Journal of Information Hiding and Multimedia Signal Processing ©2018 ISSN 2073-4212
Ubiquitous International Volume **9**, Number **4**, July **2018**

Three Orders Mixture Algorithm of Audio Steganography Combining Cryptography

Mun Chun Lee and Chee Yong Lau

Faculty of Computing, Engineering and Technology
Asia Pacific University
Kuala Lumpur, Malaysia
lee_munchun@hotmail.com, dr.laucheeyong@apu.edu.my

Received September, 2017; revised February, 2018

Abstract. *In this paper, an enhanced audio steganography method 'Three Orders Mixture Algorithm' is presented which combines the techniques of steganography and cryptography. The objective of this paper is to design and implement a system which can perform the audio steganography process by embedding a series of text messages which is composed by alphabets, space and full stop symbol into an audio file without distorting the audio quality. Hence, enabling the secret communication between sender and receiver when the audio file is being transferred. The method combines the algorithms such as Least-Significant Bit (LSB), Dynamic Cipher Text and Rivest-Shamir-Adleman (RSA), and rearranges them as one algorithm hence creating a high complexity of steganography encryption module. At the same time, it also allows multiple diversity patterns of data encryption and decryption due to the combination of multiple algorithms. Besides, the proposed system also provides audio recording, Email, SMS features which can further improve the security level. In short, this method presents a high transparency and high robustness of audio steganography process.*
Keywords: Audio steganography, Cryptography, Mixed algorithms

1. **Introduction.** Steganography is a practice of hiding secret message/information in aspects of video, audio, text, and image from any forms of interception that may leaked and caused unwanted circumstances especially when it comes to private and confidential information [1]. Steganography is similar to cryptography at where information is hidden in such way that are not presented in the actual and exact original message, it is not understandable by others except the intended sender and receiver. However, an advantage of steganography over cryptography is that cryptography is solely protecting particular message, it is still noticeable because it is presented directly as a visible form as texts and words which could arouse interest easily [2]. On the other hand, steganography practices minimizing the risk of detection as it does not draw attention as an object that should be awared of. For audio steganography, it would be used in a more specific way such as communications in military or any classified information.

There are 3 important factors for audio steganography to ensure it is implementable [3].

- Capacity- Refer to the amount of secret message that can be embedded into the original message.
- Transparency- The evaluation of how well a secret message are embedded into the original message.

- Robustness- Refer as measure of the ability of secret message to withstand against attacks.

Thus, the evaluation of an enhanced algorithm must satisfy from these 3 aspects.

Steganography can be implemented in any digital medium such as text, video, image, and audio. The reason why audio has been chosen in this project is because of:

1. Capacity- Audio file has higher capacity compared to text or image [4] due to its number of bits to be processed. Although video also has higher capacity than audio, however video in certain extent it become unnecessary as audio is sufficient to do the work.
2. Robustness- Audio shows the highest robustness when comes to steganography due to its difficulty to differentiate [4] by just listening whether it contains secret message. As for text, image or video, a trained eye or machine could detect the unusual matter.

Although audio steganography is preferable, however at current stage of technology, a machine can still detect a secret message that is hidden in an audio. Therefore, improvement and enhancement are needed as to improve the Signal-to-Noise Ratio (SNR) as well as Bit Error Rate (BER). Although these 2 factors often causing the trade off to each other, however it still could be optimized and enhanced [5]. Hence, this paper introduces a new method 'Three Orders Mixture Algorithms of Steganography and Cryptography'. 'Three Orders Mixture' involves combination of 3 different algorithms and the order of the combination can be selected thus having a total of 6 combinations. The 3 algorithms consist of 1 steganography which is 'Least Significant Bit (LSB)' while other 2 is cryptography which are 'Dynamic Cipher Text' and 'Rivest-Shamir-Adleman (RSA)'.

Table 1. Mixed Orders Combinations

combinations	**1st**	**2nd**	**3rd**	**4th**	**5th**	**6th**
LSB	1	1	2	3	2	3
Dynamic Cipher Text	2	3	1	1	3	2
RSA	3	2	3	2	1	1
Result (in orders)	1-2-3	1-3-2	2-1-3	3-1-2	2-3-1	3-2-1

The 'Mixed Algorithms' could provide higher complexity level of data security by creating various diversity of encryption and decryption patterns thus enhancing the robustness to a whole new level.

