Journal of Information Security, 2015, 6, 213-228
Published Online July 2015 in SciRes. http://www.scirp.org/journal/jis
http://dx.doi.org/10.4236/jis.2015.63022

Enhancements in the Security Level for Wireless Sensor Network

Amr M. Kishk[1], Nagy W. Messiha[2], Nawal A. El-Fishawy[3], Abd-Elrahman A. Alkafs[4], Ahmed H. Madian[5]

[1]Reactor Department, Egyptian Atomic Energy Authority (EAEA), Cairo, Egypt
[2]Electronics and Communication Engineering, Faculty of Electronic Engineering (FEE), Menouf, Egypt
[3]Computer Engineering, Faculty of Electronic Engineering (FEE), Menouf, Egypt
[4]Reactor Department, Egyptian Atomic Energy Authority (EAEA), Cairo, Egypt
[5]Radiation Engineering Department, Egyptian Atomic Energy Authority (EAEA), Cairo, Egypt
Email: amr.kishk@yahoo.com, dr.nagy_wadie@hotmail.com, nelfishawy@hotmail.com, alkafs@yahoo.com, ah_madian@hotmail.com

Received 22 May 2015; accepted 27 June 2015; published 30 June 2015

Abstract

The trade off between the energy consumption and the quality of the received image should be considered as a main point in the techniques design in Wireless Sensor Network (WSN). This paper analyzes the performance of multiple image encryption algorithms with different approaches. And also, it introduces two proposed modulation techniques to enhance the performance of WSN. These two techniques merge both the image and the audio in one signal. The merging process enhances the energy consumption data rate. In addition, it removes the effectiveness of the jamming completely from both the reconstructed image and reconstructed audio signal at the receiver. So, the receiver will reconstruct the image without jamming effectiveness. The paper introduces a proposed audio encryption algorithm. The use of encryption algorithms for both image and audio signals with the merging process enhances the security level. Popular metrics are used to compare between these image encryption algorithms and also to show the benefits from these enhancements. The results show the preference of one of these image encryption algorithms to others. And also, the merging process enhances the bit rate to high level.

Keywords

Chaotic Cryptosystems, Image Encryption Algorithms, Encrypted Audio Samples, Merging Process, Proposed Audio Encryption Algorithm

How to cite this paper: Kishk, A.M., Messiha, N.W., El-Fishawy, N.A., Alkafs, A.-E.A. and Madian, A.H. (2015) Enhancements in the Security Level for Wireless Sensor Network. *Journal of Information Security*, **6**, 213-228.
http://dx.doi.org/10.4236/jis.2015.63022

1. Introduction

Wireless Sensor Network (WSN) has been acquiring an increasing importance, and it is utilized in different modalities [1]. It constitutes of a set of light-weight devices, called sensor nodes, used for gathering specific information from the surrounding environment. Each sensor node in WSN is equipped with a radio transceiver. WSN has been rapidly growing and becoming more attractive for a variety of applications such as surveillance of information, industrial confidential information, and air pollution monitoring.

The sensor node depends on the battery as an energy source. The enhancement in the energy consumption is considered a main parameter in the schemes design. Therefore, this paper will survey on the image encryption algorithms using the public metrics and also it will present two proposed modulation techniques and a proposed audio encryption algorithm. The two proposed modulation techniques merge two signals in one signal to reduce the energy consumption and improve both the bit rate and the bandwidth utilization. And also, the dependence on the frequency shift instead of phase shift becomes more effective in dealing with the jamming effectiveness. The use of frequency shift is used at Low Frequency (LF) band. Both image and audio signals are encrypted before the merging process. The image will be encrypted by one of the image encryption algorithms discussed in this paper and the audio is encrypted by the proposed audio encryption algorithm.

The paper is organized as follows: Section 2 introduces survey on image encryption algorithms; Sections 3 and 4 illustrate the two proposed modulation techniques and the proposed audio encryption algorithm respectively; and the results and conclusions are shown at the end of this paper in Section 5 and Section 6 respectively.

2. Image Encryption Algorithms-Related Work

2.1. Chaotic Cryptosystems

There are many different chaotic systems that have been used to construct chaotic cryptosystems such as: logistic map [2], chaotic piecewise map [3], Arnold cat map [4], and Chebyshev map [4]. These chaotic cryptosystems, except Chebyshev map, depend on a change in the image pixels positions as an encryption way to hide the image contents rather than Data Encryption Standard (DES), Advanced Encryption Standard (AES), and Rivest Cipher 6 (RC6) [5] which map the original image to another image based on an encryption key.

Both logistic and piecewise maps depend on generated series as shown in (1) and (2) respectively where: both x_n and m are random numbers in the range [0, 1] while λ is in the range (3.5699, 4]. The order of these series either in descending or ascending manner will specify the new pixel position in the encrypted image. Arnold cat map uses a different approach to change the pixels positions from (x, y) to (x', y'). It depends on an equation shown in (3) and the value of two variables, *p* and *q*, where: M_d is the image dimension while *p* and *q* are two random numbers.

$$x_{n+1} = \lambda x_n \left(1 - x_n\right) \tag{1}$$

$$x_{n+1} = \begin{cases} \dfrac{x_n}{m} & 0 \le x_n < m \\ \dfrac{x_n - m}{1 - m} & m \le x_n < 1 \end{cases} \tag{2}$$

$$\begin{bmatrix} x' \\ y' \end{bmatrix} = \begin{bmatrix} 1 & p \\ q & pq+1 \end{bmatrix} \begin{bmatrix} x \\ y \end{bmatrix} \bmod M_d \tag{3}$$

Chebyshev map generates a key used to encrypt the pixels values. This key is generated in two different ways to enhance the security level. One of these ways is the key generation at the sender as follows:

1) Select *s* and *r* in the range (0, 100] as integer numbers and also *f* in the range (0, 1].

2) Generate $T_s(x) = 2 * f * T_{s-1} - T_{s-2}$ where: $T_1 = 1$, $T_2 = 2*\left(f^2\right) - 1$, $T_3 = 4*\left(f^3\right) - 3*f$, and $T_4 = 8*\left(f^4\right) - 8*\left(f^2\right) + 1$.

3) Generate $TP_r(T_s) = 2 * T_s * TP_{r-1} - TP_{r-2}$ where: $TP_1 = 1$, $TP_2 = 2*\left(T_s^2\right) - 1$, $TP_3 = 4*\left(T_s^3\right) - 3*T_s$, and $TP_4 = 8*\left(T_s^4\right) - 8*\left(T_s^2\right) + 1$.

And, the other way is the key generation at the receiver as follows:

1) Generate $TV_r(x) = 2*f*TV_{r-1} - TV_{r-2}$ where: $TV_1 = 1$, $TV_2 = 2*\left(f^2\right)-1$, $TV_3 = 4*\left(f^3\right)-3*f$, and $TV_4 = 8*\left(f^4\right)-8*\left(f^2\right)+1$.

2) Generate $TK_s(TV_r) = 2*TV_r*TK_{s-1} - TK_{s-2}$ where: $TK_1 = 1$, $TK_2 = 2*\left(TV_r^2\right)-1$, $TK_3 = 4*\left(TV_r^3\right)-3*TV_r$, and $TK_4 = 8*\left(TV_r^4\right)-8*\left(TV_r^2\right)+1$.

TP_r and TK_s are the same and they are used to encrypt the image and decrypt the encrypted image respectively. The image can be encrypted by multiplying each pixel by TP_r. The image can be recovered by dividing each pixel in the encrypted image by TK_s.

