Quaternion-based Encryption/Decryption of Audio Signal Using Digital Image as a Variable Key

M.I.Khalil

Princess Norah Bent Abdurrahman University, Faculty of Computer and Information Sciences, Information Technology (networks) Department, Riyadh, Kingdom of Saudi Arabia

Abstract: With the rapid growth of communication technology, cryptography plays a significant role in securing and verification of information exchanged via public communication channels. The current paper introduces a novel method for encrypting/decrypting audio signal using a selected digital image as a complicated key and cover for audio signal. Each sample of the audio signal is combined with the values of the three color components of a pixel fetched from the cover image yielding a quaternion number. The absolute value of this quaternion number is then transmitted and when received, the original value of the audio sample can be extracted using simple quaternion mathematics. A second level of complexity can be added to this approach by applying one of the well-known cryptographic techniques (symmetric or asymmetric). The suggested approach is implemented using Matlab simulation software and the generated audio signal is compared with the original one using some performance metrics. The obtained results show that the proposed approach is robust and more secure against cryptanalysis attacks without affecting the used bandwidth of the communication channel.

Keywords: Quaternions, Cryptography, Symmetric, Asymmetric, Encryption, Decryption, Simulink**.**

1. Introduction

Cryptography is an indispensable tool for keeping the confidentiality of information during exchange in the presence of adversaries [1-5]. It is a framework relies on the intersection of the disciplines of mathematics, computer science, and electrical engineering. It is based on various mathematical algorithms and techniques cooperate to block adversaries, and is closely related to the disciplines of cryptology and cryptanalysis. Information and computer network security aspects such as data confidentiality, data integrity, authentication, non-repudiation and the regulation of human secure behavior are deemed and covered by cryptography discipline. Applications of cryptography include ATM cards, computer passwords, and electronic commerce. The techniques used in cryptographic systems are typically classified into two generic categories: symmetric-key and public-key:

1- Symmetric (Secret-key) cryptosystems [6] where only one key is used for both encryption and decryption operations, and it is of two types: Block ciphers and stream ciphers. Data Encryption Standard (DES), Advanced Encryption Standard (AES) and Blowfish are some examples of symmetric cryptography [7].
2- Asymmetric (Public-key) cryptosystems [8] where two different but mathematically related keys are used; private keys and public keys. Public key is used for encryption while the private one is used for decryption (e.g. Digital Signatures).

Most of the cryptography encryption techniques are devoted to text data while encryption of multimedia data such as audio data has few cryptography techniques. Most of audio signal encryption techniques are based on adding specific noise to the audio signal before transmitting and this noise signal is to be extracted at the receiver to obtain the original audio signal. Raghunandhan. K. R presents two layer securities, which includes both transposition and substitution cipher. The first stage processes the audio signal with transposition cipher. While in the second stage Modulus Multiplication is used as substitution cipher, for this the key is generated using Pseudo Random Number Generation (PRNG) [9-11]. Sheetal Sharma proposed a method where a frequency domain of the wav audio signal is taken for the encryption and decryption. The DFT (Discrete Fourier Transform) is used for transforming the time domain audio signal to frequency domain audio signal. The audio signal is separated into different frequency bins with respect to phase and magnitude values by applying DFT on the audio signal. The RSA technique is applied for the encryption and decryption on the lower frequency bands because not all the frequency regions participate equally in the communication [12].

This paper introduces a new symmetric-based encryption/decryption technique for securing audio signal to guarantee end-to-end secrecy for speech in real time communication systems. The symmetric key used in this method is unlike the traditional one in two significant aspects. The first one: the secret key does not have a unique value and instead it can be one of a huge set of keys. The second difference is the way of mathematical manipulation used in encryption and decryption processes. The performance of the proposed method will be estimated using performance metrics.

The rest of this paper is organized as follows: Section II illustrates the basics of quaternion mathematics. The proposed methods will be implemented in section III. The obtained results will be concluded in section IV.

