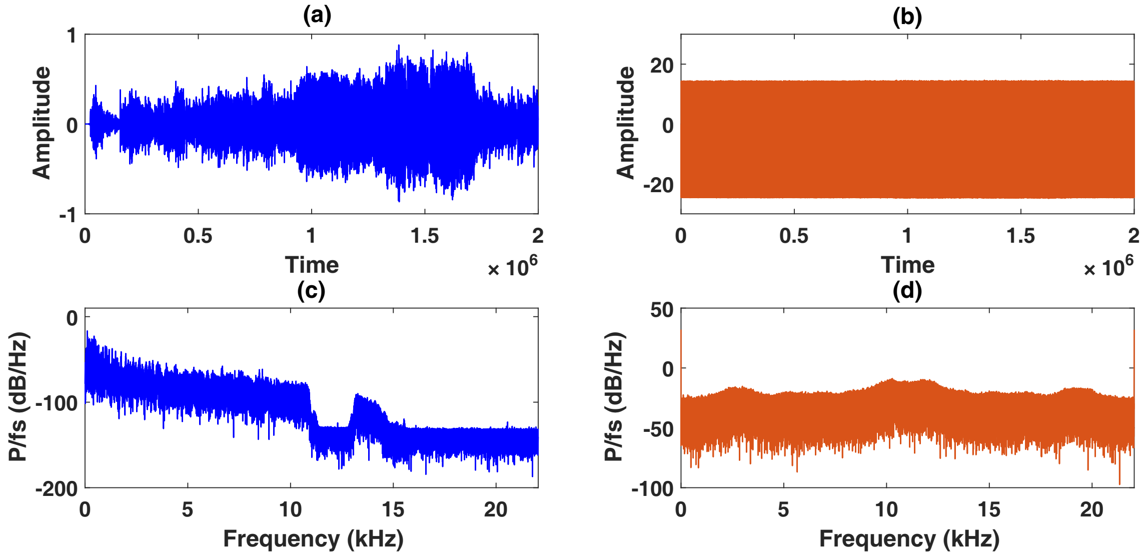


Fig. 4. Wave forms (amplitude *vs.* time) ((a) and (b)) and power spectrum (P/f_s *vs.* frequency) ((c) and (d)) of the original (upper panels) and encrypted (lower panels) audio signals.

4 Security analysis of encrypted audio signal

In this section, we perform some statistical analysis to ensure that the proposed encryption scheme is resistant to different kinds of attacks. In fact, the encrypted signal remains secured under the process of data transmission because the key space, which is based on the initial conditions of the chaotic Hénon map and the parameters θ and ϕ, has been chosen to be large enough. The security analysis comprising, namely, the key space attack and sensitivity analysis, the correlation analysis and the spectral entropy are given in subsects. 4.1 to 4.3. To this end, we consider a digital audio file (.wav format) as in fig. 4. It is shown that even a small change in the key matrix M cannot help recover the original audio file, *i.e.*, the encryption is free from any brute-force attack.

4.1 Key space attack and sensitive analysis

To prevent an adversary from using a brute-force attack of finding the key to encrypt an audio signal, the key space is designed to be large enough to make such a search infeasible. Here, the key space size is basically meant for the total number of possible different keys in the encryption process. Another desirable attribute is that the key must be selected truly randomly from all possible key permutations. The size of the key space can be obtained as follows:

- The generation of chaotic data set as in sect. 3.2 with a random choice of ϕ results into the key space to be of order 10^9 for each Y_{k_i}, $i = 1, 2$. So, the key space size at this stage will be $(10^9)^2 = 10^{18}$.
- Since the key matrix M is considered to be of order 4 and in each element of the matrix m_i, s_i is multiplied by 10^{16} in order to retain the corresponding values up to 16 significant digits, the size of the key space at this stage will be $(10^{16})^4 = 10^{64}$.
- In the process of key hiding in the chaotic medium using the BitXor operation (8 bit operation), each layer of matrix has order 4. So, the size of the key space in the process of key hiding is $(2^8)^4 = 2^{32}$.
- In the process of encryption and decryption with a random choice of θ, the length of the chaotic data set l (*i.e.*, the number of iterations) gives the key space size of order l^2.
- Finally, the total key space size in our proposed algorithm is $l^2 \times 10^{64} \times 10^{18} \times 2^{32} \approx 4.295 \times l^2 \times 10^{91}$.

