International Journal of Electrical and Computer Engineering (IJECE)
Vol. 12, No. 1, February 2022, pp. 320~330
ISSN: 2088-8708, DOI: 10.11591/ijece.v12i1.pp320-330

Audio steganography based on least significant bits algorithm with 4D grid multi-wing hyper-chaotic system

Hussein Abdulameer Abdulkadhim, Jinan Nsaif Shehab
Department of Communication Engineering, College of Engineering, University of Diyala, Baqubah, Iraq

Article Info

Article history:

Received Mar 3, 2021
Revised Jul 16, 2021
Accepted Aug 1, 2021

Keywords:

4D grid multi-wing hyper-chaotic system
Audio hiding
Audio steganography
Cryptography
LSB

ABSTRACT

Although variety in hiding methods used to protect data and information transmitted via channels but still need more robustness and difficulty to improve protection level of the secret messages from hacking or attacking. Moreover, hiding several medias in one media to reduce the transmission time and band of channel is the important task and define as a gain channel. This calls to find other ways to be more complexity in detecting the secret message. Therefore, this paper proposes cryptography/steganography method to hide an audio/voice message (secret message) in two different cover medias: audio and video. This method is use least significant bits (LSB) algorithm combined with 4D grid multi-wing hyper-chaotic (GMWH) system. Shuffling of an audio using key generated by GMWH system and then hiding message using LSB algorithm will provide more difficulty of extracting the original audio by hackers or attackers. According to analyses of obtained results in the receiver using peak signal-to-noise ratio (PSNR)/ mean square error (MSE) and sensitivity of encryption key, the proposed method has more security level and robustness. Finally, this work will provide extra security to the mixture base of crypto-steganographic methods.

This is an open access article under the CC BY-SA license.

Corresponding Author:

Hussein Abdulameer Abdulkadhim
Department of Communication Engineering, College of Engineering, University of Diyala
Baqubah 32001, Diyala, Iraq
Email: hussein73@mail.ru

1. INTRODUCTION

The widespread development of digital telecommunications and multimedia information network is lead to increase relevance of stealth information transfer systems used in the data stream systems [1]. Also, a new direction of computer (or digital) steganography was appeared, which is aimed to hide messages in various cover file types (graphic, audio, video). Steganography (literally translated from Greek as “secret writing”) is the science of hidden information by keeping the fact of transmission a secret [2], [3]. Unlike cryptography, which ciphers the secret message, steganography hides message inside visual contains of the cover media [4]. Hiding a message based on steganography technique is significantly minimize the probability of detection. If the message is also encrypted, then this provide extra level of protection [5], [6]. Although these two technologies are usually shared in a one system, but the advantages are to remove and decrease the risks of editing and detecting of the hidden information [3], [4]. Moreover, transmitting several medias in one media to reduce the time of transmission and band of channel define as a gain of channel. In the other side, there is a huge amount of information in social networks now and it’s not difficult to hide a message in one way or another [5], [7]. In this case, if the disguised message under the typical content of a social network, then will be quite problematic to detect the fact of hiding information [1], [8], [9]. This information may be, for example, images or audio and hiding one at the other is a required task.

Basically, there are many works proposed for the purpose of audio steganography. Most of these works are efficient, but unfortunately the main attention may by on hiding information more than encryption. Recent researches have been presented for hiding secret data in audio or video. For example, Alisabir [10] presents a ciphering and hiding text method into an audio wave file. firstly, the text was converted to its equivalent American standard code for information interchange (ASCII) code and then scrambled by using data encryption standard (DES) technique. After that, according to secret key generated, the ciphered text is embedded inside a cover audio. While, in the proposed work of [11], the carrier file and secret message are taken into audio format. A pattern matching algorithm is used which will identify a part of the message from the carrier file and return its location. Then by using the standard least significant bits (LSB) method, the location will be embedded with the carrier file to form the stego file. In the same vein, the proposed model of [12] deals with the application of echo hiding for the binary message bits in a carrier signal. 2D-discrete haar wavelet transform was applied on the cover signal to obtain the transform coefficients. Moreover, data encryption is follow pseudorandom sequence, which provide more efficiency and prevents unauthorized decoding. Also, Shah *et al.* [13] suggests audio steganography approach to improve data hiding security. The author uses LSB and most significant bit (MSB) differencing method along with fletcher-munson curve-based method to hide a secret message into a cover audio file and add new samples to the existing audio channel. While in [14], Banik and Bandyopadhyay proposes a key based blind audio steganography method with the discrete wavelet transform (DWT) as well as discrete cosine transform (DCT). To make the system more robust and undetectable, the cocktail party problem has been explored for wrapping stego audio. The DWT technique was also used in [15] for data hiding in the specific location of frame selected. LSB algorithm was used to replace the last bit from original pixel value with the secret data. In addition, a technique of [16] is started audio file sampling operation and then select a suitable bit of each sample to hide the textual information. The resulted file is then encrypted by Rivest–Shamir–Adleman (RSA) algorithm to improve safety in the audio steganography process. But Acharya *et al.* [17] focus on the triangularization method with LSB algorithm for hiding message in video. In the same direction, Alhaj *et al.* [18] presents a novel video steganography technique to hide greyscale image in different layers of a colored video. Furthermore, the work of [19] have presentation of video steganography based on zero order hold (ZOH) technique. Also, a new video steganographic method was proposed in [20] and works directly on the frames selected to hide the secret message using LSB method. The works of [21], [22] suggests video steganography methods based on either human vision interest region with face detection algorithm or a hybrid steganography model which satisfies the kerckhoffs principle.