2. Related Work

Cryptography is an indispensable tool based on many mathematical techniques or algorithms for keeping the confidentiality of information during exchange in communication media. Research effort on cryptography is still required for secured communication. Most attacks on a signal are assumed to be made by nature (noise) or by intelligent adversary (espionage and spoofing). The idea behind cryptography is to use randomization to make attacking difficult for any adversary where randomness is inherent in the signal, not in the algorithms themselves. This is attributed to the fact that once the encryption method is known, any one can find embedded message [13]. Most of encryption/decryption techniques are implemented based on either symmetric (private-key) or asymmetric (public-key) algorithms. Some basic symmetric encryption algorithms are DES (Data Encryption Standard), Triple-DES, Blowfish, RC2, RC4, RC6 and AES. RSA (Rivest-Shamir-Adleman) is the most widely used asymmetric algorithm where a pair of keys (one public and one private) are used. Many of the concepts of cryptography have been applied to multimedia objects such as text, image, video and audio. Real–time audio encryption faces a greater challenge due to large amount of data processing involved. Some audio encryption approaches aimed to reduce audio encryption time by only encrypting selected parts of the audio file [13]. An example of partial encryption of audio files is done using the Discrete Fourier Transform to encrypt lower frequency bands. Considering audio cryptography, A.V. Prabu, et al. introduced a method to encrypt audio (sound) stream of data by applying chaos where a pair of one-dimensional logistic maps is used for generating a chaotic sequence. The proposed scheme is then implemented in real time on a mobile phone [14]. Abdelfatah A. Tamimi and Ayman M. Abdalla introduced an algorithm that employs a shuffling procedure to perform encryption of audio files, applying the stream cipher method. The algorithm uses a private key to perform encryption that is key dependent and data dependent[y]. Juliano B. LimaIn and Eronides F. Da Silva Neto introduced an audio encryption scheme based on the cosine number transform (CNT). The transform, which is defined over a finite field, is recursively applied to blocks of samples of a non-compressed digital audio signal. The blocks are selected using a simple overlapping rule, which provides diffusion of the ciphered data to all processed blocks. A secret-key is used to specify the number of times the transform is applied to each one of such blocks [15]. Bartosz Czaplewsk, et al. proposed a new idea of digital images fingerprinting. The method is based on quaternion encryption in the Cipher Block Chaining (CBC) mode. The encryption algorithm described is designed for gray tone images but can easily be adopted for color ones. For the encryption purpose, the algorithm uses the rotation of data vectors presented as quaternions in a three-dimensional space around another quaternion (key). On the receiver's side, a small amount of unnoticeable by human eye errors occurs in the decrypted images. These errors are used as a user's digital fingerprint for the purpose of traitor tracing in case of copyright violation [16]. Nadia Alsaidi , et al. introduced a new NTRU (Number Theory Research Unit) cryptosystem which is based on using commutative ring of quaternions CQ. It has the same structure of QTRU but depends on the polynomial algebra with coefficients in CQ. It will be referred to as CQTRU. Some conditions on the parameter selection are placed to allow the proposed system high chance for successful decryption [17]. Mariusz Dzwonkowski, et al. introduced a new quaternion-based lossless encryption technique for digital image and communication on medicine (DICOM) images. They have scrutinized and slightly modified the concept of the DICOM network to point out the best location for the proposed encryption scheme, which significantly improves speed of DICOM images encryption in comparison with those originally embedded into DICOM advanced encryption standard and triple data encryption standard algorithms. The proposed algorithm decomposes a DICOM image into two 8-bit gray-tone images in order to perform encryption. The algorithm implements Feistel network like the scheme proposed by Sastry and Kumar. It uses special properties of quaternions to perform rotations of data sequences in 3D space for each of the cipher rounds. The images are written as Lipschitz quaternions, and modular arithmetic was implemented for operations with the quaternions [18]. Shaoquan Wu and Jiwu Huang proposed a self-synchronization algorithm for audio watermarking to facilitate assured audio data transmission. The synchronization codes are embedded into audio with the informative data, thus the embedded data have the self-synchronization ability. To achieve robustness, they embed the synchronization codes and the hidden informative data into the low frequency coefficients in DWT (discrete wavelet transform) domain. By exploiting the time-frequency localization characteristics of DWT, the computational load in searching synchronization codes has been dramatically reduced, thus resolving the contending requirements between robustness of hidden data and efficiency of synchronization codes searching [19].

