TELKOMNIKA Telecommunication, Computing, Electronics and Control
Vol. 18, No. 4, August 2020, pp. 2012~2017
ISSN: 1693-6930, accredited First Grade by Kemenristekdikti, Decree No: 21/E/KPT/2018
DOI: 10.12928/TELKOMNIKA.v18i4.14216

Encrypting an audio file based on integer wavelet transform and hand geometry

Zeena N. Al-Kateeb, Saja J. Mohammed
Department of Computer Science, College of Computer Science and Mathematics, University of Mosul, Iraq

Article Info

Article history:

Received Sep 26, 2019
Revised Feb 17, 2020
Accepted Mar 18, 2020

Keywords:

An audio file
Decryption
Encryption,
Hand geometry
Integer wavelet transformation

ABSTRACT

A new algorithm suggested for audio file encryption and decryption utilizing integer wavelet transform to take advantage of the property for adaptive context-based lossless audio coding. In addition, biometrics are used to give a significant level of classification and unwavering quality because the procedure has numerous qualities and points of interest. The offered algorithm utilized many properties of hand geometry estimations as keys to encode and decode the audio file. Many tests were carried out on a set of audio files and quality metrics such as mean square error and correlations were calculated which in turn confirmed the efficiency and quality of the work.

Corresponding Author:

Zeena N. Al-Kateeb,
Department of Computer Science,
College of Computer Science and Mathematics,
University of Mosul, Mosul, Iraq.
Email: zeenaalkateeb@yahoo.com, zeenaalkateeb@uomosul.edu.iq

1. INTRODUCTION

Data encryption has a great importance to preserve the real information from detection and forgery and works on its non-visibility in all of its types. It considered a contributing factor in adding more protection against reading, hearing, tampering or destruction. The techniques used to encode the information are differed, also their methods evolved to reach as which it is currently. Because of the extraordinary improvement and the electronic uprising, the concept of biometric information then it was introduced into secret data encryption systems has emerged. This led to developing the concept of bio-encryption systems.

Cryptography is the ability and study of keeping significant data from disturber and hackers who try to utilize them for forbidden usage. What's more, it might be characterized as a procedure that guarantees the protection of the correspondence between the two gatherings [1, 2]. It chiefly includes two parts: encryption and decryption. Encryption manages mixed the substance of a safe message to make it disjointed or undecipherable for any unapproved individual or program. Where decryption is a process of converting the encrypted message to its identical plaintext [3, 4].

The wavelet space is growing up rapidly. Wavelets have been adequately used as an amazing asset in numerous various fields such as signal processing, star watching, and cryptography [5]. Integer wavelet transform is a kind of wavelet transform that map integer data set with another integer data set, the significant property of the integer wavelet transform (IWT) its coefficients have a similar dynamical range as the first sign. This makes simpler usage contemplations in regards to the size of the factors to be utilized and the reaches to accommodate in the coding calculation [6].

Many encryption methods have appeared and many researchers have tried to develop new, modern and novel ways to encrypt confidential data, such as [7], they used the RSA algorithm in a new way to encrypt and decrypt audio files, in order to protect its confidential data. In [8] a voice encryption framework is created as a real-time software application using advanced encryption standards (AES) to perform this cryptography. Where [9] presented an application to encrypt audio and stereo data samples using single and double dimension discrete-time chaotic systems were. To enhance security during encryption. [10] gives a complete presentation about some of the existing cryptographic techniques and their performance for all data types chiefly audio files.

Some researchers have attempted to decrease audio encryption time by choosing parts of the audio file carefully [11-13], where in [11] the audio files encrypted using the discrete fourier transform (DFT) to encrypt lower frequency bands, and some researchers perform encoding by employing a shuffle stream cipher [14]. In [15] the researchers try to use block cipher encryption system with (.wav) file. They mix block ciphers and chaotic systems to encrypt speech file (.wav) using two of block cipher modes (CBC, CFB). Other scientists utilized chaotic maps, [16] used deoxyribonucleic acid (DNA) encrypting rules and hybrid chaotic shift transform (HCST) to perform a novel audio cryptosystem. Nishith Sinha, et al. Embedding encoded data in the audio files, where the original text message encoded by updating Vigenère cipher, and using LSB encoding to hide it into the cover audio, next, exposed the audio file to transposition utilizing of Blum Blum Shub pseudo-random number generator [17].