To achieve robustness in protection and more difficulty in detection, this paper proposes a cryptography/steganography algorithm in the channel of information. This method is to hide a secret audio /voice message in two different medias in the same time: audio and video (cover media). This aim will be achieved by using LSB algorithm combined with 4-D grid multi-wing hyper-chaotic (GMWH) system. Of course, LSB steganography method is a well-known method used for hiding information, but not enough to protect secret message. Therefore, combining LSB with novel grid multi-wing hyper-chaotic system will produce robustness of security (high level security). In the sender side, shuffling of an audio using key generated by GMWH system and then hiding message by using LSB algorithm will provide more difficulty of extracting the original audio by hackers or attackers. In case of hiding in video, there are two options: hiding in the frames and/or in audio of the video. This will expand the area of hiding and difficulty of detection as well as the format type of audio (secret & cover), for example, MP3 and WAV. will assisted on the process of hiding. In the receiver side, the reconstruction process and extraction secret audio will be opposite to the process in the sender. However, contribution of this work represents one of the series started by the authors works explained previously in [2], [4], [23] to develop image/audio steganographic techniques. Additionally, the present work will solve the security task of the stego-audio with high sensitivity, as well as the selection of cover media, length, format. Finally, the other sections are organized as: Preliminaries, the proposed procedure, results and discussion, and finally, conclusions.

2. PRELIMINARIES

2.1. LSB hiding method

Hiding information in the least significant bits of the container is historically one of the first and perhaps the most well-known to the general public approach, which can be used both for steganography and protecting signals with digital watermarks. It is very simple and allows embedding a sufficiently large amount of information without any noticeable distortion of the container. However, these methods that used this approach, as a rule, have low resistance to distortion of the information carrier and easily can be relatively subjected to stego-analysis. Therefore, they have very limited applicability. Nevertheless, LSB-embedding is quite suitable for tasks in which there are no stringent requirements for resistance to certain types of attacks [9], [18]. The essence of LSB is to replace the last significant bits in the cover message (image, audio or video) with the secret message bits to be hidden. The difference between empty and filled areas should not be perceptible to human eyes. LSB is more resistant to geometric transformations through by varying in a wide range of image quality, which makes it impossible to determine the source of the image. A basic LSB substitution algorithm is to take m samples of secret message (the total length) and then convert from integer numbers into binary. At the end, each last bit pixel of the cover frame will be substituted by the secret message bits [2], [4], [9].

2.2. Novel GMWH-chaotic system

According to [24], [25] the modified Sprott B system was produced by adding a linear feedback control to the construction of the famous Sprott B chaotic system to generate a novel 4-Dimension independent system described as shown in Figure 1.

$$\begin{aligned} x &= -yz - dw \\ y &= z^2 - 1 \\ z &= -ax - byz - z \\ w &= cz \end{aligned} \qquad (1)$$

Where x, y, z and w are the state variables and a, b, c and d are constant coefficients. In this work, the values of a=8, b=3, c=1, d=0.01, x=-0.7, y=0.1, z=0, w=0 are selected as coefficients and initial conditions.

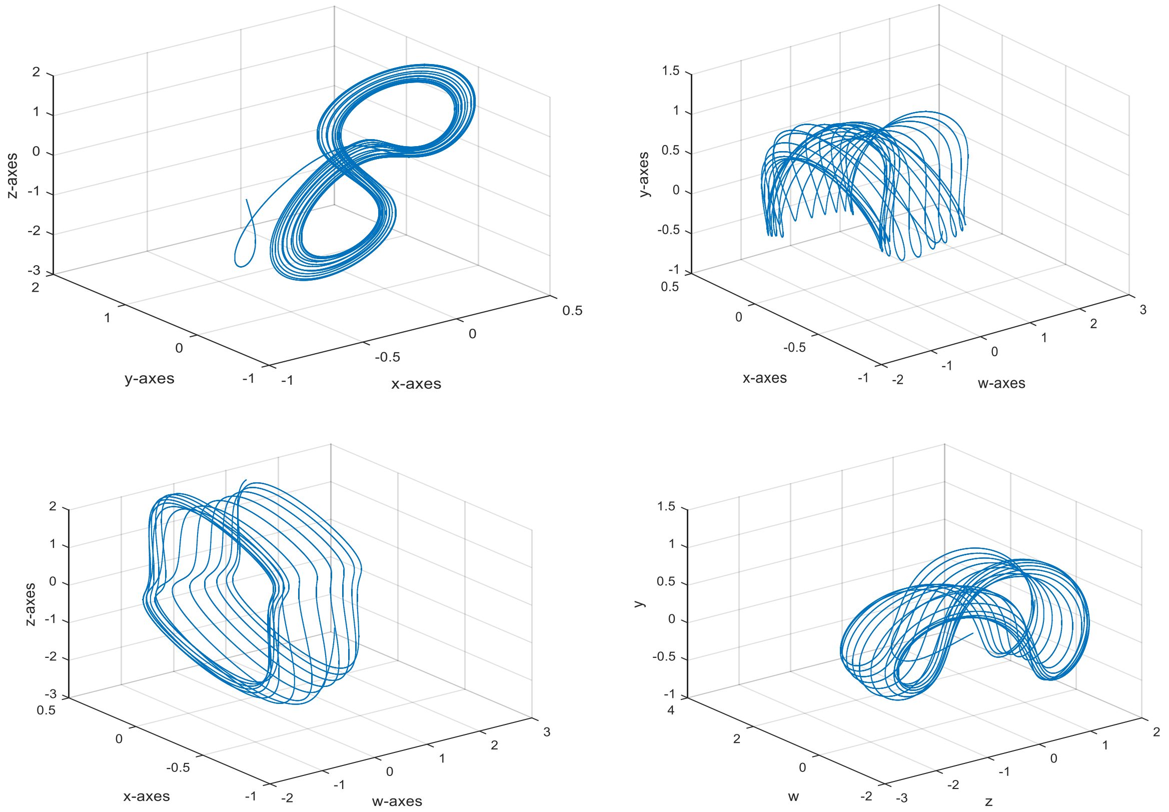


Figure 1. GMWH system attractors

3. THE PROPOSED PROCEDURE

In this work, the suggested cryptography/steganography system is shown in Figure 2. Shuffling of the secret audio will be based on a random number generated by 4D GMWH. This secret audio will be hide into cover message (audio or video) in the transmitter channel, but the two messages (secret and cover) will be reconstructed in the receiver. Moreover, the hiding process briefly will be in three main types: i) hiding an audio in an audio and/or in the audio of a video, ii) hiding an audio in the frames of a video, and iii) hiding an audio in both (audio and video). However, format of the secret audio used in the tests is either WAV or MP3.