Thus, in our proposed algorithm, the key space is sufficient enough to resist all kinds of brute-force attacks.

It has already been mentioned that under suitable choice of the initial condition and the parameters α and β, the Hénon map exhibits chaos. In the process of encryption, the chaotic data set, thus obtained, are then used to hide the key matrix in the optical medium. Next, we send the initial condition and the parameters to the receiver section for decryption. The chaotic Hénon map is so sensitive to the initial condition that a small change in it results in a huge change in the key matrix. The steps for the generation of keys should also be followed in order. Otherwise, any change between the steps results in an incorrect key, *i.e.*, an incorrect representation of the audio signal. In this case, the positions of each values of the audio data will be changed and the effectiveness of sound of the audio file will result in a blur audio. Thus, it is impossible to recover the audio signal even if one guesses a value of the key, *i.e.*, the audio signal will be transmitted to the receiver section secretly (see fig. 5).

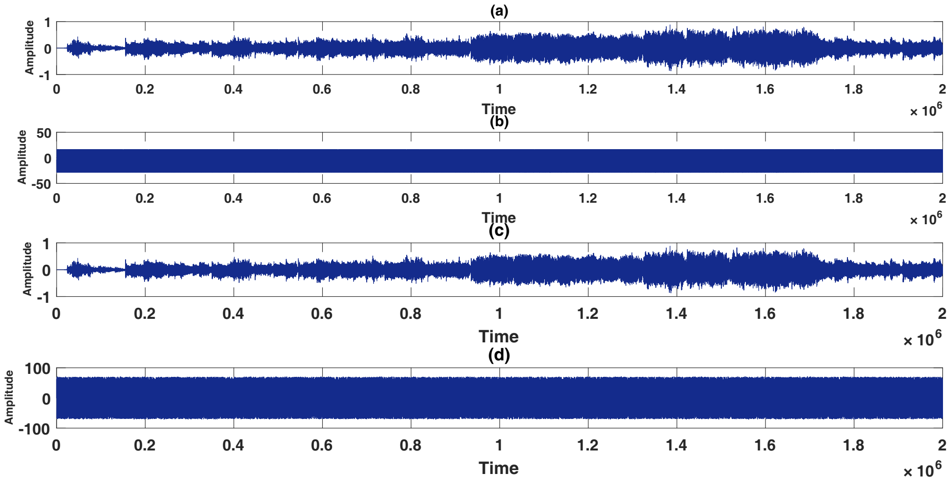


Fig. 5. Decryption of an audio signal with right key and wrong key matrix representations. Subplots (a) and (b), respectively, are the original audio signal and the encrypted audio signal, while subplots (c) and (d), respectively, are the decrypted audio signals with right and wrong key representations.

Table 1. Correlation coefficients of a pair of adjacent sample values of an original and encrypted audio data signal.