2. UTILIZING BIOMETRIC TECHNOLOGIES

As of late, a new science (or term) is appeared, it is a concept of biometrics "Biometric technologies". It is defined as a programmed strategies for verifying/or recognizing. Biometric technologies have grown and used in different areas of life, the personality of a living individual depends on two types [18, 19]:

- Behavioral biometrics: It can be defined as a scale of human actions such as gait, signature. Behavioral biometrics, measure human electrocardiograms also such as (ECG) signals which can employ in personality recognition and authentication
- Physiological biometrics: It can be used to distinguish individual, from one to others, depending on are the individual physical properties of such as hand geometry, fingerprint, odor, hand vein, ear, iris, palm print, retina, face, voice, infrared thermogram and DNA.

Biometric technologies must meet the predetermined necessities to be useful and dependable [20, 21]:

- Uniqueness: There are no two people who can have this property identically,
- Availability: It means, that everyone has this characteristic or property,
- Permanence: It means, this characteristic is stable and does not change by time's factors or that it is slightly affected by the time's factors, then the template should be updated periodically,
- Collectability: It means the adjective can be quantified by electronic sensors easily,
- Performance: that means the use of characteristic gives accurate results at a good speed of distinction, and that the material resources to use that attribute are available,
- Acceptability: It means the collection of this property is accepted by the public and does not meet objections,
- Resistance to Circumvent: It means the technology can resist the fraud tactics that hackers can use [20-22].

Biometric encryption systems are an important application of biometric technologies, It combins the benefits of encryption and biometrics for exploiting the advantages of both [23]. Encryption provides high levels of security, as well as provids biometrics with a non-disclaimer feature. All of these things saves our efforts to protect the symbols and saves us from forgetting passwords problems. In biometric cryptosystems, a cryptographic key is created from the biometric template for a client kept in the database so that the key can't be found without a fruitful biometric validation [19, 24]. There are many domains deal with encryption and steganography the audio signal, such as transform domain, temporal domain, and coded domain. Encryption/steganography in transform domain gives greater security [25, 26]. Other researchers have also suggested using chaotic and hyperchaotic systems in encryption to increase data security [27-40].

3. INTEGER WAVELET TRANSFORM OF AN AUDIO SIGNAL

Integer wavelet transform (IWT) is a type of discrete wavelet transform (DWT). It has a significant property that making it better than (DWT), where IWT coefficients have the similar dynamical range as the original signal. This facilitates the progress, especially, the considerations deal with the size of the variables to be utilized, and the ranges to accommodate in the coding algorithm [41, 42]. IWT It is used as an efficient transform that converts and rebuilds data without loss. This provides high efficiency of encryption systems and makes the decoding process for data retrieval work with high accuracy [43-45].

3.1. Audio file encryption using hand geometry

The proposed algorithm encrypt data of audio file in the frequency domain, where the algorithm first converts the audio file from the spatial domain into the frequency domain using integer wavelet transform (IWT), taking advantage of the characteristics and features of this transform, as mention above, the most important of these properties is converts and rebuilds data without loss. Then the algorithm receives an image of a human hand in order to deduce the geometry characteristics of its. The hand geometry features used as keys to encrypt the audio file data. The extracting characteristics of the hand image are reaching to 50 characteristics, such as, the width of the five fingers in three different regions, the finger lengths, some angles, reference points the and width of the palm in two areas. We are noting, that the value of each property is a real value that has an integer part and a fractional part, each part of them will be used as a separate key to encrypt audio data. The encryption is applied to the integer wavelet transform (IWT) coefficient using the extracted bio_encryption keys. Next, the IWT two parts are switched to increase randomness and complexity. Final, changes over the encrypted sound from the frequency domain to the spatial domain and sent from the sender to receiver via the transport channel. The encrypted message is received by an authorized person and similar activities are performed in reverse order to get the confidential voice message. In Figure 1 is shown diagram illuminates the encryption and encryption of the proposed algorithm. By using hand geometric properties in the encryption field, any audio file can be encoded depending on the hand image of a specific client, that will give us protection, privacy and reliability. Besides, each part of the audio file is encrypted.