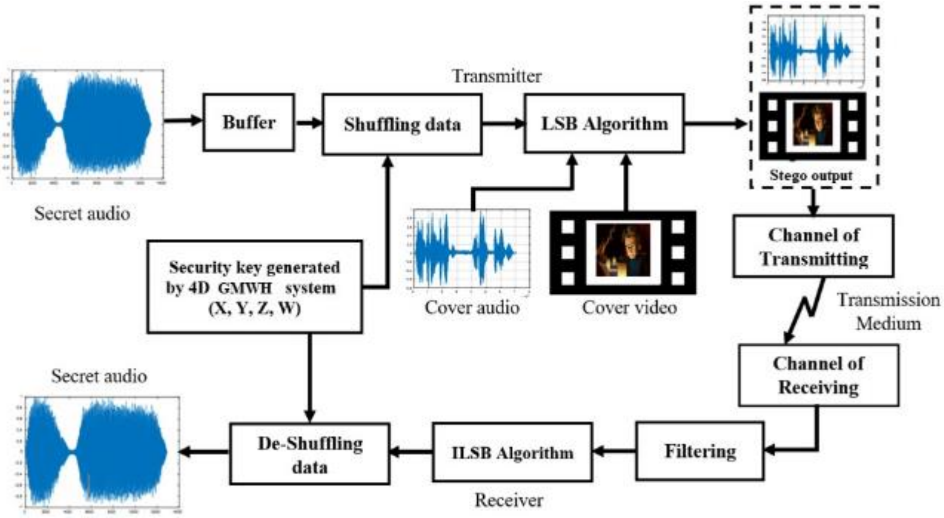


Figure 2. The steganography system proposed for hiding and reconstruction message

3.1. Hiding an audio in a cover audio

Proposed procedure presented in this work is depend on the quality of both secret and cover audio. In fact, the quality of hiding obtained will mainly follow the audio quality, which is 8 bit per second or more (16, 24 bps). Furthermore, the cover audio format such as MP3 or WAV will produce different quality of hiding. Consequently, this will effect on the reconstructed results at the receiver.

Consider a secret audio with format of MP3 and length (L_S)=1 second and a cover audio with format of MP3 and quality of 8, 16, and 24 bps. The procedure starts by shuffling of secret data samples positions according to positions of the key generated by grid multi-wing hyper-chaotic system to create random position values:

$$X_{i+1}(s) = mod(floor(X_i(s).10^{16}), 256) \tag{2}$$

where $X_{i+1}(s)$ secret key generated from GMWH system. The shuffling results are shown in the Figure 3. The next step is converting the secret and cover audios to decimal and then to binary form, then the results are stored in temporary arrays and apply hiding using LSB algorithm.

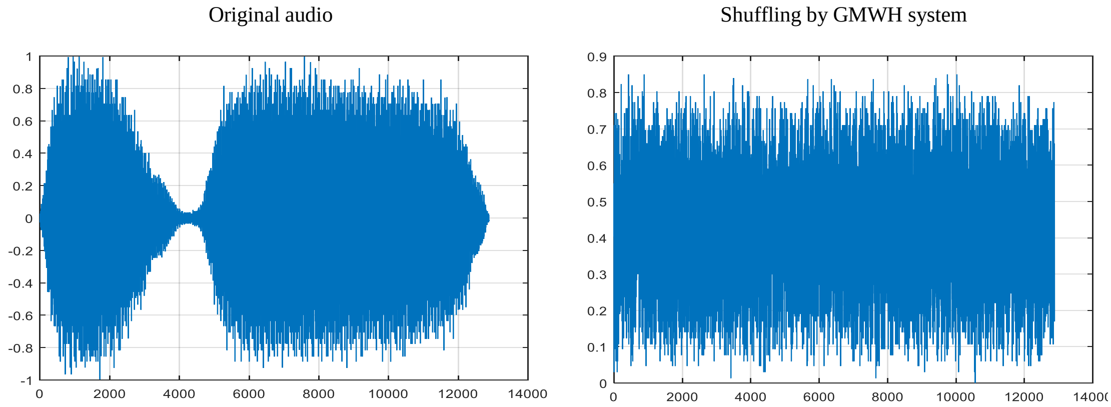


Figure 3. Shuffling of secret audio

Note that the sorting process for the new positions obtained from GMWH chaotic $X_{i+1}(s)$ is to construct the index array scrambled. This array has similar dimension of the secret audio with arranging in form of ascending order as shown in Table 1. Moreover, by using the following expressions for the secret shuffled and cover audios, the scale values of sample will be from 0 to (2^n-1) based on (1) and (2):

$$S_{new} = S_{val} + abs(min(S_{val}))$$
$$S_{sc} = ROUND(S_{new} * (2^n - 1)/ max(S_{new})) \quad (3)$$

where S_{new}- new sample selected; S_{val} the sample value; S_{sc} decimal sample value, which will be convert to binary; $n = 8, 16, 24\ bits$. Figure 4 represents the applied steps of hiding operation.