Correlation coefficient	Original audio	Encrypted audio
ρ	0.9939	-0.1578

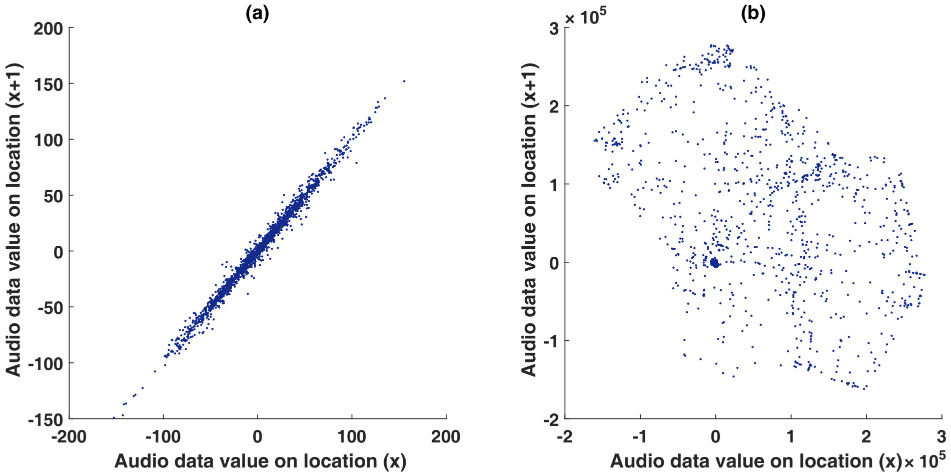


Fig. 6. Scatter plots of the correlation coefficients between the adjacent data points of the original (subplot (a)) and the encrypted (subplot (b)) audio signals.

4.2 Correlation analysis

In an original audio signal, the adjacent data are highly correlated, *i.e.*, their correlation coefficient is always high, while in an encrypted audio data, the correlation coefficient of the adjacent data is expected to be nearly zero or negative. Thus, a secure encryption scheme requires an original audio signal to be transformed into a random-like encrypted signal with very low correlation coefficient to resist any statistical attack. We define the covariance between a pair of data values x and y as $\mathrm{Cov}(x,y) = E[(x - E(x))(y - E(y))]$ and the corresponding correlation coefficient is given by

$$\rho_(xy) = \frac{\mathrm{Cov}(x,y)}{\sigma(x)\sigma(y)}, \quad \sigma(x),\ \sigma(y) \neq 0, \tag{7}$$

where $E(x)$ and $E(y)$ are the means, and $\sigma(x)$ and $\sigma(y)$ are the standard deviations of the distribution of the audio signal data values. The correlation coefficients for the original and encrypted audio signals are given in table 1, while the corresponding scatter plot is shown in fig. 6. It is seen that the original signal is highly correlated ($\rho \sim 1$), however, the encrypted one is too much randomized in its region. Thus, our proposed encryption scheme satisfies the correlation performance and is secure against statistical attacks.

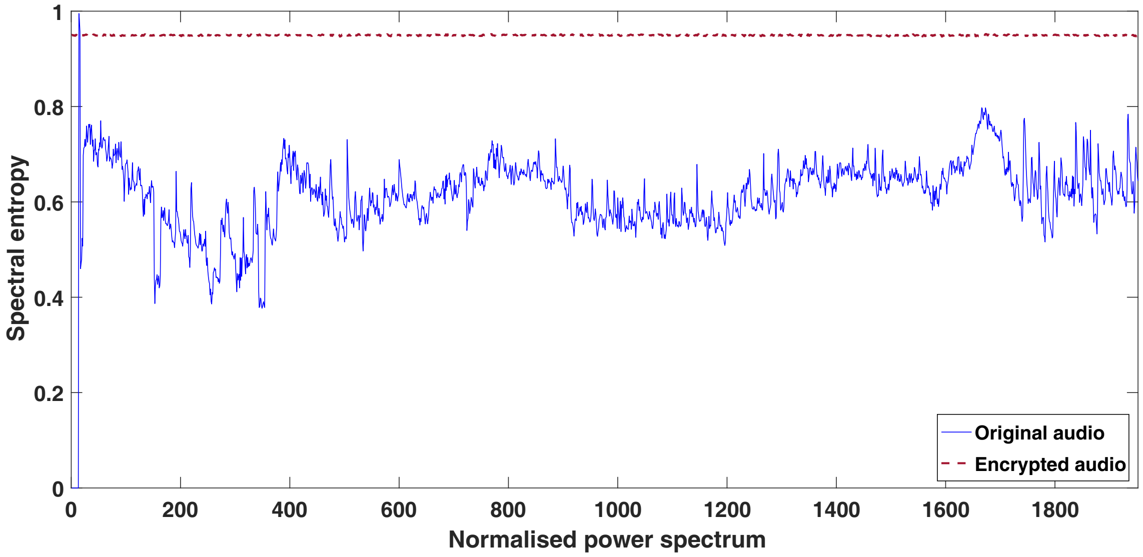


Fig. 7. Spectral entropy values of the original (solid line) and the encrypted (dashed line) audio signals with mean spectral values 0.6124 (*i.e.*, between 0.5 and 0.65; regular beats) and 0.9451 (*i.e.*, close to 1; irregular beats), respectively.