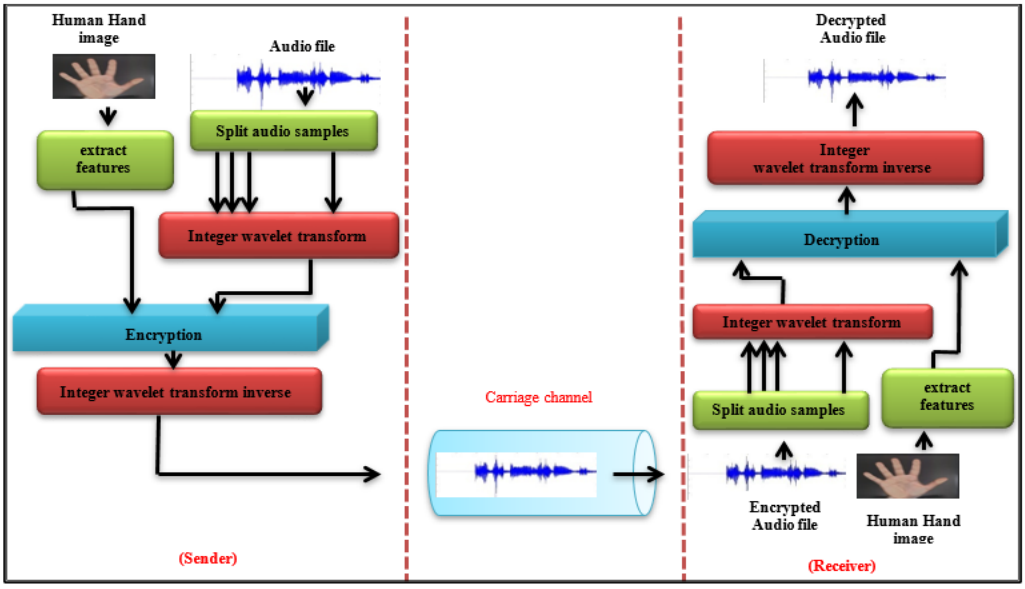

Figure 1. Block diagram of the proposed algorithm

3.2. The steps of the proposed encryption algorithm

We can explain the steps of the proposed encryption algorithm as follows:

Input: Audio file, Hand image
Output: Encrypted audio file.

1. Begin
2. Find the hand properties which are 50 properties, each one of them is a real number.
3. Split each feature value (say F) to two parts, E_key1 is the integer number of F and E_key2 is an F fractional part. Note E_key1 and E_key2 must be [1-255]
4. Split the audio file into N of segments, where N is a number of the founded hand properties.
5. Convert each segment to IWT which will be producing two other portions: CA and CD.
6. All CA segments encrypt by E_key1 and E_key2 depending on CD coefficients, the following equation show that more clearly:

$$\text{Encrypted CA} = \begin{cases} ((CA \oplus E\_key1) \oplus E\_key2) & \text{if } CD < 0 \\ ((CA \oplus E\_key2) \oplus E\_key1) & \text{if } CD >= 0 \end{cases}$$

7. Switching locations between the two segments (CA and CD) and usage IWT inverse to convert the two segments of the special domain.
8. Reconstruct the signal by segment combination.

9. Randomize the resulted signal to guarantee strong security.
10. Keep the encoded data in a new wave file, and send the resulted audio file to the receiver side via a transmission channel.
11. End.

3.3. The proposed decryption algorithm

Input: Encrypted audio file, Hand image
Output: Decrypted audio file.

1. Begin
2. Find the hand properties, and split each value of them into two parts (D_key1 & D_key2).
3. Reorganize the encoded audio data.
4. Split audio signal into N of segments, where N is a number of the founded hand properties.
5. Convert each segment to IWT that will generate two parts: CA and CD.
6. Switching locations between the two segments (CA and CD).
7. Decrypt CA part using D_key1 with D_key2 depending on CD coefficients, the following equation shows that more clearly:

$$\text{Decrypted CA} = \begin{cases} ((\text{CA} \oplus \text{D\_key1}) \oplus \text{D\_key2}) & \text{if CD} < 0 \\ ((\text{CA} \oplus \text{D\_key2}) \oplus \text{D\_key1}) & \text{if CD} >= 0 \end{cases}$$

8. Use IWT inverse to convert the encoded segments of the special domain.
9. Collective all segments to construct the retrieved signal and play it.
10. End.

4. EXPERIMENTAL

Some metrics are calculated to measure the efficiency and quality of encryption and decoding performance. These metrics are: the value of mean square error (Mse1) among the original audio file and encrypted audio as well as the value of correlation among them (Corrl1). Also calculate the value of mean square error (Mse2) and the value of the correlation (Corrl2) among the original audio file and decrypted audio. Figure 2 explain the audio file before encryption then after encryption and last one after decryption process. Where Table 1 shows the gotten results from applying the proposed algorithm on a set of different size of WAV type audio files.