Table 1. The index array scrambled

Original position for the samples	Sort according to GMWH system X_{new}	New position to the sample
0.026062011718750	6	0.011199951171875
0.003204345703125	3	0.003082275390625
0.010864257812500	4	0.003204345703125
0.003082275390625	2	0.010864257812500
0.011199951171875	1	0.008789062500000
0.008789062500000	5	0.026062011718750

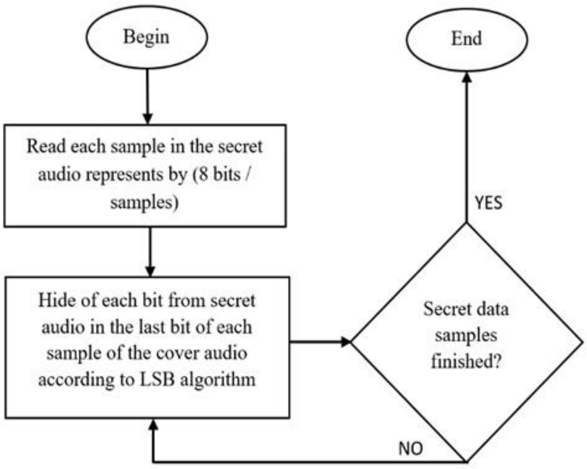

Begin
Read each sample in the secret audio represents by (8 bits / samples)
Hide of each bit from secret audio in the last bit of each sample of the cover audio according to LSB algorithm
Secret data samples finished?
YES
NO
End

Figure 4. Flow graph of hiding process

In the receiver side, reconstruction process of the secret audio is a converse process of the transmitter as shown in Figure 2. Coefficients and initial conditions of GMWH system, ((0), y(0), z(0), w(0),(a,b,c,v,k)), with the stego-audio and the secret key should be existing in the receiver side. Reconstruction process with least errors will be as the following algorithm:

```
Begin
{
Converting the stego-audio to decimal number and then into binary number.
Choosing the last bit of (8, 16, 24) bit from each number and save in the temporary buffer.
Converting binary to decimal number and then into sample value.
By depending on coefficients and initial conditions of 4D GMWH system, set each sample to
the original position
At the end, {reconstruct the target audio}
}
End
```

3.2. Hiding an audio in the frames of a video

The second procedure is based on shuffling of the secret audio by a random key provided from 4-D GMWH chaotic system and hiding into a cover frame with (512×512×3) to produce stego-frame. Consider the cover frame as shown in Figure 5, then one secret audio shuffled will hide in frames of the video. The values obtained from the secret audio shuffled are substituted in the pixels. Hiding will be in a last bit of the pixel according to the length of the audio (hiding in the last bit of the red color, then in the last bit of the green color, and then in the last bit of the blue color). Consequently, the cover frame will be constructed with a least noticeable damage. Moreover, in each frame, it can be hide one secret audio with length (LS) of 1 or 2 sec (audio 1-channel). In case of hiding audio with long length (LS>2 sec.), then it possible to split audio to M parts as follow and hide each part in one frame of the video:

$$M = ROUND\left(\frac{L_S}{2}\right),\ L_S = 3,4,5\ldots\ in\ sec.$$

Consider the length of a video (Lvideo) is n sec. with k-frames per sec., and the video has color frames, then the capacity of hiding will be: sec where M and N are the numbers of rows and column in one frame. Depending on this expression, C sec. of audio can be hide in k frames. For example, in this work, length of the secret audio hidden will be 1 or 2 sec. in one frame and 6 sec. under division in the frame (red, green and blue of color video).

Figure 5. Selected frame from the video

Procedure of hiding will be as the following pseudocode:

```
Begin
{
Select frame from a video;
Convert this frame from decimal to binary;
Save results in an array of the temporary buffer;
Read data samples of the audio;
Shuffling data according to the key generated from GMWH system according to the (2);
The resulted values are modified to integer between (0,255);
Scale the sample value selected from 0 to (2n-1) using (3);
Apply the following to complete hiding operation:
Begin subroutine
{
Read every sample of 8, 16 or 24-bit/sample secret audio;
do
{
Hide every bit from the secret audio using LSB algorithm in the last bit of every pixel of
the cover frame (the 8-bit for gray frame or 24-bit for color frame);
}while samples not finished
}End do
Produce stego-frame by Converting back from binary to decimal;
}
End
```

To achieve reconstruction process with least errors in the receiver side, stego-frame, secret key and coefficients and initial conditions of 4D GMWH system should be available in the receiver, then:

```
Begin
{
Convert the received stego-frame to 3-color layers (red, green, and blue);
Convert each frame from decimal mode to binary mode;
Choose the last bit from every pixel;
Convert to decimal value and then into sample number;
Return every sample to its original position based on coefficients & initial conditions of
4D GMWH chaotic sys.;
Finally {Reconstruct audio}
}
End
```

4. RESULTS AND DISCUSSION

4.1. Peak signal-to-noise ratio (PSNR) analysis

The peak signal-to-noise ratio (PSNR) is estimated for the original frame and stego-frame to illustrate quality [2]. Table 2 contains results of PSNR values for obtained audio before and after hiding using MATLAB program according to:

$$PSNR(dB) = 10\, log_{10} \frac{\rho^2_{max}}{\frac{1}{RC}\sum_{i=0}^{R-1}\sum_{j=0}^{C-1}[X_{i,j}-\hat{X}_{i,j}]^2} \quad (4)$$

where ρ-max. pixel or sample value; R, C total number of pixels or samples in every row and column respectively; i,j - row and column numbers, $X_{i,j}$-original audio or video (frame) and $\hat{X}_{i,j}$-stego-audio or stego-frame. The Table 2 represents the first case, which is hiding 1 second with (8, 16, or 24 b/s) in different lengths. In case of the audio is 16 or 24 b/s, there is no results obtained because of both secret & cover audios have the same length, therefore, we need a longer length. When the audio reached to 3 seconds, the process is completed at least bit only. The insignificant variance in storage size with the same sampling frequency between the audios produces an insignificant difference in PSNR.