3. Quaternions Mathematics

The quaternions mathematics, or hypercomplex mathematics, were discovered by Hamilton in 1843 [20, 21]. They combine by the normal rules of algebra with the exception that multiplication is not commutative. A quaternion has four components, one real and three imaginary. The usual notation, extended from that of the complex numbers is:

$$q = w + xi + yj + zk \tag{1}$$

Where w, x, y and z are real, and i, j and k are complex operators which obey the following rules:

$$i^2 = j^2 = k^2 = ijk = -1 \tag{2}$$

$$ij = k, \;\; jk = i, \;\; ki = j \tag{3}$$

$$ji = -k, \;\; kj = -i, \;\; ik = -j \tag{4}$$

The pattern of signs in the products of different operators is easily remembered if the operators $i, j\ and\ k$ are imagined on a clock face, arranged clockwise in alphabetical order. Multiplication of any pair of operators in a clockwise sequence produces a positive product, while multiplication in anti-clockwise sequence yields a negative product. The quaternion conjugate is:

$$\bar{q} = w - xi - yj - zk \quad \epsilon\ \mathrm{H} \tag{5}$$

In addition, the modulus of a quaternion is given by:

$$\|q\| = \sqrt{q\tilde{q}} = \sqrt{w^2 + x^2 + y^2 + z^2} \tag{6}$$

Define the real and imaginary parts of q as:

$$Re(q) = w \;\in\; \mathbb{R},$$

$$and\ Im(q) = xi + yj + zk \;\in\; \mathbb{I} \tag{7}$$

The inverse of a non-zero quaternion $q \neq \mathrm{H}$ is:

$$q^{-1} = \frac{\tilde{q}}{|q^2|} \tag{8}$$

A quaternion with zero real part is called a pure quaternion, and a quaternion with unit modulus is called a unit quaternion.

The imaginary part of a quaternion has three components and may be associated with a 3-space vector. For this reason, it is sometimes useful to consider the quaternion as composed of a vector part and a scalar part, thus:

$$q = S(q) + V(q) \tag{9}$$

The traditional quaternion Fourier transform (QFT) [22,23] is only defined for real or quaternion valued signals over the domain ℝ, while the quaternion discrete Fourier transform (QDFT) for $h \in$ H can be defined, based on the concept of quaternion multiplication and exponential and non-commutative property of the quaternion multiplication , as three different types:

a) The two-sided DQFT:

$$F_{L-R}(u,v) = \frac{1}{\sqrt{MN}} \sum_{x=0}^{M-1} \sum_{y=0}^{N-1} e^{-\mu 2\pi \frac{xu}{M}} f(x,y) e^{-\mu 2\pi \frac{vy}{N}} \tag{10}$$

b) The left-sided DQFT:

$$F_L(u,v) = \frac{1}{\sqrt{MN}} \sum_{x=0}^{M-1} \sum_{y=0}^{N-1} e^{-\mu 2\pi \left(\frac{xu}{M} + \frac{vy}{N}\right)} f(x,y) \tag{11}$$

c) The right-sided DQFT:

$$F_R(u,v) = \frac{1}{\sqrt{MN}} \sum_{x=0}^{M-1} \sum_{y=0}^{N-1} f(x,y)\ e^{-\mu 2\pi \left(\frac{xu}{M} + \frac{vy}{N}\right)} \tag{12}$$

μ is any unit pure quaternion.

$$F_f^{-q}\left[F_f^q\right](m,n) = f(m,n) = \frac{1}{MN} \sum_{u=0}^{M-1} \sum_{v=0}^{N-1} F_f^q(u,v) e^{\mu 2\pi (\frac{mu}{M} + \frac{nv}{N})} \tag{13}$$

Due to its important properties, quaternion discrete Fourier transform (QDFT) and its counterparts quaternion discrete cosine transform (QDCT) and quaternion wavelet transform have been widely used and applied to both single and two dimensional signals in the fields of image processing, radar, robotics and cryptographic.

4. The Proposed System

Encryption Process

The proposed system is composed of two opposite subsystems or parts: the first part (encryption process) is at the transmitter side, while the second one (decryption process) is at the receiver side. The block diagrams both for the first and second subsystems are shown in Fig.1 and Fig.2 respectively. A frame consisting of n samples ($a_1, a_2, \ldots, a_n$) is acquired from the audio signal and an equal number of pixels ($p_1, p_2, \ldots, p_n$) is fetched from image I where each pixel consists of its three color components r, g and b and b. A quaternion number q_1 with zero-real part is composed of the values ($0, r, g, b$):

$$q_1 = 0 + r\,\boldsymbol{i} + g\,\boldsymbol{j} + b\,\boldsymbol{k} \tag{14}$$

Where $r, g, b \in \mathbb{R}$

The quaternion discrete Fourier transform (QDFT) is then obtained as: $Q_1 = qfft(q_1)$, and the quaternion conjugate $\overline{Q_1} = conj(qfft(q_1))$ is also obtained as well.