4.3 Spectral entropy

We also perform an another statistical measure of uncertainty for the audio signal. There are, in fact, several ways to estimate changes in the amplitude of the original audio signal and the encrypted one. This method of spectral entropy [12] uses the amplitude component of the power spectrum as "probability" in entropy calculation. This entropy indicates a measurement of the amount of disorders in the amplitude of encrypted data samples. To calculate the spectral entropy we follow this algorithm:

- Read the amplitudes of the data sample of both the original and the encrypted audio signals.
- Compute the power spectrum for both the audio signals.
- Normalize the power spectrum as PSD_n by the establishment of a normalization constant C_n, so that the sum of the normalized power spectrum of the audio samples is 1, *i.e.*, $\sum_n \frac{PSD_n}{C_n} = 1$, where n is the number of sample values. This represents a probability diagram.
- Calculate the entropy as $E_i = -\sum_n PSD_n(f_i)\log(PSD_n(f_i))$ for $i = 1, 2, 3, \ldots, n$ and f_i denotes the frequency of the signal. Then, the entropy value is normalized to vary in between 0 (total regularity) and 1 (maximum irregularity).

In fig. 7, we show the disorders of the amplitudes of the original sample and the encrypted one. From the measurements of the spectral entropy of both the signals we can see that for the encrypted sample the mean entropy is near about 1, which concludes the maximum irregularity of the frequency distribution, while in case of the original one, it is in between 0.5 to 0.65 which means that it maintains the regularity.

5 Conclusion

A new scheme for the encryption of an audio signal is proposed. The scheme is based on the lifting wavelet transforms and the chaotic Hénon map together with Sine and Cosine hyperbolic functions. We have applied the lifting scheme for the first time to encrypt an audio signal owing to its many advantages compared to the ordinary scheme of wavelet transforms. The encryption scheme is designed mainly in two phases: one in which the audio signal is transformed into a data signal by the lifting wavelet scheme, and the other where the transformed data is encrypted by the cahotic data set from the Hénon map and sine and cosine hyperbolic functions. In the encryption scheme, we have also proposed new algorithms both for the generation of keys and key hiding in the chaotic medium. The key space is considered to be large enough to resist any kind of attack. We have also performed several statistical analysis for the security of encrypted signals, namely the key space analysis, the correlation analysis and the spectral entropy analysis which ensure that the proposed encryption algorithm is resistant to any cryptographic attacks.

References

1. A. Belazi, A. AbdEl-Latif, A.-V. Diaconu, R. Rhouma, S. Belghith, Opt. Lasers Eng. **88**, 37 (2017).
2. A.M. Elshamy, A.N.Z. Rashed, A. El-Naser, A. Mohamed, O.S. Faragalla, Y. Mu, S.A. Alshebeili, F.E. Abdel-Samie, J. Lightwave Tech. **31**, 2533 (2013).
3. S.E. Assad, M. Farajallah, Opt. Commun. **41**, 144 (2016).
4. D. Xiao, Q. Fu, T. Xiang, Int. J. Bifurc. Chaos **26**, 1650193 (2016).
5. S. Banerjee, L. Rondoni, S. Mukhopadhyay, A.P. Misra, Opt. Commun. **284**, 2278 (2011).
6. A. Roy, A.P. Misra, S. Banerjee, *Chaos-based image encryption using vertical-cavity surface-emitting lasers*, arXiv:1705.00975 [physics.optics].
7. K. Kordov, L. Bonchev, Math. Soft. Eng. **3**, 183 (2017).
8. M.S. Baptista, Phys. Lett. A **240**, 50 (1998).
9. J. Yang, T. Xiang, D. Xiao, Multimedia Tools Appl. **74**, 10873 (2015).
10. W. Sweldens, SIAM J. Math. Analysis, May 1995 **29**, 511 (1998).
11. W.F.H. Al-Shameri, Int. J. Math. Anal. **6**, 2419 (2012).
12. C.E. Shannon, Bell Syst. Tech. J. **27**, 623 (1948).