Table 2. PSNR results for hiding audio in audio

Secret audio	Properties	Cover Audio	Properties	PSNR (dB) for (8 bps)	PSNR (dB) for (16 bps)	PSNR (dB) for (24 bps)
Train.wav	Length=1 sec Bitrate=131 kbps Size=25.1 kB Sample Rate: 8192 Total Samples: 12880	Baby cry.wav (24 bps) Baby cry.wav (16 bps)	Length:1 sec. Bitrate:705 kbps Size:137 kB Duration: 1.5950 Sample Rate: 44100 Total Samples: 70340	89.7097 41.5447	No result	No result
		Baby cry.mp3 (24 bps) Baby cry.mp3 (16 bps)	Length:1 sec. Bitrate: 128 kbps Size:25.8 kB Duration: 1.6560 Sample Rate: 48000 Total Samples: 79488	89.6307 41.4658	No result	No result
		Wolf .wav (24 bps) Wolf .wav (16 bps)	Length:2 sec. Bitrate:705 kbps Size:238 kB Duration: 2.7725 Sample Rate: 44100 Total Samples: 122268	90.6739 42.5089	90.6738 42.5089	No result
		Wolf.mp3 (24 bps) Wolf.mp3 (16 bps)	Length:2 sec. Bitrate:128 kbps Size:44.6 kB Duration: 2.8560 Sample Rate: 48000 Total Samples: 137088	90.6281 42.4631	90.6281 42.4632	No result
		Wolf.wav (24 bps) Wolf.wav (16 bps)	Length:3 sec. Bitrate:705 kbps Size:328 kB Duration: 3.8114 Sample Rate: 44100 Total Samples: 168084	90.3123 42.1474	90.3123 42.1474	90.3124 42.1474
		Wolf.mp3 (24 bps) Wolf.mp3 (16 bps)	Length:3 sec. Bitrate:128 kbps Size:60.7 kB Duration: 3.8880 Sample Rate: 48000 Total Samples: 186624	90.3057 42.1407	90.3056 42.1407	90.3057 42.1407
		Music.wav (24 bps) Music.wav (16 bps)	Length:6 sec. Bitrate:1536 kbps Size:1.15 MB Duration: 6.3065 Sample Rate: 48000 Total Samples: 302712	90.4016 42.2367	90.4016 42.2367	90.4017 42.2367
		Speaker man.wav (24 bps) Speaker man.wav (16 bps)	Length:11 sec. Bitrate:1411 kbps Size:1.97 MB Duration: 11.7499 Sample Rate: 44100 Total Samples: 518169	90.4690 42.3040	90.4690 42.3041	90.4693 42.3041

In the Table 3, whenever the data transmitted is less, the transmission is faster and has less risk and a one-second audio with 16 or 24-bits cannot be hide in one second at the least bit only. Therefore, we suggested full benefit of the cover by hiding these data in the bit 22, 23, and 24 in case of 24 b/s and in 14, 15, and 16 in case of 16 b/s according of audio representation. Consequently, hiding audio with length of 1 sec. in the cover with 1 sec. will be accomplished easily and efficiently, but if the length is more than 1 sec, then the above suggestion will be used too. As a result, high resolution, short time of transmission and least damage will be obtained.

Another solution is suggested by divide the encrypted audio into, as example, four equal parts, and then hide the first part in bit 24, the second part in bit 23, the third part in bit 22 and the fourth by 21. The same procedure will be applied in case of 16 bit/sample, where hiding will be in bits 16, 15, 14, and 13. The benefit of using these bits will be effective and efficient, especially the audio of 24 bit/sample gives better results and represents a better area for hiding with less distortion occurs.

Table 3. PSNR results of hiding audio with 16- and 24- bit/sample

Secret audio	Properties	Cover Audio	PSNR (dB)	PSNR (dB)	PSNR (dB)
			for (8bps)	for (16bps)	for (24 bps)
Train.wav	Length=1 sec	Baby cry.wav (24 bps)	89.7104	89.7104	89.7104
	Bitrate=131 kbps	Baby cry.wav (16 bps)	41.5419	41.5419	41.5419
	Size=25.1 kB	Baby cry.mp3 (24 bps)	89.7025	89.7025	89.7025
	Sample Rate: 8192	Baby cry.mp3 (16 bps)	41.5375	41.5339	41.5339
	Total Samples: 12880	Wolf .wav (24 bps)	90.6737	90.6737	90.6737
		Wolf .wav (16 bps)	42.5087	42.5087	42.5087
		Wolf.mp3 (24bps)	90.6277	90.6277	90.6277
		Wolf.mp3 (16 bps)	42.4628	42.4628	42.4628
		Wolf.wav (24 bps)	90.3219	90.3219	90.3219
		Wolf.wav (16 bps)	42.1552	42.1552	42.1552
		Wolf.mp3 (24 bps)	90.3051	90.3051	90.3052
		Wolf.mp3 (16 bps)	42.1402	42.1389	42.1389
		Music.wav (24 bps)	90.4025	90.4025	90.4025
		Music.wav (16 bps)	42.2376	42.2376	42.2376
		Speaker man.wav (24 bps)	90.4691	90.4691	90.4691
		Speaker man.wav (16 bps)	42.3042	42.3042	42.3042

Through comparison with the results of Table 3, the following Table 4 has a slight change obtained with a higher security level in case of long length (more than 1 sec. and more than one channel) and 16 and 24 bit/s cover audios. This solution has more efficiency if the channels are separated, and hiding will be in MSB as well as LSB. Therefore, MSB and LSB methods have been merged to solve the problem of hiding long length audio to achieve the required accuracy and thus obtained good results with more efficient to use the cover.