2. **Related Work.** Several techniques were highlighted in the previous studies regarding the steganography and cryptography techniques, as well as the algorithms combination enhancements.

Jayaram, Ranganatha & Anupama [6] had applied Least Significant Bit (LSB) method for audio steganography. The concept of this algorithm is to substitute the LSB in each sample, bit by bit with the secret message bits. By using the reverse algorithm and extract the LSB the secret message could be retrieved. The advantages of LSB is it does not produce much difference compare to original audio file, could be embedded with large amount secret messages and easy to implement. However, it is also prone to detection. Intruder could extract the secret message using same algorithm easily.

Asad, Gilani & Khalid [3] proposed an improved method of audio steganography based on LSB known as 'Three Layered Model'. It consists of 3 independent layers of security. The secret message was still remained hidden even though some info were extracted at layer 1 and 2. It uses "Huffman Coding [7]" Advanced encryption standard (AES) [8], and the 6^{th}, 7^{th} & 8^{th} LSB method which is depends on the value of first three most significant

bit (MSB), and there decide which LSB is being substituted by the bit of secret message. Three layered model offered more transparency and robustness, although there are more minimum samples required 5 times larger [3] to perform the three-layered model.

Divya & Ram Mohan Reddy [9] proposed a multiple LSB steganography with combination of Richet-Shamir-Adleman (RSA) cryptography. Multiple LSB steganography means instead of the 8th bit, other bit were substituted with the bit of secret message except for MSB. MSB decides the bit which is being substituted. On the other hand, RSA is one of the type of cryptography. The RSA algorithm is fixed which involved arithmetic calculation with 2 prime numbers to generate RSA key pairs (Public keys and private keys). The product of 2 very large prime number (termed as p & q) forms a composite number whereas it is difficult to detect the private key by intruders. In overall, the combination of RSA cryptography method has greatly enhanced the robustness of secret message security which is embedded into the LSB while it also has the result of high Peak Signal-to-Noise Ratio (PNSR) and low Mean Squared Error (MSE).

Abdulzahra, Ahmad & Norliza [10] has also proposed LSB steganography with combining a cryptography method which improves the security level. The bits of secret message that embedded into the last bit of samples were transformed to a type of alphabet cipher text according to a dynamic table. It is dynamic because the alphabet represented for each number of words are different. First, alphabet 'a' to 'z' and 'space' are being assigned each of them a code range from '01' to '27'. The series of alphabet keeps shuffling to the full length of secret message. By applying this proposed algorithm, the Peak signal-to-noise ratio (PSNR) has increased 1 2% while mean squared error (MSE) has reduced up to 2 3% compared to simple LSB method. Although the overall security has improved but there is some gap yet to be done. The secret message only allowing alphabets and space, numbers (0-9) should be incorporated.

Taneja & Gupta [11] have introduced an implementation of dual security through Digital Signature Algorithm (DSA) and audio steganography. DSA is a type of public key cryptography. It is very similar to RSA which generates public key and private key in the end. DSA uses a technique called Hashing function to produce message digest. A message digest is some sequences formed by alphanumeric & symbols which replaces the original message. There are 2 phases in DSA. Phase 1 generates global public key while phase 2 generates private key. There are multiple categories could be found in hash function. This paper introduces the implementation of hash function SHA1, SHA256 and SHA256. The secret messages are only being embedded into the audio data after the process of DSA. Thus, this has greatly improved the robustness of the system. However, due to the high complexity of the algorithm of DSA, the verification process is fairly slow for the receiver not mentioning if the message size is huge.