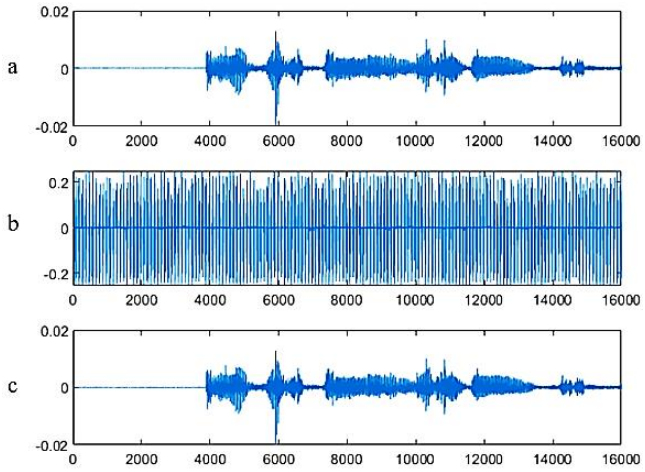

Figure 2. The audio file; (a) original sound, (b) encrypt sound, (c) decrypt sound

Table 1. Show the results gotten from the proposed algorithm on a set of different size of WAV type audio files

File name	Mse1	Corrl1	Mse2	Corrl2	File size
Auf 1.wav	0.008026188663009	6.900753870297950e-04	9.711840286945674e-36	1	16000×1
Auf 2.wav	0.043354788896016	-0.005671487632175	5.290580000000001e-04	0.986451026200484	16000×1
Auf 3.wav	0.003572735902461	-0.002034611144430	1.171953761837611e-35	1	32000×1
Auf 4.wav	0.008312414386621	-0.004513955165074	7.877442169342467e-36	1	24000×1
Auf 5.wav	0.008084075614115	0.007854030696005	5.540245934747540e-36	1	40000×1
Auf 6.wav	0.005824275896583	0.006411342208959	5.232360454380166e-37	1	16000×1

5. CONCLUSION

Due to the growth of information security technology and the fact that it has become a necessity of life, and the introduction of the concept of biometric technology in all areas of life due to the power and advantages of that technology, so the research suggested a system to encrypt important audio files and voice messages using the characteristics of human hand geometry as a kind of Biometrics, 50 of these properties were extracted and used as keys to encrypt the audio file, First, the audio file is divided into 50 segments, according to the number of extracted properties. The algorithm suggested that encryption should be in the frequency domain using the integer wavelet transform to increase the efficiency of the encryption algorithm and to take advantage of the non-loss property of this transform. The quality measures that were calculated shows the goodness of work, where the Mse1 between the original file and the encrypted file was a very small value, and the correlation coefficient between them is also very small value, which indicates that the file is encrypted in high quality. While the Mse2 between the original file and the retrieved file was very large value in addition to the fact that the correlation coefficient has a value close to the one, which gives a clear indication that the recovery process is done almost completely efficiently.

ACKNOWLEDGEMENTS

The authors are very grateful to the University of Mosul/College of Computer Science and Mathematics for their provided facilities, which helped to improve the quality of this work.