2.2. Another Encryption Algorithms

The use of the encryption key has introduced in two different encryption algorithms. Some of them depends on an encryption key for all transmitted packets such as: Data Encryption Standard (DES), Advanced Encryption Standard (AES), and Rivest Cipher 6 (RC6) [5]. The others depend on the key-updating periodically such as: Chaos Block Cipher for Wireless Sensor Network (CBCW) [6] and New Encryption Algorithm for Wireless Sensor Network (NEA-WSN) [7]. Another way to encrypt the image has introduced in an algorithm denoted by New Image Encryption Scheme Based on a Chaotic Function and will be referred to by (NIES) in this paper [8]. Both CBCW and NEA-WSN enhance the performance of the security depending on the key updating with each pixel and with each row in the image respectively, while NIES deal with contents of the image as bits and change their positions inside the image many times specified by a program to determine the number of the iterations. NIES is similar to the concept of chaotic cryptosystems to change the positions but NIES changes the **bits** positions many times while chaotic cryptosystems change the **pixels** positions once. The details of CBCW, NEA-WSN, and NIES are not shown here but the steps of NEA-WSN [7] CBCW [6] are shown in **Figure 1** and **Figure 2** respectively. In NEA-WSN, the encryption of a plain image depends on four keys generated from K_o. These four keys are N_1, N_2, K_1, and K_2. N_1 and N_2 are used for horizontal and vertical circular shift processes respectively. N_1 and N_2 sizes are M and N respectively. They are generated from K_o. Their contents are updated for each next new image [7]. In CBCW, the key-updating is based on updating the encryption key K_j with each pixel which is decomposed as four 8-bits sub-keys K_{j1}, K_{j2}, K_{j3}, and K_{j4}, that are used in 4-round iterations of feistel structure, respectively [6]. The advantages and disadvantages of both NEA-WSN [7] CBCW are shown in the results discussion. The steps of the last image encryption algorithm, NIES, are shown as a program code as follows:

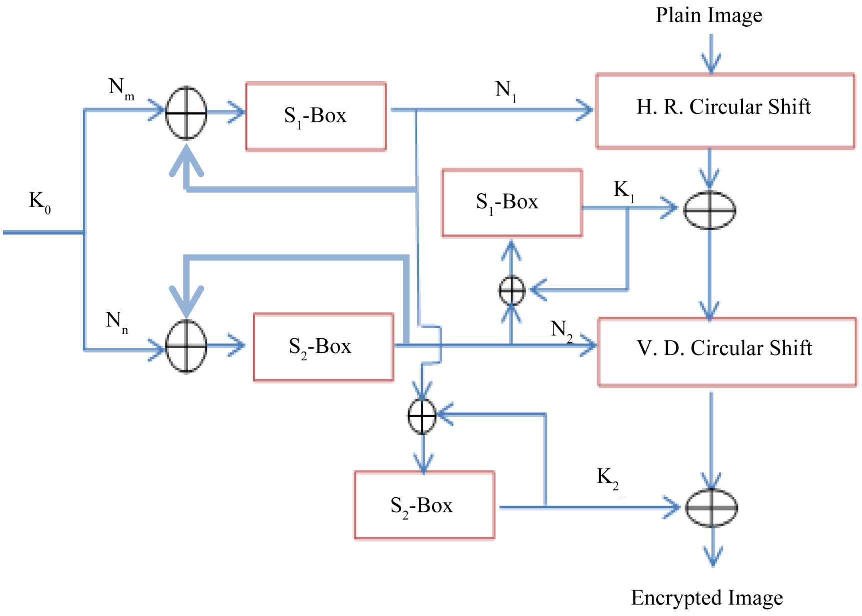


Figure 1. NEA-WSN encryption algorithm.

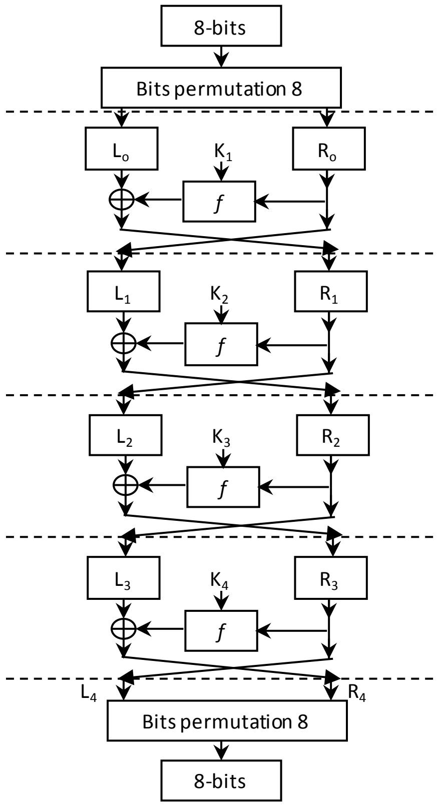


Figure 2. CBCW encryption algorithm.

```
Algorithm 1 (Main loop of the NIES encryption algorithm ($I_o \rightarrow I_R$))
  Require: $I_o$; L; R; $g_1$, $\cdots$, R;
      Initialization r=1; F=L-2;  $I_o^b \rightarrow I_o$
    While r≤R do
        i=0; S=L-1; X=$g_r$; Xg=$X^2$
       While i≤F do
           X←[($X^2$ mod S)X+$X_g$] mod S
            j←i+1+X
      $Z_1 \leftarrow I_{r-1}^b$ [i]
      $Z_2 \leftarrow I_{r-1}^b$ [j]
      $Z_3 \leftarrow Z_1+Z_2$ mod 2
      $I_{r-1}^b$ [i]←$Z_3$
      $I_{r-1}^b$ [j]←$Z_1$
      i←i+1
      S←S-1
        End while
        r←r+1
    End while
    $I_R \leftarrow I_R^b$
    Return $I_R$
```

3. Two Proposed Merging Techniques

In WSN, the encrypted data modulates the carrier phase of the Offset Quadrature Phase Shift Keying (O-QPSK) according to bits values of original message [9]. O-QPSK cannot face the effectiveness of the jamming during the transmission. The disturber stays in the communication channels to exhaust the sensor battery and damage the transmitted message. **Figure 3** shows three signals: transmitted signal (the upper signal), jamming signal (the middle signal), and received signal (the last signal). The disturber adds his jamming signal to the transmitted signal to jam it. He successes to jam both amplitude and phase but he cannot jam the frequency. The inability to jam the signal frequency is the condition of the jamming which is the disturber must use the same frequency of the transmitted signal to jam it.

So, the weakness point of the disturber is the inability to distort the frequency of the transmitted signal which is the main approach of the two proposed merging techniques. The proposed techniques depend on the frequency shift, Δf, instead of the phase shift to face the disturber in the communication channel. The two proposed merging techniques are namely by Image and Audio Interpenetration Technique (IAIT) and Image and Audio Merging Technique (IAMT). IAIT represents both the image **bits** and audio samples by one Low Frequency (LF) signal while IAMT represents both the image **pixels** and audio samples by two different LF signals.

3.1. Image and Audio Interpenetration Technique (IAIT)

At the sender:

Step 1: Encrypt the image using a suitable encryption algorithm.

Step 2: Encrypt the audio using a suitable audio encryption algorithm.

Step 3: Let $f_m(i)$ and $E_x(i)$ be the values of the encrypted audio sample i and the **bit** i of the encrypted image respectively.

Step 4: Multiply each encrypted audio sample by r to get $f_m(i) * r$ where: r is selected carefully to get the form xxx000. For example, let $f_m(i) = 0.897$ then, we can select $r = 10^6$ to get $f_m(i) * r = 897000$. *All the samples values should be converted to positive values.*

Step 5: Let $\Delta f = 500$ Hz.

Step 6: Generate a sinusoidal signal in the time domain, t, as shown in (4) where: A_m is the signal amplitude.

Step 7: Use the general merging equation shown in (4) as a modulating signal and Amplitude Modulation (AM) to transmit $S(t)$ at Super High Frequency (SHF) band or at 2.4 GHz band to the receiver.

$$S_i(t) = A_m \sin\left(2\pi\left(f_m(i) * 10^r + \left(1 - E_x(i)\right)\Delta f\right)t\right) \tag{4}$$

At the receiver:

Step 1: Use AM demodulator to recover the unmodulated signal, $U_i(t)$, where: $U_i(t) = A_u * \sin\left(2\pi f_z(i)t\right)$ with distorted amplitude A_u and frequency $f_z(i) = f_m(i) * 10^r + \left(1 - E_x(i)\right)\Delta f$.

Step 2: Differentiate $U_i(t)$ twice to get $\ddot{U}_i(t) = -A_u\left(2\pi f_z(i)\right)^2 \sin\left(2\pi f_z(i)t\right)$.