Gandhi & Garg [12] has proposed a modified LSB audio steganography. First there will be two file 'audio file' and 'text file' where the 'text file' contains the secret message. The secret message will convert to ASCII representative and then convert again into binary equivalent. User will be prompt to enter a password. The password is used to determine whether or not the particular samples will be embedded with the secret message bits. The entered password will undergo a permutation function and out of all the outcome only one will selected randomly, and saved it in the audio file for verification purpose at the receiver side. By convert the alphanumeric password into sequence of bits then mapping with the data chunk in the audio file if value is '1' the LSB of the sample will be replaced by the message bit while for '0' there will be no embedding process and skip the current sample. As a result, this algorithm has improved the simple LSB method by introducing an external layer of password which modify the way on how message bit are embedding into the audio samples. However, it has drawback which the password saved in the audio

file that used to do mapping could be easily detected, intruder could have change their direction towards the breakable password unless the password is being protected with some extra mechanism.

3. Investigation on Algorithms.

3.1. **Least Significant Bit (LSB).** The concept of LSB is to substitute the last bit which is the 8^{th} bit in a byte information with the bit of the secret message [13]. As audio .WAV file has the specification of 2 bytes per sample, LSB is substituted twice per sample as example below.

Example: 2 original audio bytes: 01001101 00101110

Example: secret message = 'a' (**01**100001 in binary)

Thus, by substituting bit by bit of the secret message into the LSB of original audio bytes, the secret message is embedded.

Final result = 01001100 00101111

Total of 4 samples are required to encrypt an alphabet 'a'. For the receiver side, it just requires to extract the LSB for every byte so that the secret message can be formed.

Justification: This algorithm serves as a strong fundamental method for steganography, it has advantages of providing wider scale of transparency due to the LSB contains the less information, in other words it would not alter much of the originality of the audio file thus reduce the risk of being detected.

3.2. **Dynamic Cipher Text.** Cipher Text is a series of scrambled and meaningless text that only sender and receiver could understand [1]. A cipher is a type of cryptography method where it is categorized as private key algorithm, the sender and receiver must be in contact in order to know the specific key (rules) to encrypt and decrypt the text. In this case, alphabet 'a-z' in small letters are assigned each of them a number from 1-26, symbols like 'space', 'fullstop' also were assigned number starting from 27-28 [9].

If Dynamic Cipher Text is at 1^{st} order:

TABLE 2. 1^{st} order cipher text

a	1	f	6	k	11	p	16	u	21	z	26
b	2	g	7	l	12	q	17	v	22	space	27
c	3	h	8	m	13	r	18	w	23	.	28
d	4	i	9	n	14	s	19	x	24		
e	5	j	10	o	15	t	20	y	25		

If Dynamic Cipher Text is at 2^{nd} order:

TABLE 3. 2^{nd} order cipher text

b	1	g	6	l	11	q	16	v	21	space	26
c	2	h	7	m	12	r	17	w	22	.	27
d	3	i	8	n	13	s	18	x	23	a	28
e	4	j	9	o	14	t	19	y	24		
f	5	k	10	p	15	u	20	z	25		

The difference between the 3 tables is that if 2^{nd} order dynamic cipher is selected, the overall sequence is shifted left by 1 place in which alphabet 'a' go after symbol '.' while for third order, the sequence is shifted right by 1 place where symbol '.' go before alphabet 'a'. The first order is the standard sequence with no changes.

The number assigned is totally different for every next character in message, for example a secret message 'aa', the assigned numbers are '1 and 28' instead of '1 and 1' due to the sequence has been rotated for the second 'a'.

If Dynamic Cipher Text is at 3^{rd} order:

Table 4. 3^{rd} order cipher text

.	1	e	6	j	11	o	16	t	21	y	26
a	2	f	7	k	12	p	17	u	22	z	27
b	3	g	8	l	13	q	18	v	23	space	28
c	4	h	9	m	14	r	19	w	24		
d	5	i	10	n	15	s	20	x	25		

Justification: This algorithm could improve the robustness compared to the LSB steganography. Due to the dynamic property, the message is difficult to be decrypted by the intruder. Besides, there are 6 different combinations in the mixed orders hence this dynamic cipher algorithm could create multiple patterns by using the same concept.

3.3. **Rivest-Shamir-Adleman (RSA).** RSA is also a cryptography but it is a public key instead of private key. It does not require sender and receiver to be in contact in order to know the key for encryption and decryption. However, this is not the focus due to it is combined with LSB steganography which sender and receiver needs to know in the end. RSA involved the operation of factorization of large prime numbers. The operations are as follows [14].