Table 4. PSNR results of using MSB with LSB

Secret audio	Properties	Cover Audio	PSNR (dB)	PSNR (dB)	PSNR (dB)
		Speaker.wav (11sec)	for (8bps)	for (16bps)	for (24 bps)
Train.mp3	Length=13 sec, 2 channels	(24 bps)	90.4837	90.4886	90.4901
	Size=308 kB Bit Rate: 186.4240	(16 bps)	42.3187	42.3236	42.349
Speaker.wav	Length=11 sec,2 channels	(24 bps)	90.4706	90.4790	90.4810
	Size=308 kB Bit Rate: 186.4240	(16 bps)	42.3131	42.3140	42.3161

Table 5 contains PSNR results for hiding audio with more than one channel (2, 3, …) in a video (frames). These channels are separated into many channels. Each channel will be processed separately to perform the steganography process. In this work, we suggested that the locations of the pixels be changed, while the audio is divided into channels and each channel is divided into small parts and converted into Bits. This method gives a higher level of security because the audio has been changed by pixels, then partitioned and hidden, and has been retrieved efficiently. Tests are proving that the insignificant changes in few pixels of a frame will not be noticeable and not effect on the resolution. Moreover, the tests are proving that using the WAV, audio format is a better than using MP3 format, and hiding process depends on the audio length and frequency.

Table 5. PSNR results of hiding audio in video

Secret audio	Properties	Cover Frame	Properties	PSNR (dB) (8 bps)	PSNR (dB) (16 bps)	PSNR (dB) (24 bps)
Train.wav	Length=2 sec. Bitrate=13 kbps Size=25.1 kB Sample rate: 8192 Total sample: 12880	Vtest.avi	Length=11 sec. Size=1.13 MB Frame width=512 Frame height=512 Frame rate=23 frame/sec. Data rate=652 kbps Total bitrate=844 kbps	59.9923	56.9911	55.2318

4.2. Histogram analysis

Histogram analysis is a well-known algorithm used to illustrate and prove that the statistical properties of the secret and cover (stego-) messages are not affected by varying bits in some pixels or samples [26]-[28]. Table 6 contains some results for the cover audio and stego-audio before and after hiding, while Table 7 contains some results for the cover and stego-frame before & after hiding. Analysis results show that the histogram of frame/audio before hiding are the same that after reconstruction. In fact, there are no change noted between original and reconstructed MP3 audio format despite of minor changes in histogram. These changes follow the properties of MP3 format.

4.3. Key space examination

The whole different keys, which are used in the encrypting is so-called “key space size” [2], [4], [28]. In this work, the key size applied is 10^{64}, while the chance of detection key is equal to $(2 \times \mathit{key\ size\ in\ bits})$. This led to conclusion that combining of GMWH coefficients & initial conditions are great enough to avoid any in-depth search.

Table 6. Histogram of the cover and stego-audio before and after hiding

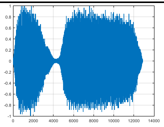
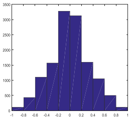
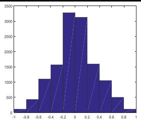
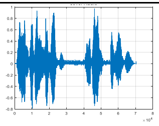
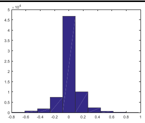
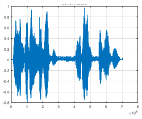
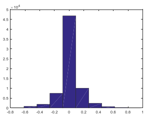
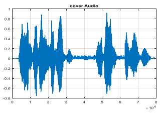
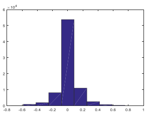
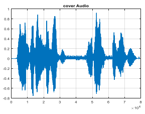
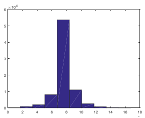
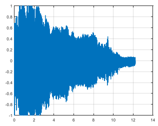
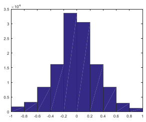
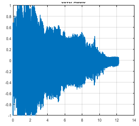
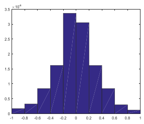
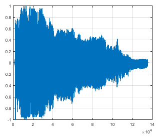
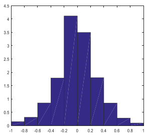
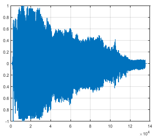
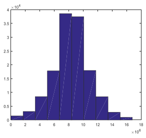
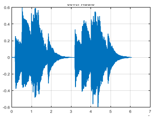
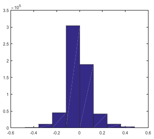
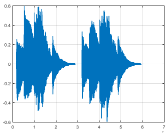
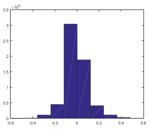
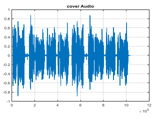
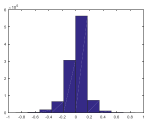
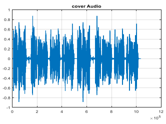
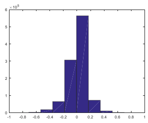
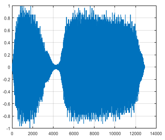
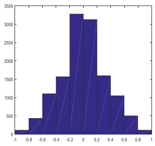
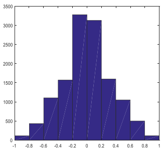
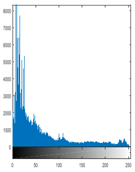
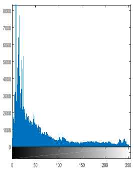
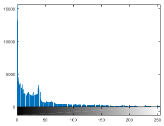
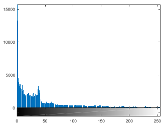
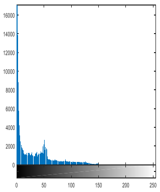
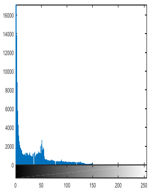
Secret Audio	Histogram Before Hiding	Histogram After Reconstruction	Cover Audio	Histogram Before Hiding	Stego-Audio	Histogram After Hiding
 Train.wav			 Baby cry.wav	 Baby cry.wav		
			 Baby cry.mp3		 Baby cry.mp3	
			 Wolf.wav		 Wolf.wav	
			 Wolf.mp3		 Wolf.mp3	
			 Music.wav		 Music.wav	
			 Speaker man.wav		 Speaker man.wav	