Step 3: Divide $\ddot{U}_m(t)$ by $U_m(t)$ to get $-(2\pi f_z)^2$.

Step 4: from step 3, we can get f_z where: $f_z = f_m * 10^r + \left(1 - E_x\right)\Delta f$.

Step 5: As shown later, if $f_z(i)$ value is in the form xxx000, then the value of the encrypted image bit will be 1 and the value of the encrypted audio sample will be xxx000 $* 10^{-r}$. And also, if $f_z(i)$ value is in the form xxx500, then the value of the encrypted image bit will be 0 and the value of the encrypted audio sample is (xxx500 – Δf) $* 10^{-r}$.

Figure 4 shows the merging process through three signals. The first signal (upper signal) is the encrypted image bits which shows only one encrypted pixel of values 10101010 while the second signal (the next one) is

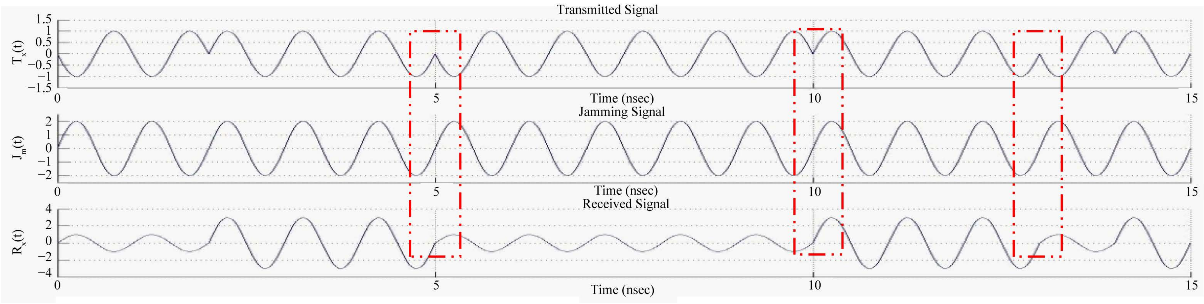


Figure 3. Effectiveness of Jamming on the amplitude, phase, and frequency of the transmitted signal.

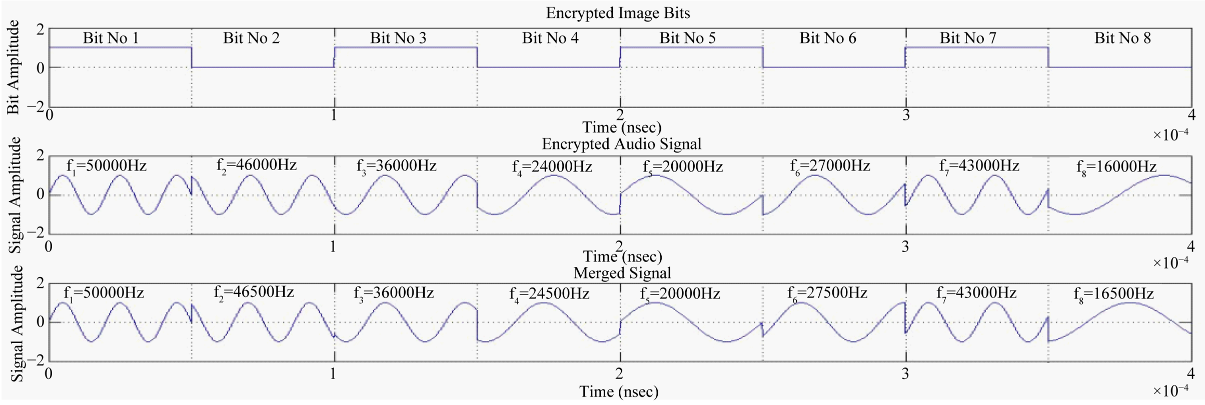


Figure 4. The merging process and jamming effectiveness.

the encrypted audio samples of values {0.5 0.46 0.36 0.24 0.2 0.27 0.43 0.16} which are converted to the form xxx000 to get {50000 46000 36000 24000 20000 27000 43000 16000} respectively. The third signal (the merged signal) is the same as the encrypted audio signal when the encrypted image bit is 1 and Δf = 500 Hz is added to get $f_m(i)*r+\Delta f$ when the encrypted image bit is 0. So, the frequency of the merged signal contains both the encrypted audio samples and the encrypted image bits. Figure 3 shows the jamming effectiveness on both the amplitude and the phase without effectiveness on the signal frequency.

3.2. Image and Audio Merging Technique (IAMT)

At the sender:

Step 1: Encrypt the image using a suitable encryption algorithm.

Step 2: Encrypt the audio using a suitable audio encryption algorithm.

Step 3: Let $f_a(i)$ and $E_{im}(i)$ be the values of the encrypted audio sample i and the **pixel (byte)** i value as a decimal value of the encrypted image respectively.

Step 4: Multiply each encrypted audio sample by r to get $f_a(i)*r$ and r is selected carefully to get the form xxx000. For example, let $f_a(i)=0.897$ then, we can select $r = 10^6$ to get $f_a(i)*r=897000$. *All the samples values should be converted to positive values.*

Step 5: Let Δf_a = 500 KHz and Δf_{im} = 1 KHz.

Step 6: Generate two sinusoidal signals as shown in (5) and (6) where: A_m is the signal amplitude, X_{FMi} is the sinusoidal signal that represented the pixel i of the original image, and Y_{FMi} is the sinusoidal signal that represented the sample i of the original audio. $X_{FMi}(t)$ frequencies are in [1 KHz, 256 KHz] band while $Y_{FMi}(t)$ frequencies are in [0.5 MHz, 1.5 MHz] band. So, both $X_{FMi}(t)$ and $Y_{FMi}(t)$ are in different bands and at LF band.

Step 7: Use AM to transmit both $X_{FMi}(t)$ and $Y_{FMi}(t)$ at Super High Frequency (SHF) band or at 2.4 GHz band to the receiver as shown in Figure 5(a).

$$X_{FMi}(t)=A_m\sin\left(2\pi\left(E_{im}(i)*1000+\Delta f_{im}\right)t\right) \tag{5}$$

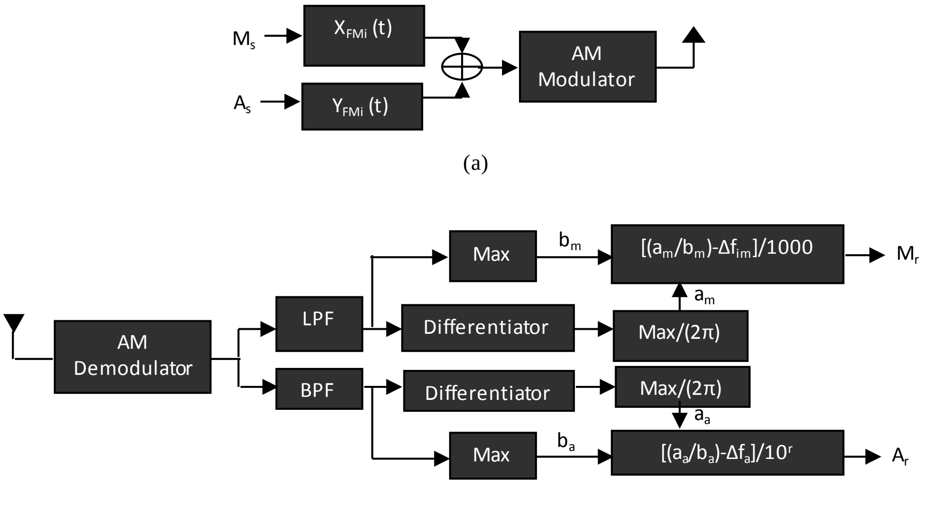
$$Y_{FMi}(t)=A_m\sin\left(2\pi\left(f_a(i)*10^r+\Delta f_a\right)t\right) \tag{6}$$

At the receiver:

Step 1: Use AM demodulator followed by Low Pass Filter (LPF) and Band Bass Filter (BPF) as shown in Figure 5(b). LPF is used to filter the unmodulated image signal, $U_{FMi}(t)$, where: $U_{FMi}(t)=A_{u1}\sin\left(2\pi f_{z1}(i)t\right)$ with distorted amplitude A_{u1} and frequency $f_{z1}(i)=1000E_{im}(i)+\Delta f_{im}$. And also, BPF is used to filter the unmodulated audio signal, $C_{FMi}(t)$, where: $C_{FMi}(t)=A_{u2}\sin\left(2\pi f_{z2}(i)t\right)$ with distorted amplitude A_{u2} and frequency $f_{z1}(i)=f_a(i)*10^r+\Delta f_a$.