REFERENCES

[1] S. F. Yousif, "Encryption and Decryption of Audio Signal Based on RSA Algorithm," *International Journal of Engineering Technologies and Management Research*, vol. 5, pp. 57-64, July 2018.
[2] A. Chadha, et al., "Dual-Layer Video Encryption using RSA Algorithm," *International Journal of Computer*, vol. 16, no. 1, pp. 33-40, April 2015.
[3] A.V. Prabu, et al., "Audio Encryption in Handsets," *International Journal of Computer Applications*, vol. 40, no. 6, pp. 40-45, February 2012.
[4] E. O. Osaghae, "Replication of Ciphertext in Cryptographic System," *Journal of Applied Sciences and Environmental Management*, vol. 22, no. 8, pp. 1193 –1197, August 2018.
[5] M. F. Tolba, et al., "Using Integer Wavelet Transforms in Colored Image-Steganography," *International Journal on Intelligent Cooperative Information Systems*, vol. 4, no. 2, pp. 75-85, July 2004.
[6] R. Punidha and M. Sivaram, "Integer Wavelet Transform Based Approach for High Robustness of Audio Signal Transmission," *International Journal of Pure and Applied Mathematics*, vol. 116, no. 23, pp. 295-304. Apr 2017.
[7] A. Gambhir and S. Khara, "Integrating RSA cryptography & audio steganography," *2016 International Conference on Computing, Communication and Automation (ICCCA)*, Noida, pp. 481-484, 2016.
[8] A. Agarwal, et al., "Secured Audio Encryption Using AES Algorithm," *International Journal of Computer Applications*, vol. 178, no. 22, pp. 29-33, June 2019.
[9] A. Akgül, et al., "An Audio Data Encryption with Single and Double Dimension Discrete-Time Chaotic Systems," *The Online Journal of Science and Technology*, vol. 5, pp. 14-23, July 2015.
[10] R. A. Gandhi and A. M. Gosai, "A Study on Current Scenario of Audio Encryption," *International Journal of Computer Applications*, vol. 116, no. 7, pp. 13-17, April 2015.
[11] S. Sharma, et al., "Encryption of An Audio File on Lower Frequency Band for Secure Communication," *International Journal of Advanced Research in Computer Science and Software Engineering*, vol. 3, pp. 79-84, July 2013.
[12] B. Gadanayak, et al., "Comparative Study of Different Encryption Techniques on MP3 Compression," *International Journal of Computer Applications*, vol. 26, no. 3, pp. 28-31, July 2011.
[13] B. Gadanayak, et al., "Secured Partial MP3 Encryption Technique," *International Journal of Computer Science and Information Technologies*, vol. 2, pp.1584-1587, 2011.
[14] A. A. Tamimi and A. M. Abdalla, "An Audio Shuffle-Encryption Algorithm," *Proceedings of the World Congress on Engineering and Computer Science* (*WCECS 2014)*, vol. I, 2014.
[15] A. Mouafak, et al." Apply new algorithm for chaotic Encryption using CBC&CFB," *Australian Journal of Basic and Applied Sciences*, vol. 7, no. 12, pp. 221-228, October 2013.
[16] S. J. Sheela, et al., "A Novel Audio Cryptosystem Using Chaotic Maps and DNA Encoding," *Journal of Computer Networks and Communications*, vol. 2017, pp.12, August 2017.
[17] N. Sinha, et al., "Encrypted Information Hiding Using Audio Steganography and Audio Cryptography," *International Journal of Computer Applications*, vol. 112, no. 5, pp. 49-53, February 2015.
[18] R. Gad and A. El-Sayed, "Multi-Biometric Systems: A State-of-the-Art Survey and Research Directions," *International Journal of Advanced Computer Science and Applications*, vol. 6, no. 6, pp. 128-138, 2015.
[19] K. P. Singh, "Biometric based Network Security Using MIPS Cryptography Processor," *International Conference on Emerging & Futuristic Trends in Engineering & Technology*, *International Journal of Exploration in Engineering and Technology*, 2015.
[20] N. Radha and A. Kavitha, "Rank Level Fusion Using Fingerprint and Iris Biometrics," *Indian Journal of Computer Science and Engineering (IJCSE)*, vol. 2, no. 6, pp. 917-923, January 2012.