Another quaternion number with zero-imaginary parts is composed of the value of the audio sample:

$$q_2 = a + 0\,\boldsymbol{i} + 0\,\boldsymbol{j} + 0\,\boldsymbol{k} \tag{15}$$

$$q_T = (Q_1 * \overline{Q_1} + q_2) \in \text{H} \tag{16}$$

Then the norm of a quaternion q_T is obtained and scaled as:

$$m = \|q_T\|/256 \quad \in \mathbb{R} \tag{17}$$

By this way, the value of the audio samples ($a_1, a_2, \ldots, a_n$) is embedded within the vector ($m_1, m_2, \ldots, m_n$). The ciphered samples ($m_1, m_2, \ldots, m_n$) are sequentially transmitted. The pseudo codes of the encryption algorithm at the transmitter side is shown in List-1.

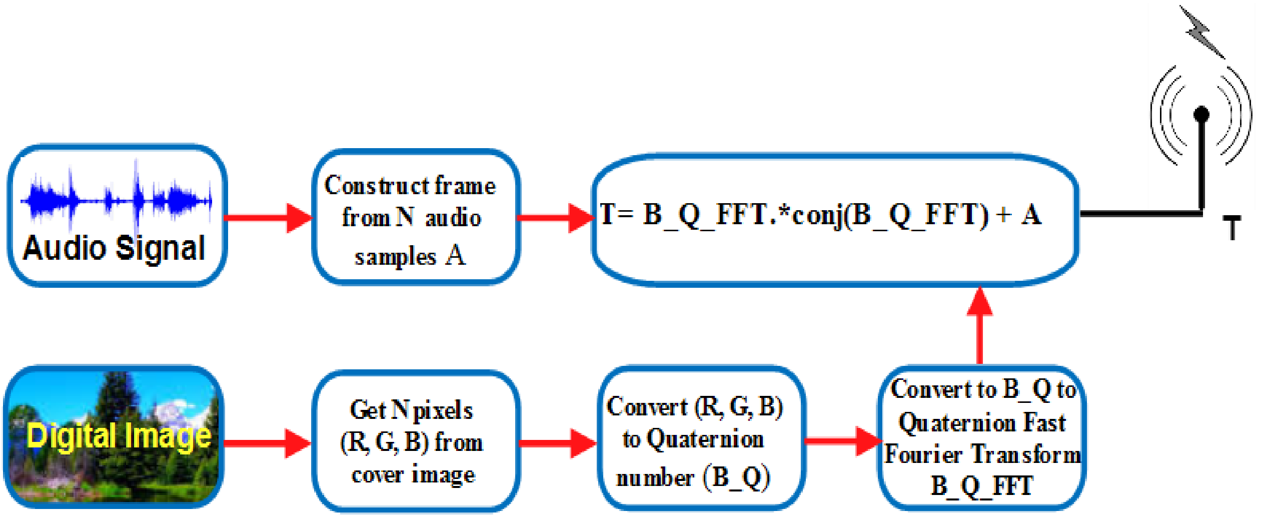
Audio Signal
Construct frame from N audio samples A
T= B_Q_FFT.*conj(B_Q_FFT) + A
T
Digital Image
Get N pixels (R, G, B) from cover image
Convert (R, G, B) to Quaternion number (B_Q)
Convert to B_Q to Quaternion Fast Fourier Transform B_Q_FFT