Step 3: Differentiate both $U_{FMi}(t)$ and $C_{FMi}(t)$ once to get $U'_{FMi}(t)=A_{u1}\left(2\pi f_{z1}(i)\right)\cos\left(2\pi f_{z1}(i)t\right)$ and $C'_{FMi}(t)=A_{u2}\left(2\pi f_{z2}(i)\right)\cos\left(2\pi f_{z2}(i)t\right)$ respectively as shown in Figure 5(b).

Step 4: The reconstructed value of pixel i, M_{ri}, and the reconstructed value of audio sample i, A_{ri}, can be estimated as shown in (7) and (8) respectively.



(a)

(b)

Figure 5. Image and audio merging technique (IAMT). (a) Sender; (b) Receiver.

$$M_{ri} = \frac{1}{10^3}\left(\frac{\max\left(U'_{FMi}(t)\right)}{2\pi\max\left(U_{FMi}(t)\right)} - \Delta f_{im}\right) \tag{7}$$

$$A_{ri} = \frac{1}{10^r}\left(\frac{\max\left(C'_{FMi}(t)\right)}{2\pi\max\left(C_{FMi}(t)\right)} - \Delta f_a\right) \tag{8}$$

4. The Proposed Audio Encryption Algorithm (PAEA)

The image is composed from pixels and it can be encrypted by one of the image encryption algorithms shown later while the audio is composed from samples and it can be encrypted by the proposed audio encryption algorithm (PAEA) shown in **Figure 6** as follows:

Step 1: Partition the audio samples from one vector into multiple sub-vectors to form a Matrix of size Ma ∗ Na.

Step 2: Apply horizontal right circular shift and vertical down circular shift on the resulted matrix according to the contents of N_h and N_v respectively as shown in **Figure 6**. For example, if the fourth value of N_h is 38 then the contents of row number 4 in the matrix will be circular shifted by 38.

N_h and N_v sizes are M_a and N_a respectively. They are generated from N_m. The first Ma-contents of N_m, denoted by N_{s1}, are applied to S_1-Box to generate N_h while The first Na-contents of N_m, denoted by N_{s2}, are applied to S_2-Box to generate N_v. Their contents are updated with each next matrix by applying XOR operation on N_{s1} and N_{s2} with N_h and N_v before S_1-Box and S_2-Box stage respectively.

S_1-box and S_2-box size is 16 × 16. These *S*-Boxes are used for N_h and N_v updating processes [1]. For example, if the input value applied to S_1-Box is 8D in a hexadecimal format, then the input value will be mapped to the value of row 8 and column D in S_1-Box.

Step 3: Change the samples positions in the resulting matrix using Arnold Cat map encryption algorithm [3] as shown in **Figure 6**.

The decryption procedure is inverse of these steps to get the audio samples in one vector as shown in **Figure 7**.

5. Results and Discussions

This section will discuss both the comparison between decrypted image algorithms and the concept of merging both the image and the audio samples in one signal. So, the discussions of the results will take the following steps:

- Image encryption algorithms.
- Proposed Audio Encryption Algorithm (PAEA).

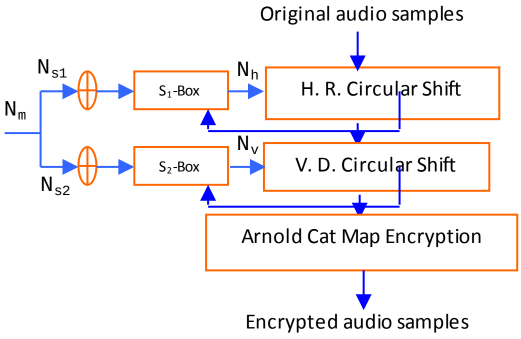


Figure 6. Proposed audio encryption algorithm (PAEA).

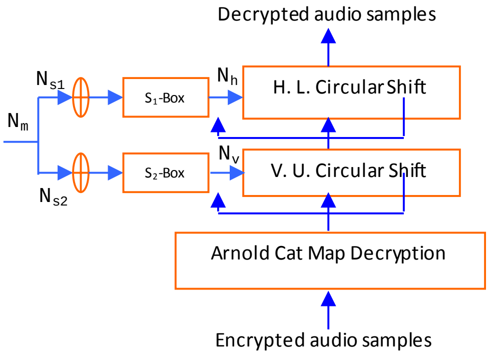


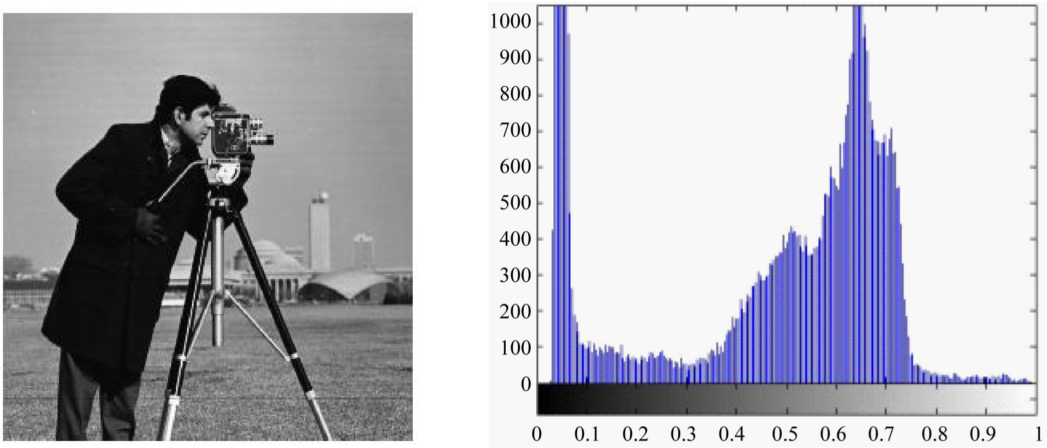
Figure 7. PAEA decryption procedures.

- Two proposed merging techniques.

5.1. Image Encryption Algorithms

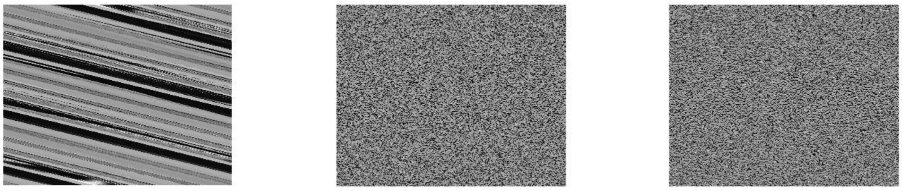
Generally, the image encryption is based on the main general concepts, namely the use of encryption key and the change in the image pixels/bits positions, both of which disturb the image to hid its contents before the transmission in the communication channel. These encryption algorithms are applied on an image of size 256 × 256 as shown in **Figure 8(a)** and its histogram shown in **Figure 8(b)**. The histogram represents number of occurrence of each pixel value in the encrypt image. The y-coordinate represent the number of occurrence of the values of the x-coordinate. The results of the image encryption algorithms show that:

- The change in the **pixels** positions leads to disturb the image as shown in **Figure 9**. Their histograms shown in **Figure 10** are identical to the histogram of the original image shown in **Figure 8(b)**. Although the encrypted images of the encryption algorithms are disturbed shown in **Figure 9** compared with the original image shown in **Figure 8(a)**, attackers can use the histograms as a tool to get some information about transmitted images. Attackers can also use this information to define the nature of the sensor nodes tasks and position.
- And also, the change in the **bits** positions disturbs both the image and its histogram completely as shown in **Figure 11** in comparison with the original image shown in **Figure 8**. So, the change in bits positions disturbed the contents of the original image completely while the change in the pixels positions left the histogram without change.
- The use of an encryption key has appeared in the traditional algorithms such as DES, AES, and RC6. These encryption algorithms use one encryption key with all packets. So, periodic updating of this key is essential because attackers utilize many tools to analyze these encryption algorithms to get the encryption key which may enable them to crack the systems. Both CBCW and NEA-WSN have solved this problem by updating the key with each pixel or with each row and column respectively to avoid the problem of the key-updating periodically through Base Station (BS). So, both CBCW and NEA-WSN defeat DES, AES, and RC6 and also enhance the security level of the systems. The effectiveness of the key updating on the encrypted image



(a) (b)

Figure 8. The original image and its histogram. (a) Original image; (b) Histogram.