First, 2 prime numbers are selected and called them as 'p' and 'q'.

1) Compute n = p*q

2) Compute z = (p-1) * (q-1)

3) Then, choose a prime number 'e' in such that $1 < e < z$

4) Compute the value of 'd' where (d*e) modulo z = 1

Thus, the values for n, d and e are computed.

For public key is (e,n), for private key is (d,n).

Table 5. Dynamic Cipher Text

1	2	3	4	5	6	7	8	9	10	11	12	13	14
a	b	c	d	e	f	g	h	i	j	k	l	m	n
b	c	d	e	f	g	h	i	j	k	l	m	n	o
c	d	e	f	g	h	i	j	k	l	m	n	o	p
d	e	f	g	h	i	j	k	l	m	n	o	p	q
e	f	g	h	i	j	k	l	m	n	o	p	q	r
f	g	h	i	j	k	l	m	n	o	p	q	r	s
.	.	.	.	.	.	.	.	.	.	.	.	.	.
15	16	17	18	19	20	21	22	23	24	25	26	27	28
o	p	q	r	s	t	u	v	w	x	y	z	_	.
p	q	r	s	t	u	v	w	x	y	z	_	.	a
q	r	s	t	u	v	w	x	y	z	_	.	a	b
r	s	t	u	v	w	x	y	z	_	.	a	b	c
s	t	u	v	w	x	y	z	_	.	a	b	c	d
t	u	v	w	x	y	z	_	.	a	b	c	d	e
.	.	.	.	.	.	.	.	.	.	.	.	.	.

By knowing the keys, if secret message is 'm'
Encryption: c=m^e modulo n, 'c' is the encrypted message.
Decryption: c^d modulo n = m, 'm' is the original message.
Justification: This algorithm often applies prime numbers p and q which are in 10 power of 100. If intruder intended to decode the information, decomposition of large number with factorization of the prime numbers would be required. On the other hand, relating to the 3 orders mixture algorithms that was proposed earlier, it create an advantage where 6 different cases of p and q can be selected hence non-linearity of the algorithms can be produced.

- If RSA is at 1st order: p=3, q=11;
- If RSA is at 2nd order: p=5, q=7;
- If RSA is at 3rd order: p=3, q=13;

Different encryption could be generated by using different order of RSA algorithm.

4. **Proposed Methodology.** The entire system is categorized into 2 sections: sender function and receiver function. Both sections are combined to achieve data protection by applying encryption which is on sender side, while decryption is on receiver side.

4.1. **Encrypting.** There are 2 elements which is crucial to perform the encryption which is an audio source file and secret message as shown in Fig. 1. At current stage, the audio file has to be in WAV format and the content audio can be in any form such as music or any sound. The system also provides voice recording to create audio carrier. After that, the secret message that are keyed in by user are then being processed together with the audio source file with 6 types of encryption orders depends on user selection. Every type of encryption orders are using different parameters from each other. For final product, a stego audio file is produced. A stego audio file has the same property almost like the original audio source file but with secret message embedded inside. When playing the stego audio file, it is still the same music or sound thus it is hard for human to detect whether the file contains hidden message. Even though a stego audio file is marked as suspicious, but it is still difficult to be decoded due to high robustness of multiple layers of encryption orders. The next focus point is on how receiver know what is the encryption orders which is chosen by sender. Hence, the system also let sender to notify the types of encryption orders using Email or SMS features.