Figure 1. The block diagram of encryption algorithm

List 1. Pseudo code of the encryption algorithm

```
// get  ( $p_1, p_2, \dots, p_n$ ) pixels from image $I$  and
// ( $a_1, a_2, \dots, a_n$ ) samples from audio signal

for i = 1: n
{
    $p_i \leftarrow r_i, g_i, b_i$
    $a_i \leftarrow$ value of audio sample
    $q1_i \leftarrow 0 + r_i\, \boldsymbol{i} + g_i\, \boldsymbol{j} + b_i\, \boldsymbol{k}$
    $q2_i \leftarrow a_i + 0\, \boldsymbol{i} + 0\, \boldsymbol{j} + 0\, \boldsymbol{k}$
}

$Q1 \leftarrow qfft(q1)$ ,   $\overline{Q1} \leftarrow conj(qfft(q1))$
$q_T \leftarrow (Q1 * \overline{Q1} + q2)$

// norm and scale to get encrypted message

$m = \|q_T\|/256$

// ready for transmission
```

Decryption Process

When the ciphered samples ($z_1, z_2, \dots, z_n$) are sequentially received, the audio samples are then extracted at the receiver as following:
The same copy of the digital image used in the encryption process is used here in the receiver side. The quaternion number v_1, with zero-real part, is computed from the image pixels as previously mentioned in Eq.14:

$$v_1 = 0 + r\, \boldsymbol{i} + g\, \boldsymbol{j} + b\, \boldsymbol{k} \qquad (18)$$

Hence, the quaternion discrete Fourier transform (QDFT) is obtained as: $V_1 = qfft(v_1)$, and the quaternion conjugate $\overline{V_1} = conj(qfft(v_1))$ is also obtained. Assuming that the received signal is z, then:

$$b = \|256 * z - V_1 * \overline{V_1}\| \qquad (19)$$

Taking into consideration that the multiplication product of a quaternion number and its conjugate is a real number, i.e. $V_1 * \overline{V_1} \in \mathbb{R}$

For simplification, assume that the communication channel is free of noise, i.e., there is no noise added to the received signal during transmission and consequently $z = m$ yielding to the plain audio signal $b = a$;

The pseudo codes of the decryption algorithm at the receiver side is shown in List-2

List 2. Pseudo code of the decryption algorithm

```
// get  ( $p_1, p_2, \dots, p_n$ ) pixels from image $I$  and
//( $z_1, z_2, \dots, z_n$ ) samples from received audio signal

for i = 1: n
{
    $p_i \leftarrow r_i, g_i, b_i$
    $z_i \leftarrow$ value of received audio sample
    $q1_i \leftarrow 0 + r_i\, \boldsymbol{i} + g_i\, \boldsymbol{j} + b_i\, \boldsymbol{k}$
    $q2_i \leftarrow z_i + 0\, \boldsymbol{i} + 0\, \boldsymbol{j} + 0\, \boldsymbol{k}$
}

$V1 \leftarrow qfft(q1)$ ,   $\overline{V1} \leftarrow conj(qfft(q1))$

// get decrypted message

$b \leftarrow \|256 * q2 - V_1 * \overline{V_1}\|$

// ready
```

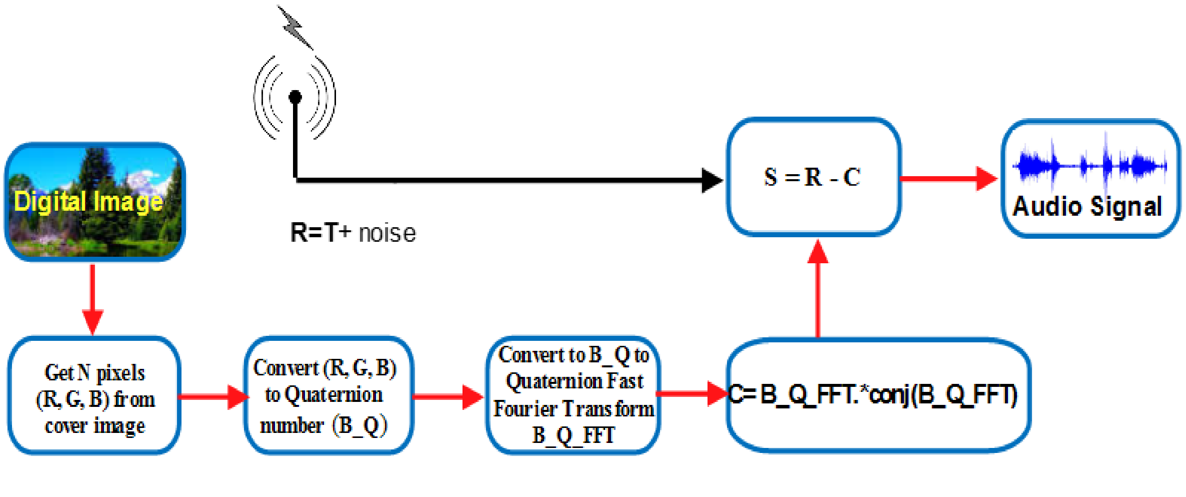
Digital Image
R=T+ noise
S = R - C
Audio Signal
Get N pixels (R, G, B) from cover image
Convert (R, G, B) to Quaternion number (B_Q)
Convert to B_Q to Quaternion Fast Fourier Transform B_Q_FFT
C=B_Q_FFT.*conj(B_Q_FFT)