[21] H. AlMahafzah, M. Z. Airwashdeh, "A Survey of Multibiometric Systems," *International Journal of Computer Applications*, vol. 43, no. 15, pp. 36-43, April 2012.
[22] T. Kisasondi, et al., "Biometric Cryptography and Network Authentication," *Journal of Information and Organizational Sciences*, vol. 31, no. 1, pp. 91-99, 2007.
[23] P. Arul and A. Shanmugam, "Generate a Key for AES Using Biometric for VOIP Network Security," *Journal of Theoretical and Applied Information Technology*, vol. 5, no. 2, pp.107-112, 2009.
[24] S. J. Mohammed, "Using biometric watermarking for video file protection based on chaotic principle," *International Journal of Computer Science and Information Security (IJCSIS)*, vol. 15, no. 12, pp. 201-206, December 2017.
[25] Z. N. Al-Kateeb and M. R. Al-Bazaz, "Steganography in Colored Images Based on Biometrics," *Tikrit Journal of Pure Science*, vol. 24, no. 3, pp. 111-117, May 2019.
[26] F. Djebbar, et al., "Comparative Study of Digital Audio Steganography Techniques," *EURASIP Journal on Audio, Speech, and Music Processing*, vol. 25, pp. 1-16, October 2012.
[27] S. F. Al-Azzawi and M. M. Aziz, "Chaos Synchronization of Nonlinear Dynamical Systems via a Novel Analytical Approach," *Alexandria Engineering Journal*, vol. 57, no. 4, pp. 3493-3500, December 2018.
[28] A. S. Al-Obeidi and S. F. Al-Azzawi, "Projective Synchronization for a Class of 6-D Hyperchaotic Lorenz System, " *Indonesian Journal of Electrical Engineering and Computer Science*, vol. 16, no. 2, pp. 692-700, November 2019.
[29] A. S. Al-Obeidi and S. F. Al-Azzawi, "Complete Synchronization of a Novel 6-D Hyperchaotic Lorenz System with Known Parameters," *International Journal of Engineering & Technology*, vol. 7, no. 4, pp. 5345-5349, 2018.
[30] A. S. Al-Obeidi and S. F. Al-Azzawi, "Chaos Synchronization of a Class 6-D Hyperchaotic Lorenz System," *Modelling, Measurement and Control B*, vol. 88, no. 1, pp. 17-22, September 2019.
[31] S. F. Al-Azzawi and M. M. Aziz, "Strategies of Linear Feedback Control and its classification," *TELKOMNIKA Telecommunication Computing Electronics and Control*, vol. 17, no. 4, pp. 1931-1940, August 2019.
[32] Z. Sh. Al-Talib, S. F. AL-Azzawi, "Projective and Hybrid Projective Synchronization of 4-D Hyperchaotic System via Nonlinear Controller Strategy," *TELKOMNIKA Telecommunication Computing, Electronics and Control*, vol. 18, no 2, pp. 1012-1020, April 2020.
[33] S. Y. Al-Hayali and S. F. AL-Azzawi, "An Optimal Control for Complete Synchronization of 4D Rabinovich Hyperchaotic Systems," *TELKOMNIKA Telecommunication Computing Electronics and Control*, vol. 18, no 2, pp. 994-1000, April 2020.
[34] S. Y. Al-Hayali and S. F. AL-Azzawi, "An Optimal Nonlinear Control For Anti-Synchronization of Rabinovich Hyperchaotic System," *Indonesian Journal of Electrical Engineering and Computer Science*, vol. 19, no. 1, pp 379-386, July 2020.
[35] S. F. Al-Azzawi, "Stability and Bifurcation of Pan Chaotic System by Using Routh-Hurwitz and Gardan method," *Applied Mathematics and Computation*, vol. 219, no. 3, pp. 1144-1152, October 2012.
[36] M. M. Aziz and S. F. Al-Azzawi, "Anti-synchronization of Nonlinear Dynamical Systems Based on Gardano's Method," *Optik*, vol. 134, pp. 109-120, April 2017.
[37] M. M. Aziz and S. F. Al-Azzawi, "Hybrid Chaos Synchronization Between Two Different Hyperchaotic Systems via Two Approaches," *Optik*, vol. 138, pp. 328-340, June 2017.
[38] A. S. Al-Obeidi and S. F. Al-Azzawi, "Chaos Synchronization in a 6-D Hyperchaotic System with Self-Excited Attractor," *TELKOMNIKA Telecommunication, Computing, Electronics and Control*, vol. 18, no 3, pp. 1483-1490, June 2020.
[39] S. F. Al-Azzawi, et al., "Chaotic Lorenz System and it's Suppressed," *Journal of Advanced Research in Dynamical and Control Systems*, vol.12, no. 2, pp. 548-555, 2020.
[40] Z. Sh. Al-Talib and S. F. AL-Azzawi, "Projective Synchronization for 4D Hyperchaotic System Based on Adaptive Nonlinear Control Strategy," *Indonesian Journal of Electrical Engineering and Computer Science*, vol. 19, no. 2, August 2020.
[41] Z. N. Al-Khateeb and S J. Mohammedand, "A Novel Approach for Audio File Encryption Using Hand Geometry," *Multimedia Tools and Applications*, March 2020.
[42] Z. N. Al-Khateeb, M. F. Jader, "Encryption and Hiding Text Using DNA Coding and Hyperchaotic System," *Indonesian Journal of Electrical Engineering and Computer Science*, vol. 19, no. 2, August 2020.
[43] C. D. G. Aneanu et al., "Integer Wavelet Transforms Based Lossless Audio Compression," *Proceedings of the IEEE-EURASIP Workshop on Nonlinear Signal and Image Processing (NSIP'99), Antalya, Turkey, June 20-23, 1999.*
[44] R. Punidha, "Integer Wavelet Transform Based Approach for High Robustness of Audio Signal Transmission," *International Journal of Pure and Applied Mathematics*, vol. 116, no. 23, pp. 295-304, 2017.
[45] S. Chakravarthy, *et al.* "Enhanced Playfair Cipher for Image Encryption Using Integer Wavelet Transform," *Indian Journal of Science and Technology*, vol. 9, no. 39, pp. 1-12, October 2016.