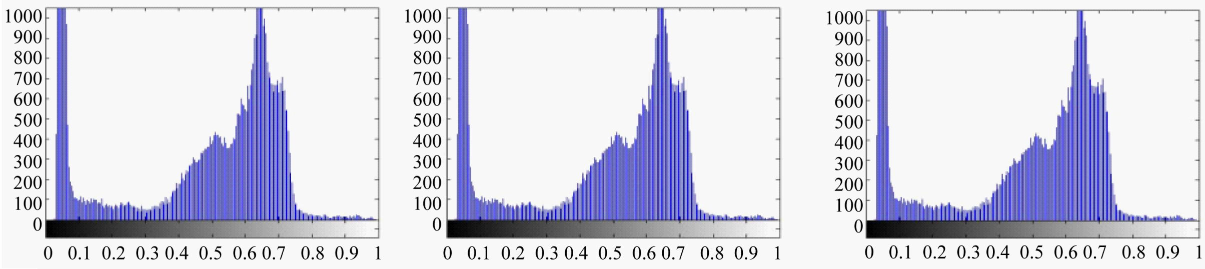


Encrypted image using Arnold cat map

Encrypted image using chaotic piecewise map

Encrypted image using chaotic map

Figure 9. The effectiveness of the change in the image pixels positions.

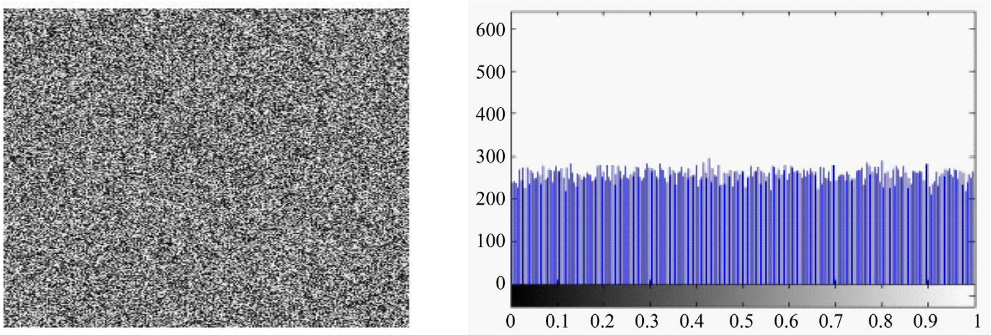


Histogram of the encrypted image using Arnold cat map

Histogram of the encrypted image using chaotic piecewise map

Histogram of the encrypted image using chaotic map

Figure 10. The histograms of the encrypted images shown in **Figure 9**.



(a) (b)

Figure 11. The encrypted image of NIES and its histogram. (a) Encrypted image; (b) Histogram of the encrypted image using NIES.

has been shown by the comparison between CBCW and NEA-WSN using the Correlation Coefficient (CC) as a metric to measure the 30 different encrypted images for the same original image and they are independent as shown in **Figure 12** [7] to ensure the success of key-updating process.

- Active attackers can jam all the transmitted images. So, the noise resistance as a metric is one of the tools used to compare between these image encryption algorithms. Many metrics can be used to measure the effectiveness of the noise on the recovered image such as Mean Absolute Error (MAE) [10]. MAE is a metric used to measure the absolute error between the noisy decrypted image and the original one. The noisy channel is simulated using MATLAB by adding Gaussian white noise of mean zero and variance 0.01 to the encrypted image in the communication channel. The comparison between these algorithms using the noise resistance measurement, MAE metric, shows that:

1) All the chaotic cryptosystems which depend on the change in the pixels positions score lower MAE than the others and NEA-WSN is the next one as shown in **Figure 13** which shows the noise effectiveness without merging process.

2) Chebyshev encryption algorithm scores the highest MAE or the lowest noise resistance.

3) Both NIES which depends on the change in the bits positions and CBCW which updates the encryption key with each pixel are weak to deal with the noise in the communication channel.

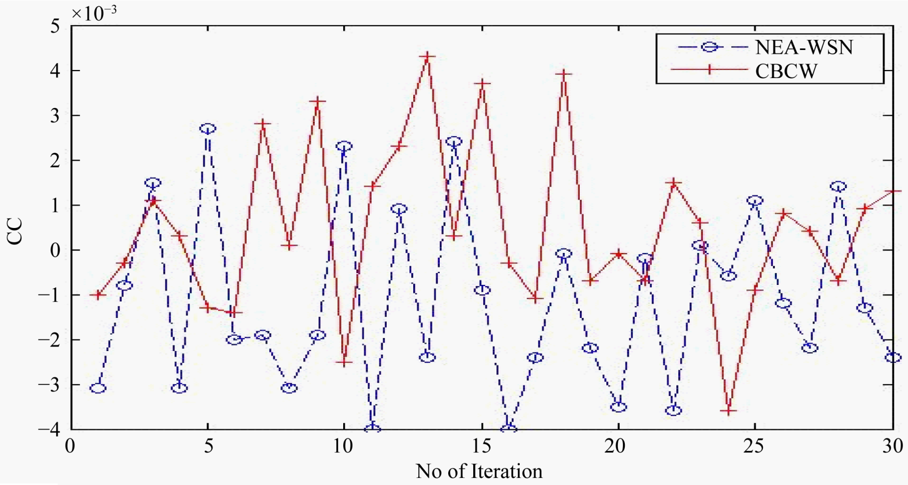


Figure 12. CC measurements for NEA-WSN and CBCW to ensure the success of the key updating process [7].

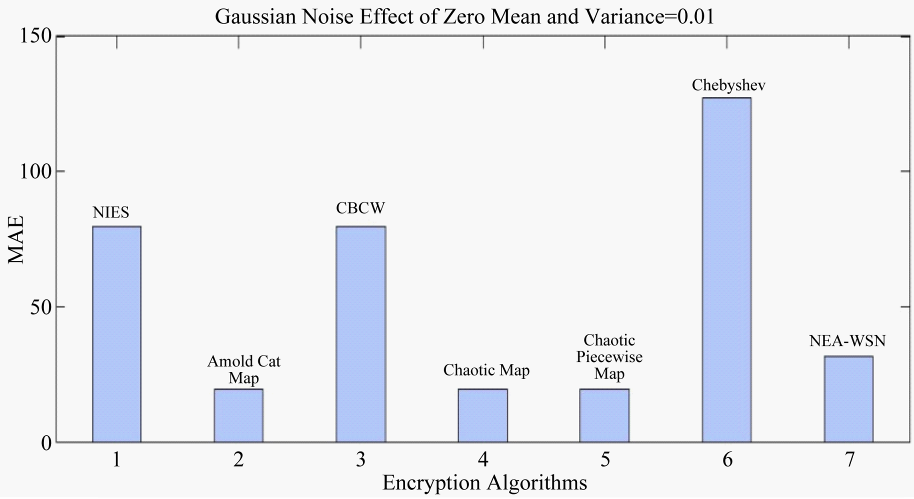


Figure 13. Noise resistance comparison.