Figure 2. The block diagram of decryption algorithm

5. Implementation and Experimental Results

The encryption and decryption of real-time audio signal using the proposed algorithm is implemented using Matlab 2016 simulator. Hereby, the real-time audio signal is acquired either from a real audio file or real microphone. A frame of *N* samples is sequentially constructed from the acquired samples. Another frame with equal number of pixels are retrieved from a predetermined color image. The three-color components, R,G and B, of each pixel is used to compose the imaginary part of a quaternion number with zero real part yielding B_Q. The quaternion numbers corresponding to the frame are transferred to the frequency domain using the quaternion fast Fourier transform (QFFT) yielding B_Q_FFT. Absolute numbers are generated as a result of multiplying B_Q_FFT and its conjugate. These absolute values are added to the corresponding absolute values of the audio frame's samples. The generated values are signed with the signs of the corresponding audio samples before enrolled in the transmission stage.

At the receiver side, the same digital image is used to generate B_Q_FFT and its conjugate using the prescribed process. The value of each audio sample is extracted by subtracting the product of multiplying B_Q_FFT and its conjugate from the scaled received values. The color image in Fig.3 is used for testing the proposed method. Both the input (plain) and yielded output (decrypted) audio signals are shown in Figures 4 and 6 respectively. The transmitted (encrypted) signal is shown in Fig.5.