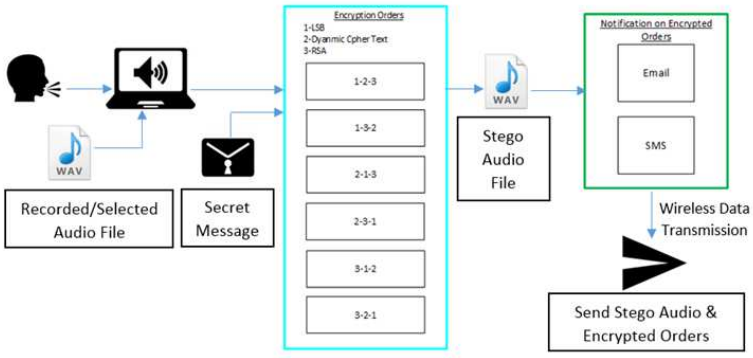

FIGURE 1. Data encryption system (sender side)

4.2. **Decrypting.** For the receiver side, it is a reverse process of sender system as shown in Fig. 2. The 2 elements needed in order to perform decryption is the received stego audio file and the information given on the encryption orders. Hence, by inserting the stego audio file into the system and select the correct encryption orders, it could extract and display the secret message which is embedded inside the audio file.

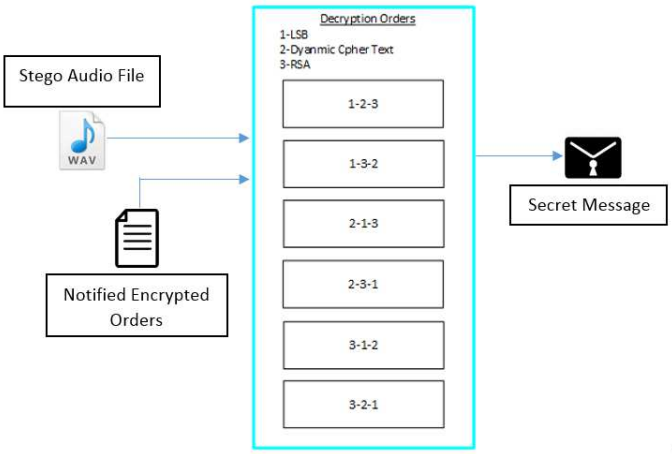

FIGURE 2. Data decryption (receiver side)

4.3. **Working principle of algorithms combinations.**

1. Get the secret message entered by user.
2. Maps the secret message with Dynamic Cipher Text to obtain the decimal value (1-28).
3. The value obtained from Dynamic Cipher Text is being substituted into RSA equation as 'm'.
4. Perform the RSA operation and obtain the encrypted message which is referred as 'c' (ASCII value).
5. The value is then converted into binary form, the binary bits are then being substituted bit by bit into the LSB of audio samples.

For decryption, it is the reverse process where LSB is being extracted first, then decrypted by RSA and lastly Dynamic Cipher Text to retrieve the message. At different orders of algorithms selected by user, the variable used for Dynamic Cipher Text and RSA would be different as stated in section III.

4.4. **GUI Interface.** Based on Fig. 3, the GUI design is categorized into 2 sections where the left section is the for encryption namely as Hide Message while the right is for decryption namely as 'Extract Message'.

5. Experimental Results and Discussions.

5.1. **ABX Listening Test.** ABX listening test is a method to compare 2 choices of audio (original and stego) to determine the detectable differences between them [15]. Three options of audios are presented to listeners where option A contains original audio, option B contains stego audio while option X could be neither A or B which is drawn at random. Listeners are required to make decision whether X is match to A or B, for 10 times. The system has been tested by 30 peoples from teenagers to middle adults, range from age 13-65 consist of male and female to have a diversity in hearing ability. The

FIGURE 3. Complete GUI interface

audio used are original 1 second beep sound and stego with maximum alphabets allowed to embed inside which is 3750 random characters.