- Measurements of CC [7] between the encrypted images without noise effectiveness and the original image show that all the encrypted images are independent from the original image except Chebyshev encryption algorithm which has a problem with its parameters. Chebyshev encryption algorithm does not encrypt the image with all values of x and number of rounds, s, because the measured CC of Chebyshev algorithm takes either 1 or −1 where: CC = 1 means no encryption while CC = −1 means good encryption. The problem is found in x-value with s-value. From the measurements, both x and s must satisfy certain values with each other to get better encryption than Chebyshev algorithm conditions which specified x and s as independent and fall in ranges [0, 1] and [1, 100] respectively. **Figure 14** shows the relationship between both x-values and s-values. The star, *, showed in **Figure 14** means the x-value and s-value at this point give good encryption while the circle, ˚, gives no encryption. So, it should use the star, *, values of both x-value and s-value which refer to the good encryption.
- In addition, Chebyshev Algorithm depends only on one value used to multiply all the image pixels by it to encrypt all the contents of the message (the image). This problem leads to weakening the encryption process and attackers can get great chance to get this value from any information in the network.
- The pervious analysis has revealed that NEA-WSN encryption algorithm is better than the other algorithms and has the highest priority to encrypt the image in the two proposed merging techniques because of the following reasons:

1) The histograms of the encryption algorithms which depend on the change in the pixels positions can give many information to the attackers.

2) The change in the bits positions as in NIES is affected by the noise and no recovered image can be gotten.

3) CBCW spends time [7] to update its key with each pixel which increases the energy consumption with each image in comparison with NEA-WSN. And also it is affected by the noise more than NEA-WSN.

4) Chebyshev Encryption Algorithm reduces the security level because of the dependence on one value to encrypt the data or the image.

5) The key-updating with each image as in NEA-WSN enhances the security level and removes the problem of the key updating periodically through BS. In additions, another enhancements in comparison with CBCW shown in [7].

5.2. Proposed Audio Encryption Algorithm (PAEA)

The Proposed Audio Encryption Algorithm (PAEA) depends on the change in the samples positions only as a way to encrypt the audio signal as shown in **Figure 6**. So, the histogram of the encrypted audio signal is the same as the original one. But, we cannot extract information from the histogram of the encrypted audio signal like the images because the image can be extracted from the natural features of the surroundings while the audio signal cannot be extracted. So, the dependence on the change in the samples positions is acceptable as a way to encrypt the audio samples.

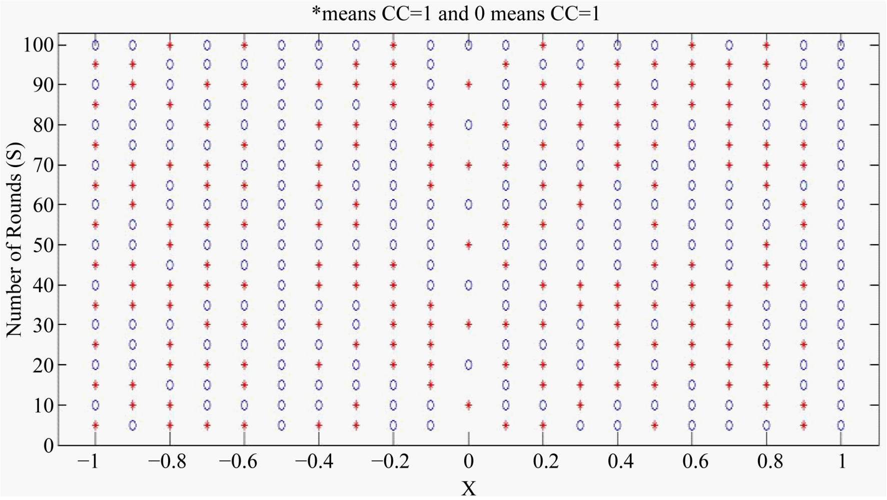


Figure 14. x and s relationship to get good Chebyshev encryption.

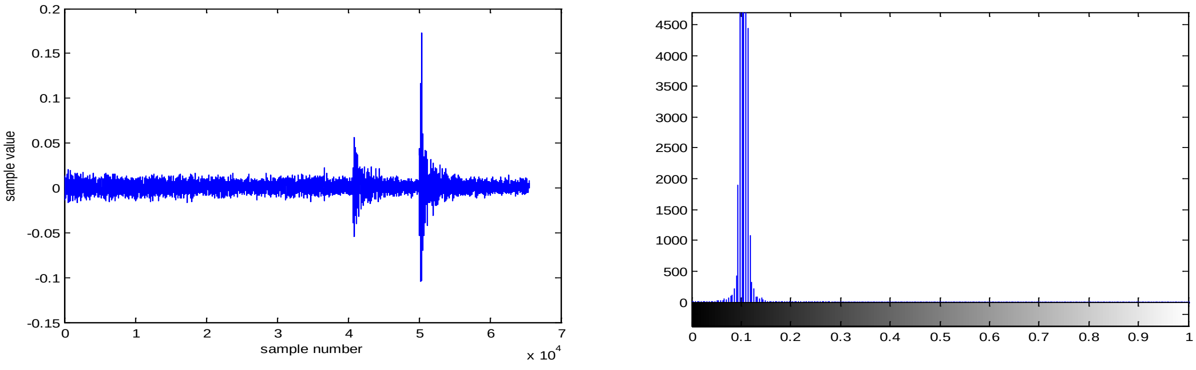
PAEA is tested by an audio sample shown in **Figure 15(a)** and its histogram shown in **Figure 15(b)**. Both encryption and decryption audio samples shown in **Figure 16(a)** and **Figure 17(a)** respectively while their histograms shown in **Figure 16(b)** and **Figure 17(b)** respectively. The histograms of both the original and the encrypted audio samples are the same which show the dependence on the change in the samples positions only.

5.3. Two Proposed Merging Techniques

The discussion of the image encryption algorithms showed the superiority of using the NEA-WSN as an image encryption algorithm in the merging process. The two proposed merging techniques, Image and Audio Interpenetration Technique (IAIT) and Image and Audio Merging Technique (IAMT), are compared with O-QPSK in the presence of jamming. O-QPSK deals with both image and audio samples as binary values separately. IAIT deals with the image as binary values and the audio samples as decimal values. IAMT deals with both image and audio samples as decimal values.

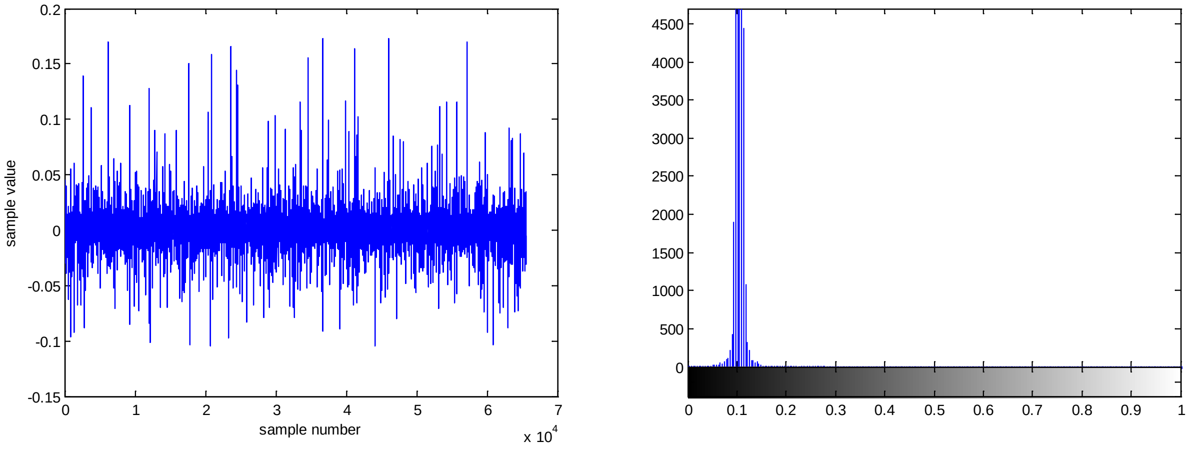
Both image and audio samples are shown in **Figure 8(a)** and **Figure 15(a)** respectively. They are jammed using a jamming signal, $J_a(t)$, shown in (9) where: A_j and f_c are the amplitude and the frequency of the jamming signal respectively. The jamming occurs at the transmission frequency or at f_c = 2.4 GHz. We will consider the amplitude of both $J_a(t)$ and the transmitted signal are the same or $A_j = 1$.