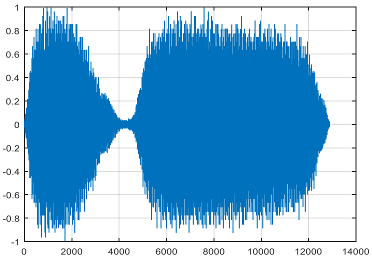
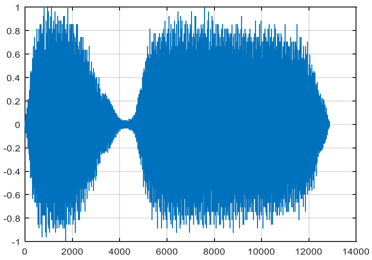
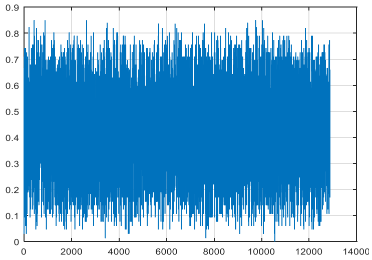
Table 7. Histogram of the cover and stego-frame before and after hiding

Secret Audio	Histogram Before Hiding	Histogram After Reconstruction	Cover Frame	Histogram Before Hiding	Steg- Frame	Histogram After Hiding
 Train Way				 Red Cover		 Red Cover
				 Green Cover		 Green Cover
				 Blue Cover		 Blue Cover

4.4. Examination of key sensitivity

Degree of the changes in an encrypted frame/audio instigated by a tiny variation in a secret key is so-called "key sensitivity" [2], [4], [29]-[31]. Table 8 show the high sensitivity to a tiny variation in secret key (just the exact key can be return the secret message in the proposed system).

Table 8. Examination of key sensitivity

Original Audio	Reconstruction by Same Key W=0.9	Reconstruction by Incorrect Key W=0.9000000000000009
		

5. CONCLUSION

This paper proposes a system to hide a secret audio (.wav, .mp3) different length and different number of channels in a cover audio/video based on different types of methods (LSB+4D GMWH Chaotic system). The efficient key provided by 4D GMWH chaotic system will support security and robustness and difficulty of detection against hackers and attackers. Furthermore, the stego-audio and stego-frame are produced with least noticeable error or damage according to PSNR and histogram analyses. In case of hiding a long audio in a video (in both audio and frames), the mentioned procedures will be applying. This will be done by utilizing all the video space and dividing the long secret audio into parts and hiding them in the video. Moreover, combining of GMWH coefficients and initial conditions are quite sufficient to prevent any comprehensive search, especially, when the key generated has high sensitivity. Exploiting an additional bit for hiding, and combining of MSB with LSB will support the hiding of long audio with reducing transmission time and provide high resolution. However, proposed algorithms provide extra security for the base of cryptography/steganography techniques. Employing of modern chaotic techniques with the digital watermarking algorithms to enhance security is the future work of our team.

REFERENCES

[1] R. Din and A. J. Qasim, "Steganography analysis techniques applied to audio and image files," *Bulletin of Electrical Engineering and Informatics (BEEI)*, vol. 8, no. 4, pp. 1297-1302, Dec. 2019, doi: 10.11591/eei.v8i4.1626.

[2] J. N. Shehab and H. A. Abdulkadhim, "Image steganography based on least significant bit (LSB) and 4-dimensional lu and liu chaotic system," *2018 International Conference on Advanced Science and Engineering (ICOASE)*, 2018, pp. 274-279, doi: 10.1109/ICOASE.2018.8548864.

[3] Z. N. Al-Kateeb and M. Jader, "Encryption and hiding text using DNA coding and hyperchaotic system," *Indonesian Journal of Electrical Engineering and Computer Science (IJEECS)*, vol. 19, no. 2, pp. 766-774, Aug. 2020, doi: 10.11591/ijeecs.v19.i2.pp766-774.

[4] H. A. Abdulkadhim, J. N. Shehab, and A. N. Albu-rghaif, "Audio security based on LSB steganography and 4-D lü system," *2018 Third Scientific Conference of Electrical Engineering (SCEE)*, 2018, pp. 203-208, doi: 10.1109/SCEE.2018.8684213.

[5] O. F. Abdel Wahab, A. I. Hussein, H. F. A. Hamed, H. M. Kelash, A. A. M. Khalaf, and H. M. Ali, "Hiding data in images using steganography techniques with compression algorithms," *TELKOMNIKA (Telecommunication Computing Electronics and Control)*, vol. 17, no. 3, pp. 1168-1175, Jun. 2019, doi: 10.12928/TELKOMNIKA.v17i3.12230.

[6] R. Divya, R. Sangeetha, and A. B. Jane Juliana, "Robust audio steganography enhanced with spy analysis for unassailable data transmission," *International Journal of Engineering Science and Computing*, vol. 9, no. 3, pp. 20982-20985, 2019.

[7] S. Pramanik, R. P. Singh, and R. Ghosh, "A new encrypted method in image steganography," *Indonesian Journal of Electrical Engineering and Computer Science (IJEECS)*, vol. 14, no. 3, Jun. 2019, pp. 1412-1419 doi: 10.11591/ijeecs.v13.i3.pp1412-1419.

[8] A. H. Ali, L. E. George, A. A. Zaidan, and M. R. Mokhtar, "High capacity, transparent and secure audio steganography model based on fractal coding and chaotic map in temporal domain," *Multimedia Tools and Applications*, vol. 77, pp. 31487-31516, 2018, doi: 10.1007/s11042-018-6213-0.

[9] S. Bhalshankar and A. K. Gulve, "Audio steganography: LSB technique using a pyramid structure and range of bytes," *International Journal of Advanced Computer Research (IJACR)*, vol. 5, no. 20, pp. 233-248, Sep. 2015, *arXiv:1509.02630*.