Figure 3. The cover image used in the test

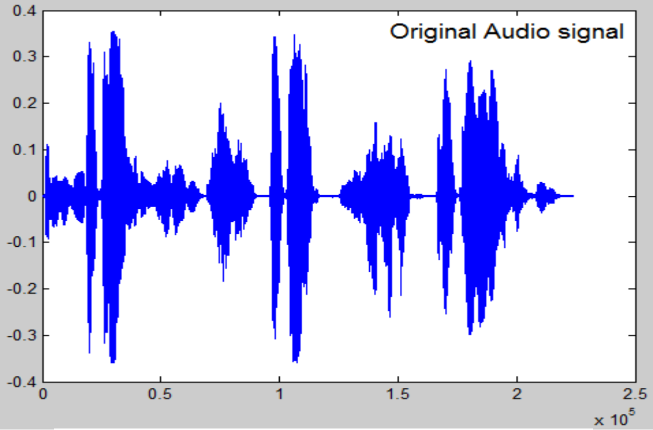

Figure 4. The original (plain) audio signal

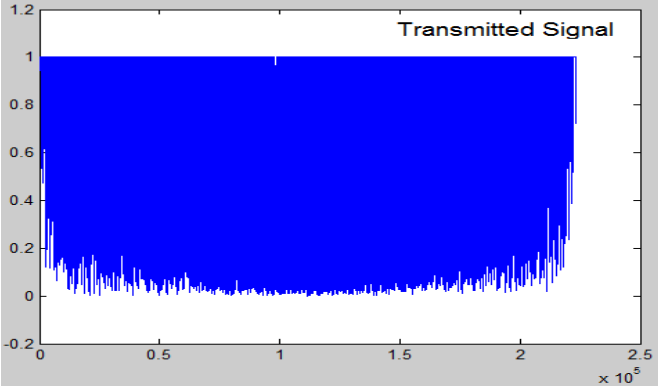

Figure 5. The transmitted (encrypted) audio signal

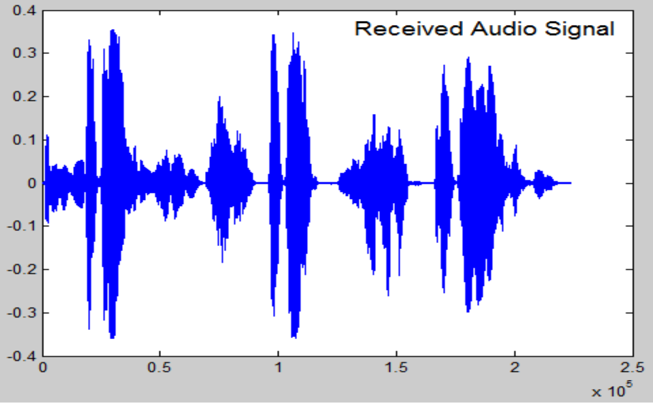

Figure 6. The extracted audio signal

Performance evaluation

To evaluate the overall performance of proposed audio encryption scheme, several objective tests were performed. To measure the performance of the reconstructed signal, various factors such as Signal to noise ratio, PSNR, RSE &NRMSE are taken into consideration [14]. The PSNR computes the peak signal-to-noise ratio, in decibels, between two signals. This ratio is often used as a quality measurement between the original and a received signal. The higher the PSNR, the better the quality of the received or reconstructed signal.

$$PSNR = 10\,log_{10}\frac{R^2}{MSE} = 20\,log_{10}\frac{R}{MSE} \qquad (20)$$

Where, *R* is the maximum fluctuation in the input audio data type.

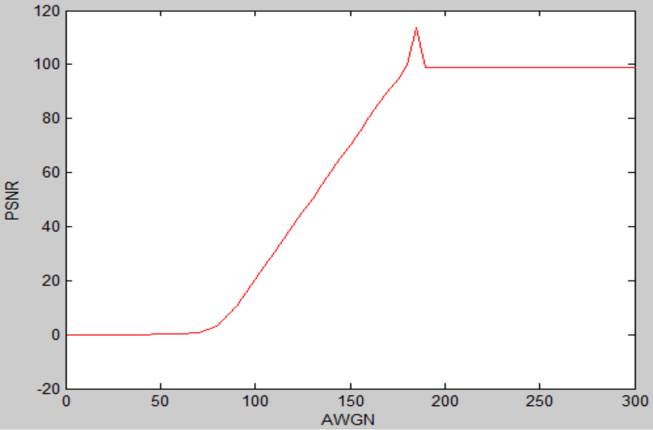

Figure 7. PSNR for the extracted audio signal

Since the input image has a double-precision floating-point data type, then *R* is one. Accordingly, the experimental results are presented in Fig.7 to demonstrate that the embedded audio samples are robust against most common signal processing and attacks, such as Gaussian noise corruption.

6. Conclusion

The current paper introduced a novel method for encrypting/decrypting of audio signal based on embedding the audio samples within the quaternion frequency domain of a digital image. Hereby, the selected digital image is used as a complicated key and cover for audio signal. The original value of the audio samples can be extracted using simple quaternion mathematics. A second level of complexity can be added to this approach by applying one of the well-known cryptographic techniques (symmetric or asymmetric). The suggested approach is implemented using Matlab simulation software and the generated audio signal is compared with the original one using some performance metrics. The same implementation could be used in a network to encrypt the files travelling through.

References

[1] Mamta. Juneja, and Parvinder S. Sandhu, “A Review of Cryptography Techniques and Implementation of AES for Images,” International Journal of Computer Science and Electronics Engineering (IJCSEE) vol. 1, no. 4 2013.

[2] Habutsu T., Nishio Y., Sasase I., and Morio S., “A secret key cryptosystem by iterating chaotic map,” Lect. Notes comput. Sci, Advances in Cryptology-EuroCrypt’91, vol. 547, page(s): pp. 127-140, 1991.

[3] Pichler F. and Scharinger J., “Finite dimensional generalized baker dynamical systems for cryptographic applications,” Lect. Notes in Comput. Sci, vol. 1030, pp. 465-476, 1996.

[4] T. ElGamal, “A prublic key cryptosystem and a signature scheme based on discrete logarithms, in Advances in Cryptology (CRYPTO ’84),” Springer, vol. 196, pp. 10–18. , 1985.

[5] Daria Lavrova and Alexander Pechenkin, “Applying Correlation and Regression Analysis to Detect Security Incidents in the Internet of Things,” International Journal of Communication Networks and Information Security (IJCNIS), vol. 7, no. 3, December 2015.