In the case of O-QPSK, both the reconstructed image and the reconstructed audio samples are affected by jamming signal as shown in **Figure 18(a)** and **Figure 19(a)** respectively and their histograms are shown in **Figure 18(b)** and **Figure 19(b)** respectively. Both PSNR and Signal-to-Noise Ratio (SNR) are used as metrics to measure the quality of the reconstructed image and audio samples respectively. SNR is calculated as shown in



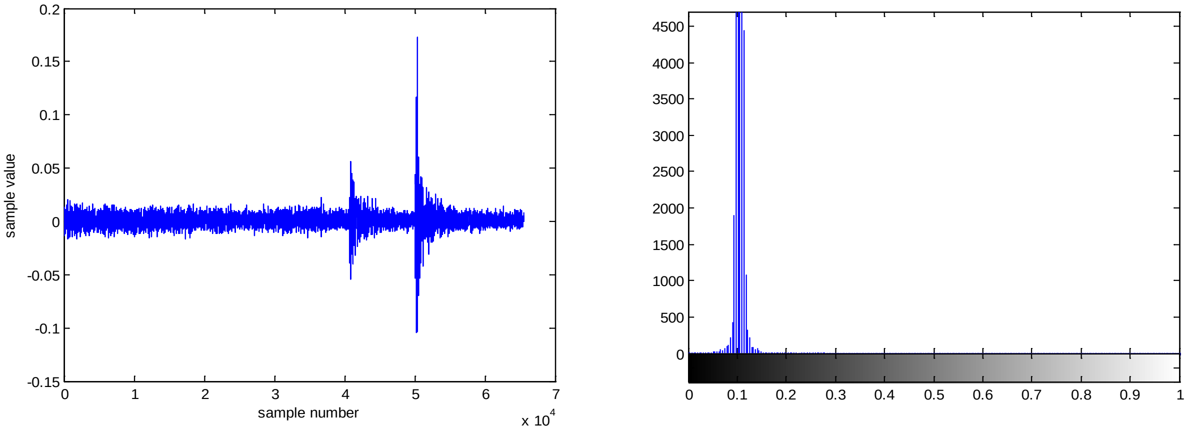
(a) (b)

Figure 15. Original audio samples and its histogram. (a) Original audio samples; (b) Histogram.



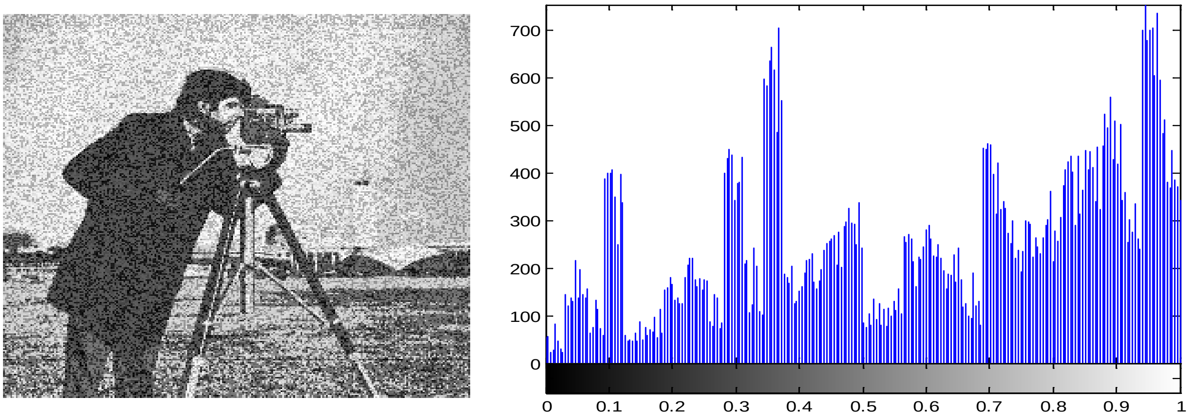
(a) (b)

Figure 16. Encrypted audio samples and its histogram. (a) Encrypted audio samples; (b) Histogram.



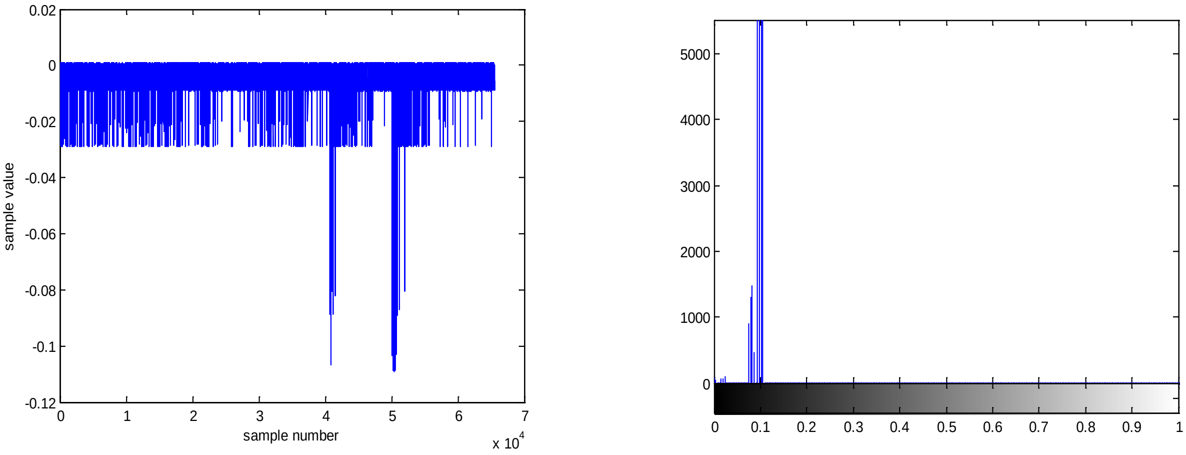
(a) (b)

Figure 17. Decrypted audio samples and its histogram. (a) Decrypted audio samples; (b) The histogram.



(a) (b)

Figure 18. Decrypted jammed image and its histogram in the case of O-QPSK. (a) Decrypted jammed image and its measured PSNR = 15.4268 db; (b) Histogram.



(a) (b)

Figure 19. Decrypted jammed audio samples and its histogram in the case of O-QPSK. (a) Decrypted jammed audio samples signal and its measured SNR = −4.2845 dB; (b) Histogram.

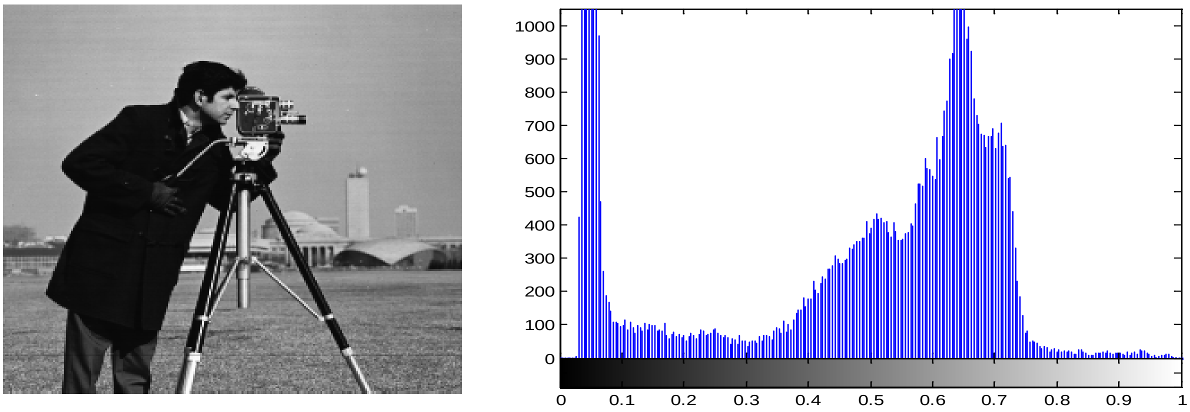
(10) where: N is number of audio samples and both A_s and A_r represent the audio samples values of the original audio and the reconstructed audio respectively. By the comparison with the original image and the audio samples, PSNR and SNR scored 15.4268 dB and −4.2845 dB respectively as shown in **Figure 18(a)** and **Figure 19(a)** respectively. So, both the reconstructed image and audio signal are affected by jamming signal.