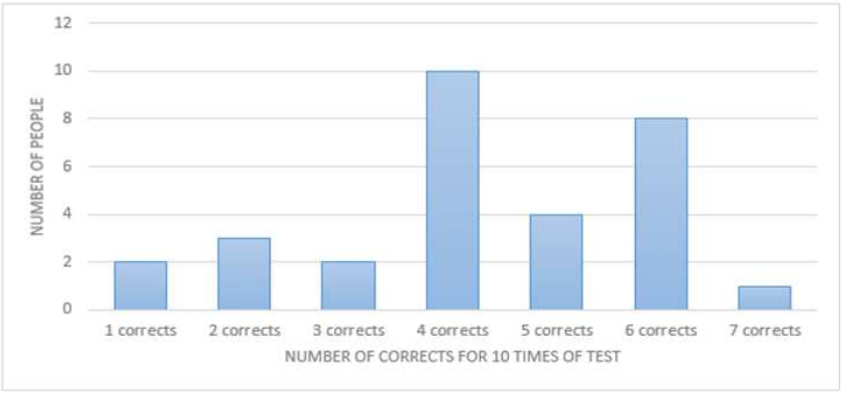

FIGURE 4. ABX listening test result

Based on Fig. 4, 5 corrects and below are consider as obviously unable to differentiate original and stego audio, thus there are total 21 peoples falls in this category which will not be discussed. On the other hand, there are 8 peoples got '6 corrects' and 1 people got '7 corrects'. A questionnaire also given to each listener, all of them give feedback in such that they could not differentiate between original and stego audio including the one who got '7 corrects'. Thus, due to there is no clear evidence on how people can differentiate a stego audio from its original audio, a conclusion can be made such that 'Three Orders Mixture Algorithm' audio steganography system has no caused any quality distortion of the audio by hearing ability of human.

5.2. **Trending Analysis.** This is to determine how age and gender would affect the ability of testees to differentiate original and stego audio.

Hence, the average corrects are calculated among the same population of gender and age group to acquire the norm value. According to the TABLE V, the norm values as shown doesnt have much differences. The value highlighted in bold represents the total average norm value that involved all age groups in male side as well as female side. The differences appeared to be only 0.07. Likewise, a conclusion can be made in such that gender and ages doesn't affect the quality of listening test results, the outcome from the listening test and questionnaire are truthful.

TABLE 6. Trending Analysis Result

Male			Female		
Age group	**Amount of testee**	**Average corrects**	**Age group**	**Amount of testee**	**Average corrects**
13-18	4	3.75	13-18	4	4.25
19-35	5	4.8	19-35	5	4.4
36-55	4	5.0	36-55	3	4.33
56-65	2	3.5	56-65	3	4.33
Total Average Value		**4.40**	Total Average Value		**4.33**

5.3. **Spectral Analysis and PSNR Result.** The spectral analysis is to determine how would the length of message causing the differences in time-domain and frequency-domain of audio.

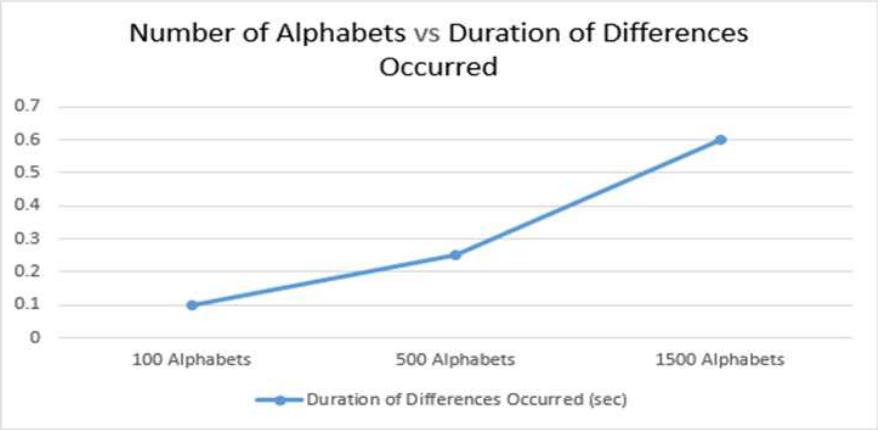

FIGURE 5. Results comparison in time domain

Based on Fig. 5, it shows that a directly proportional relationship that when number of alphabets increased, the duration of differences occurred in time domain is longer. The graph is direct proportional due to at 500 alphabets the duration is 0.25 sec, hence we can know that from 100 alphabets to 500 alphabets there is an increment of 0.15 sec for every 400 alphabets. Thus, from 500 to 1500 alphabets there is difference of 1000 alphabets and from there we can get 0.625 sec which is approximate to 0.60 sec.