[6] Yen J. C. and Guo J. I., “Efficient hierarchical image encryption algorithm and its VLSI realization,” IEEE Proceeding Vis. Image Signal Process, vol. 147, no.2, page(s): 430-437, April, 2000.

[7] Mostafa Belkasmi , Mohamed Askali, “A Dynamic Study with Side Channel against an Identification Based Encryption, Rkia Aouinatou,” International Journal of Communication Networks and Information Security (IJCNIS), vol. 7, no. 1, April 2015.

[8] Prashant Kumar Arya, Mahendra Singh Aswal and Vinod Kumar, “Comparative Study of Asymmetric Key Cryptographic Algorithms,” International Journal of Computer Science & Communication Networks,vol 5, no. 1, pp.17-21, 2015.

[9] Saïd Nouh, Idriss Chana and Mostafa Belkasmi, “Decoding of Block Codes by using Genetic Algorithms and Permutations Set,” International Journal of Communication Networks and Information Security (IJCNIS), vol. 5, no. 3, December 2013.

[10] Raghunandhan K R, Radhakrishna Dodmane, Sudeepa K B, Ganesh Aithal, “Efficient Audio Encryption Algorithm For Online Applications Using Transposition And Multiplicative Non-Binary System,” International Journal of Engineering Research & Technology, vol.2 no. 6, June 2013.

[11] R.Gnanajeyaraman, K.Prasadh, Ramar, “Audio encryption using higher dimensional chaotic map,” International Journal of Recent Trends in Engineering, Vol. 1, No. 2, May 2009.

[12] Sheetal Sharma and Lucknesh Kumar, “Encryption of an Audio File on Lower Frequency Band for Secure Communication,” International Journal of Advanced Research in Computer Science and Software Engineering, v. 3, no. 7, July 2013.

[13] S. Sharma, L. Kumar, and H. Sharma. “Encryption of an audio file on lower frequency band for secure communication,” Int. J. Adv. Res. Comput. Sc. & Software Eng., vo. 3, no. 7, pp. 79-84, 2013.

[14] A.V. Prabu, et al, “Audio Encryption in Handsets,” International Journal of Computer Applications (0975 – 8887) vo. 40, no.6, February 2012.

[15] Juliano B. LimaIn and Eronides F. Da Silva Neto, “Audio encryption based on the cosine number transform,” Multimedia Tools and Applications, vo. 75 , no. 14, pp. 8403-8418, July 2016

[16] Bartosz Czaplewski , Mariusz Dzwonkowski , and Roman Rykaczewski, “Digital Fingerprinting Based on Quaternion Encryption Scheme for Gray-Tone Images,” Journal of telecommunications and information technologies, vo., 2014.

[17] Nadia Alsaidi , Mustafa Saed , Ahmad Sadiq3 , Ali A. Majeed, “An improved NTRU Cryptosystem via Commutative Quaternions Algebra,” Int'l Conf. Security and Management | SAM'15 |p. 198-203.

[18] Mariusz Dzwonkowski, Michal Papaj and Roman Rykaczewski, “A New Quaternion-Based Encryption Method for DICOM Images,” IEEE Transactions on Image Processing, vo. 24, no.11, pp. 4614 – 4622, Nov. 2015.

[19] Shaoquan Wu and Jiwu Huang, “Efficiently Self-Synchronized Audi Watermarking for Assured Audio Data Transmission,” IEEE Transactions on Broadcasting, vol. 51, no. 1, MARCH 2005

[20] Sangwine, S., Ell, T.A., "Hypercomplex Fourier Transforms of Color Images," IEEE International Conference on Image Processing (ICIP), vol. 1, pp. 137–140, 2001.

[21] Bihan, N.L., Sangwine, S.J., "Quaternion principal component analysis of color images," IEEE International Conference on Image Processing, vol, 1, pp. 809–812, 2003.

[22] Ell T.A., "Quaternion-Fourier transforms for analysis of two dimensional linear time-invariant partial differential systems," in Proc. 32nd Con. Decision Contr., pp. 1830-1841, Dec. 1993.

[23] M.I.Khalil, “Applying Quaternion Fourier Transforms for Enhancing Color Images,” I.J. Image, Graphics and Signal Processing, vo. 2, pp. 9-15.,1793-8201, 2012.