In the case of both IAIT and IAMT, both the reconstructed image and audio samples do not affected by jamming effectiveness because of the dependence on frequency shift instead of phase shift as shown in **Figure 20(a)** and **Figure 21(a)** respectively while their histograms are shown in **Figure 20(b)** and **Figure 21(b)** respectively.

$$J_a(t) = A_j \sin(2\pi f_c t) \tag{9}$$

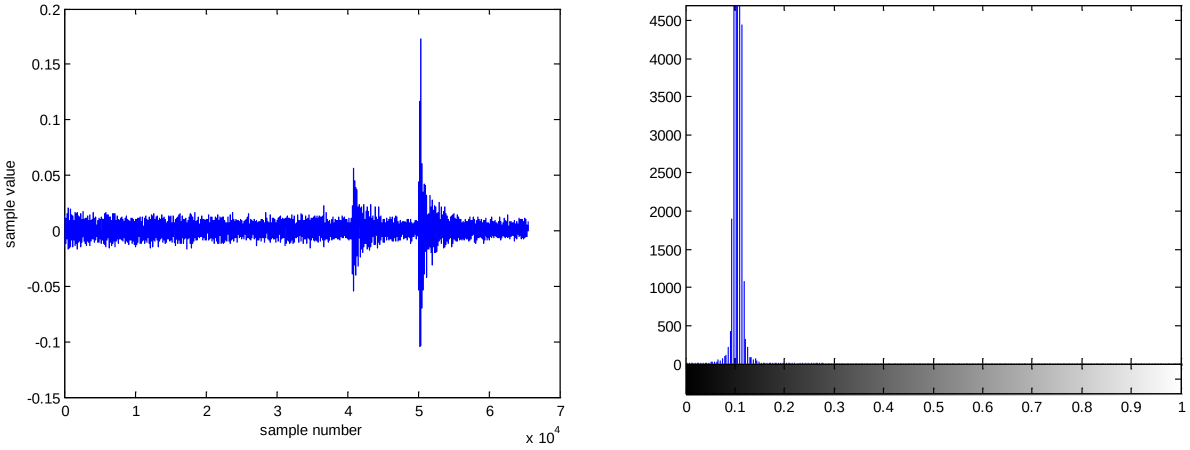
$$\mathrm{SNR} = 10\log\left(\frac{\sum_{i=1}^{N}\left(A_s(i)\right)^2}{\sum_{i=1}^{N}\left(A_s(i) - A_r(i)\right)^2}\right) \tag{10}$$

Number of image pixels used in our comparisons is 65536 pixels and number of audio samples are 65536 samples. If T_b is the duration time used to represent bit value using digital modulation techniques, then the



(a) (b)

Figure 20. Decrypted image and its histogram in the case of both IAIT and IAMT. (a) Decrypted image and its measured PSNR = Inf dB; (b) Histogram.



(a) (b)

Figure 21. Decrypted audio samples and its histogram in the case of both IAIT and IAMT. (a) Decrypted jammed audio samples signal and its measured SNR = Inf dB; (b) Histogram.

transmitted data will require 1048576T_b seconds in the case of O-QPSK, 524288T_b seconds in the case of IAIT, and 65536T_b seconds in the case of IAMT. Because both IAIT and IAMT proposed to represent the decimal values in a duration time equals to T_b. So, IAIT scores high bit rate $\left(B_R = 2T_b^{-1}\text{ bps}\right)$ in the comparison with O-QPSK $\left(B_R = T_b^{-1}\text{ bps}\right)$ while IAMT scores the best one $\left(B_R = 16T_b^{-1}\text{ bps}\right)$. The merging process introduces many benefits for video communication because of many reasons:

1) The enhancement in the bit rate of the transmission of both images (frames) and audio samples enhances the continuity of the received video at the receiver.

2) The reduction in the transmitted data time prolongs the sensor lifetime.

3) No jamming effectiveness will remove the coding techniques from the payload, or packets. So, it will enhance the bits rate of the transmission. And also, it will encourage to remove the coding process time which reduces the processing time at both the transmitter and the receiver.

4) The merging of the image bits with the audio signal in one band as in IAIT gives availability to send more data than before.

5) No need to wait Negative Acknowledgement (NACK) from the receiver.

6) In addition, both PSNR and SNR score infinity or the best reconstructed quality at the receiver.

6. Conclusion

The comparison between multiple image encryption algorithms shows the preference of using an encryption key to the change in the image pixels/bits positions to encrypt the image. Furthermore, the use of key updating in the encryption algorithm has been proved to be more effective than the periodic key updating through BS. NEA-WSN is one of these algorithms. It depends on the key updating with each row and column. Through the discussion and the comparison between these algorithms, it has been showing that NEA-WSN has the highest priority to encrypt the image in the merging process and also the drawbacks in the use of some approaches to encrypt the images. The enhancement in the bit rate is one of the benefits introduced by the two proposed merging techniques, IAIT and IAMT, which depend on the frequency shift instead of phase shift in low frequency band. Both IAIT and IAMT deal with the jamming effectiveness at the receiver. The reconstructed image and audio signals score the best quality using IAIT or IAMT in comparison with O-QPSK. Furthermore, they can remove the coding process to add a new enhancement in the bit rate and the processing time at the transmitter and the receiver. Finally, the discussions showed the superiority of using both the NEA-WSN as an image encryption algorithm and IAMT as a modulation technique to face the jamming effectiveness.

References

[1] Kishk, A.M., Messiha, N.W., Elfishawy, N.A., Elkafs, A.A. and Madian, A.H. (2014) Channel Encryption in Wireless Camera Sensor Network. *Journal of Advances in Computer Networks*, **2**, 125-128. http://dx.doi.org/10.7763/JACN.2014.V2.95

[2] Liu, R. and Tian, X. (2012) New Algorithm for Color Image Encryption Using Chaotic Map and Spatial Bit-Level Permutation. *Journal of Theoretical and Applied Information Technology*, **43**, 89.

[3] Wang, L.H. and Liao, X.B. (2012) A Novel Image Encryption Approach Based on Chaotic Piecewise Map. *Journal of Theoretical physics & Cryptography*, **1**, 37-40.

[4] Khade, P. and Narnaware, M. (2012) 3D Chaotic Functions for Image Encryption. *International Journal of Computer Science*, **9**, 323-328.

[5] Kishk, A., Messiha, N., Ayad, N., El-Fishawy, N. and Abdel-Samie, F. (2010) Fast and Flexible Symmetrical Encryption Algorithm Based on Key-Updating. *Presented at the National Radio Science Conference*.

[6] Chen, S., Zhong, X. and Wu, Z. (2008) Block Chaos Cipher for Wireless Sensor Network. *Science in China Series F*: *Information Sciences*, **51**, 1055-1063. http://dx.doi.org/10.1007/s11432-008-0102-5

[7] Kishk, A., Messiha, N., El-Fishawy, N., Alkafs, A. and Madian, A. (2014) Channel Encryption in Wireless Camera Sensor Network. *Journal of Advances in Computer Networks*, **2**, 125-128. http://dx.doi.org/10.7763/JACN.2014.V2.95

[8] Francois, M., Grosges, T., Barchiesi, D. and Erra, R. (2012) A New Image Encryption Scheme Based on a Chaotic Function. *Signal Processing*: *Image Communication*, **27**, 249-259. http://dx.doi.org/10.1016/j.image.2011.11.003

[9] Chattopadhyay, S. and Sanyal, S. (2009) Comparison of Performance Metrics for QPSK and OQPSK Transmission

Using Root Raised Cosine & Raised Cosine Pulse-Shaping Filters for Applications in Mobile Communication. *International Journal of Computer Science and Information Security*, **6**, 106-112.

[10] Boiroju, N., Yerukala, R., Venugopala, M. and Krishna, M. (2011) A Bootstrap Test for Equality of Mean Absolute Errors. *ARPN Journal of Engineering and Applied Sciences*, **6**, 9-11.