Based on Fig. 6, at first the amplitude difference has increased from 1 to 2.8 from 100 alphabets to 500 alphabets. However, after passing the 500 alphabets, there is no sign of amplitude differences increasing until 1500 alphabets which the amplitude maintained at 2.8. After taking several considerations, the amplitude has no changes even though number of alphabets has increased is due to the $2.8\text{x}10^{-3}$ is already reached the maximum amplitude differences that can be obtained in the proposed audio steganography system. A justification for this is that the proposed system is using LSB method where it only changes the least significant bit value per sample in audio which the data value represent in LSB is very low (which is equal to 1 in decimal), thus due to the low data value it will has a limit of frequency deviation that could be modified unlike the MSB which represent higher data value (149 in decimal). Hence, the maximum amplitude difference in terms of frequency is $2.8\text{x}10^{-3}$.

Based on Fig. 7, the value of PSNR is decreased as the number of alphabets increased. The highest PSNR is at 109dB which only has 100 alphabets while the lowest PSNR is

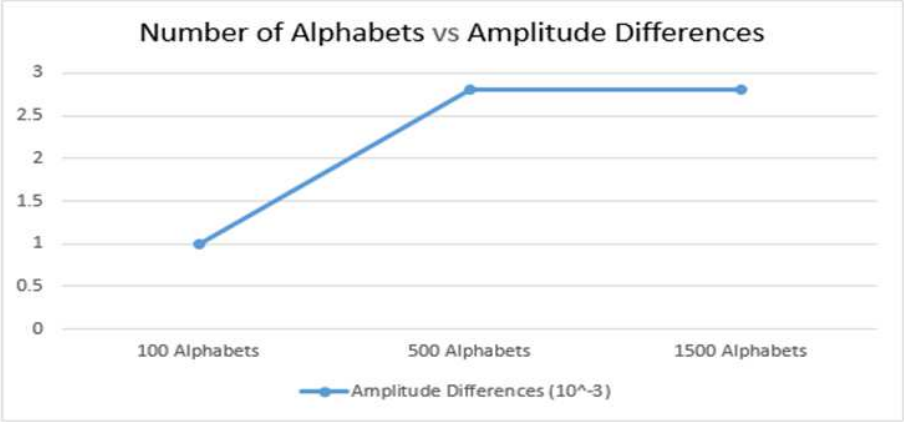

FIGURE 6. Results comparison in frequency domain

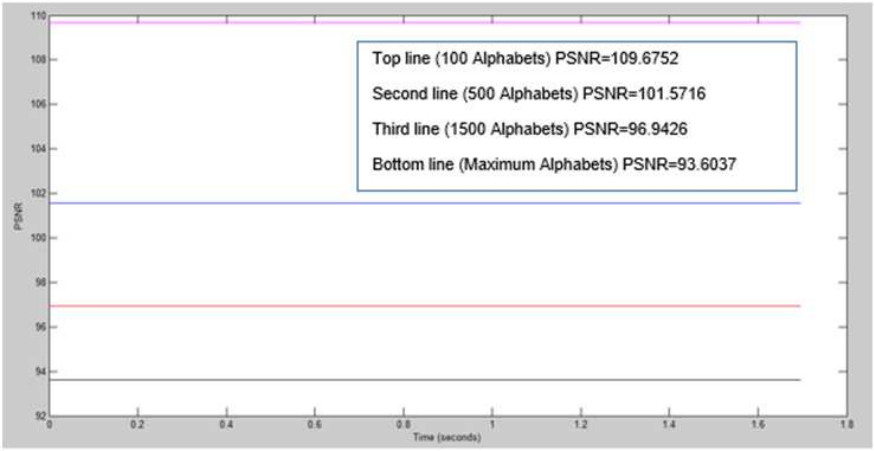

FIGURE 7. PSNR comparison between 100, 500, 1500 alphabets

93dB for maximum alphabets (3200 alphabets, 52 kilobytes). The differences between highest and lowest PSNR is approximately 16 db. At first the PSNR has dropped rapidly from 109 dB to 101 dB and after that has slowly decreased where the gap between each line is become smaller. This is because of the limit of quality that LSB could altered and the minimum PSNR that could be obtained is 93dB where it is consider as very high fidelity audio, as stated in [16] a signal-to-noise ratio with 20dB and above are considered as favourable audio quality.