[10] F. Alisabir, "Hiding encrypted data in audio wave file," *International Journal of Computer Applications*, vol. 91, no. 4, Apr. 2014, doi: 10.5120/15867-4809.

[11] R. Choudhury and S. K. Bandyopadhyay, "LSB based audio steganography using pattern matching," *Journal of Multidisciplinary Engineering Science and Technology (JMEST)*, vol. 2, no. 11, Nov. 2015.

[12] S. Lahiri, "Audio steganography using echo hiding in wavelet domain with pseudorandom sequence," *International Journal of Computer Applications*, vol. 140, no. 2, Apr. 2016, doi: 10.5120/ijca2016909223.

[13] W. A. Shah, D. Shehzad, A. I. Umar, N. Ul Amin, J. Hussain, and A. Qadir, "Audio steganography based on Lsb Msb difference and FMC," *International Journal of Computer Science and Information Security (IJCSIS)*, vol. 15, no. 6, Jun. 2017.

[14] B. G. Banik and S. K. Bandyopadhyay, "Blind key based attack resistant audio steganography using cocktail party effect," *Security and Communication Networks*, vol. 2018, 2018, Art. no. 1781384, doi: 10.1155/2018/1781384.

[15] G. S. N. Kumar, S. N. Bhavanam, and V. Midasala, "Image hiding in a video-based on DWT & LSB algorithm," *Elseiver Science and Technology*, 2014.

[16] A. Jawed and A. Das, "Security enhancement in audio steganography by RSA algorithm," *International Journal of Electronics and Communication Technology (IJECT)*, vol. 6, no. 1, Mar. 2015.

[17] S. Acharya, P. Srimany, S. Kundu, and J. Dastidar, "Data hiding in video using triangularization LSB technique," *International Journal of Advanced Trends in Computer Science and Engineering*, vol. 4, no. 3, 2015, *arXiv:1507.05242*.

[18] S. A. Alhaj, A. M. Shaheen, and T. M. Al-Kharoubi, "Multi-layers video steganography: A novel technique for image hiding," *Society for Science and Education United Kingdom*, vol. 4, no. 6, 2016, doi: 10.14738/tnc.46.2529.

[19] H. N. Shashidhara and B. A. Usha, "Video steganography using zero order hold method for secured data transmission," *International Journal of Computer Applications*, vol. 176, no. 5, 2017, doi: 10.5120/ijca2017915587.

[20] M. M. S. Rani, S. Lakshmanan, and G. Deepalakshmi, "Video steganography using mid-point circle algorithm and spatial domain technique," *International Journal of Engineering and Techniques*, vol. 4, no. 1, 2018.

[21] S. Balu, C. N. K. Babu, and K. Amudha, "Secure and efficient data transmission by video steganography in medical imaging system," *Cluster Computing*, vol. 22, pp. 4057-4063, 2019, doi: 10.1007/s10586-018-2639-4.

[22] K. Niu, J. Li, X. Yang, S. Zhang, and B. Wang, "Hybrid adaptive video steganography scheme under game model," *in IEEE access*, 2019, doi: 10.1109/ACCESS.2019.2902464.

[23] J. N. Shehab, H. A. Abdulkadhim, and T. F. H. Al-Tameemi, "Robust large image steganography using LSB algorithm and 5D hyper-chaotic system," *Bulletin of Electrical Engineering and Informatics (BEEI)*, vol. 10, no. 2, pp. 689-698, doi: 10.11591/eei.v10i2.2747.

[24] S. Zhang, Y. C. Zeng, and Z. J. Li, "A novel four-dimensional no-equilibrium hyper-chaotic system with grid multiwing hyper-chaotic hidden attractors," *Journal of Computational and Nonlinear Dynamics*, vol. 13, no. 9, 2018, doi: 10.1115/1.4039980.

[25] Y. Huang, "A novel method for constructing grid multi-wing butterfly chaotic attractors via nonlinear coupling control," *Journal of Electrical and Computer Engineering*, vol. 2016, Art. no. 9143989, 2016, doi: 10.1155/2016/9143989.

[26] D. Arraziqi and E. S. Haq, "Optimization of video steganography with additional compression and encryption," *TELKOMNIKA (Telecommunication Computing, Electronics and Control)*, vol. 17, no. 3, pp. 1417-1424, 2019, doi: 10.12928/telkomnika.v17i3.9513.

[27] M. Fuad and F. Ernawan, "Video steganography based on DCT psychovisual and object motion," *Bulletin of Electrical Engineering and Informatics (BEEI)*, vol. 9, no. 3, pp. 1015-1023, 2020, doi: 10.11591/eei.v9i3.1859.

[28] Z. N. Al-Kateeb and S. J. Mohammed, "Encrypting an audio file based on integer wavelet transform and hand geometry," *TELKOMNIKA (Telecommunication Computing, Electronics and Control)*, vol. 18, no. 4, pp. 2012-2017, 2020, doi: 10.12928/telkomnika.v18i4.14216.

[29] L. Novamizanti, G. Budiman, and E. N. F. Astuti, "Robust audio watermarking based on transform domain and SVD with compressive sampling framework," *TELKOMNIKA (Telecommunication Computing, Electronics and Control)*, vol. 18, no. 2, pp. 1079-1088, 2020, doi: 10.12928/telkomnika.v18i2.14773.

[30] Y. N. Prajapati and M. K. Srivastava, "Novel algorithms for protective digital privacy," *International Journal of Robotics and Automation (IJRA)*, vol. 8, no. 3, pp. 184-188, doi: 10.11591/ijra.v8i3.pp184-188.

[31] C. A. Sari, G. Ardiansyah, E. H. Rachmawanto, and D. R. I. M. Setiadi, "An improved security and message capacity using AES and Huffman coding on image steganography," *TELKOMNIKA (Telecommunication Computing, Electronics and Control)*, vol. 17, no. 5, pp. 2400-2409, 2019, doi: 10.12928/TELKOMNIKA.v17i5.9570.