Based on the outcome from Fig. 5, 6 and 7, a conclusion can be made in such that the time-domain and frequency-domain differences occurred in stego audio is very small and could not detected with human ear even with maximum characters are embedded. Besides, a high PSNR stego audio also ensure a high audio quality where distortions are not possible to be detected.

6. **Conlusion and Future Work.** In this paper, 'Three Orders Mixture Algorithms' audio steganography implemented by combining LSB, Dynamic Cipher Text and RSA these 3 methods. Due to their flexibility and ability to design a multiple layers and diverse patterns of encryption and decryption mixed algorithm. The stego audio produced by this algorithm has high fidelity of audio quality which stayed at 90dB and above even with maximum characters embedded in the audio.

The proposed system can be further enhanced such as expand the forms of secret message like digits and symbols. It also can develop some new modus of secret message such as embed an image or another audio into the audio instead of just embedding text as the secret message as they could further enhance the effectiveness of steganography.

REFERENCES

[1] R. Patel, Cryptography, *Engineering & Technology Reference*, vol. 1, no. 1, 2012.

[2] J. Vimal, Literature review on audio steganographic techniques, *International Journal of Engineering Trends and Technology*, vol. 11, no. 5, pp. 246-248, 2014.

[3] M. Asad, J. Gilani and A. Khalid, Three layered model for audio steganography, *International Conference on Emerging Technologies*, 2012.

[4] F. Djebbar, B. Ayad, K. Meraim and H. Hamam, Comparative study of digital audio steganography techniques, *EURASIP Journal on Audio, Speech, and Music Processing*, vol. 2012, no. 1, 2012.

[5] M. Zhao, J.S. Pan and S.T. Chen, Entropy-based audio watermarking via the point of view on the compact particle swarm optimization, *Journal of Internet Technology*, vol. 16, no. 3, pp. 485-495, 2015

[6] Jayaram, Ranganatha and Anupama, Information hiding using audio steganography - a survey, *The International journal of Multimedia & Its Applications*, vol. 3, no. 3, pp. 86-96, 2011.

[7] A. Jas, J. Ghosh-Dastidar, M. Ng and N. A. Touba, An efficient test vector compression scheme using selective huffman coding, *IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems*, vol. 22, no. 6, pp. 797-806, 2003.

[8] A. M. Sagheer, S. S. Al-Rawi and O. A. Dawood, Proposing of developed advance encryption standard, *Developments in E-systems Engineering (DeSE)*, pp. 197-202, 2011.

[9] S. Divya and M. Ram Mohan Reddy, Hiding text in audio using multiple LSB steganography and provide security using cryptography, *International Journal of Scientific & Technology Research*, vol. 1, no. 6, pp. 68-70, 2012.

[10] H. Abdulzhara Atee, R. Ahmad and N. Mohd Noor, Cryptography and image steganography using dynamic encryption on LSB and color image based data hiding, *Middle-East Journal of Scientific Research*, vol. 23, no. 7, pp. 1450-1460, 2015.

[11] N. Taneja and P. Gupta, Dual security: proposed architecture, *International Journal of Science, Technology & Management*, vol. 4, no. 2, pp. 154-157, 2015.

[12] K. Gandhi and G. Garg, Modified LSB audio steganography approach, *International Journal of Emerging Technology and Advanced Engineering*, vol. 3, no. 6, pp. 158-161, 2017.

[13] M. Sutaone and M. Khandare, Image based steganography using LSB insertion, *IET Conference on Wireless, Mobile and Multimedia Networks*, pp. 146-151, 2008.

[14] J. Gordon, Strong RSA keys, *Electronics Letters*, vol. 20, no. 12, pp. 514-516, 1984.

[15] M. Zamani, A. Bt Abdul Manaf and S. M. Abdullah, An overview on audio steganography techniques, *International Journal of Digital Content Technology and its Applications(JDCTA)*, vol. 6, no. 13, pp. 107-122, 2012.

[16] M. Nutzinger, Real-time attacks on audio steganography, *Journal of Information Hiding and Multimedia Signal Processing*, vol. 3, no. 1, pp. 47-65, 2012.