

Enhancing The Data Security by using Audio Steganography with Taylor Series Cryptosystem

Muharrem Tuncay GENÇOĞLU^{1*}, Mehmet VURAL²

¹ Vocational School of Technical Sciences, Fırat University, Elazığ, Türkiye

² Fırat University, Elazığ, Türkiye

*¹ mt.gencoglu@firat.edu.tr ² mvural002@gmail.com

(Geliş/Received: 10/12/2020;

Kabul/Accepted: 14/01/2021)

Abstract: Especially in recent years, the security of information and computer systems appears to be a very important issue. Because the heavily used communication network has made life easier as well as accompany serious security problems. To solve these problems, cryptography and steganography have been widely used. To present a more secure model for audios, a simple and secure stego-crypto method is presented. In this work, the hidden data is encrypted by the proposed Taylor series based encryption method and the encrypted data are hidden audio signals by applying the least significant bit (LSB) method. A real-world application is implemented in the proposed model. According to the results, the used encryption model is more efficient than AES. The results and findings demonstrated that this model can be used in a communication security system.

Key words: Cryptography, Audio Steganography, Data Steganography, Text Steganography

Taylor Serisi Kriptosistem ile Ses Steganografisi Kullanılarak Veri Güvenliğinin Arttırılması

Öz: Özellikle son yıllarda bilgi ve bilgisayar sistemlerinin güvenliği oldukça önemli bir konu olarak karşımıza çıkmaktadır. Çünkü yoğun bir şekilde kullanılan iletişim ağı, hayatı kolaylaştırdığı gibi ciddi güvenlik sorunlarına da beraberinde getirmektedir. Bu sorunların çözümü için kriptografi ve steganografi yaygın olarak kullanılmıştır. Çalışmamızda Ses steganografisinde daha güvenli bir model oluşturmak için basit ve güvenli bir stego-kripto yöntemi sunulmuştur. Bu çalışmada, gizli veriler önerilen Taylor serisi tabanlı şifreleme yöntemi ile şifrelenmiş daha sonra şifrelenen veriler en az önemli bit (LSB) yöntemi uygulanarak ses sinyallerine gömülmüştür. Önerilen modelde gerçek bir uygulama yapılmış ve bu uygulamada kullanılan şifreleme modelinin AES'den daha verimli olduğu gözlemlenmiştir. Sonuçlar ve bulgular, bu modelin bir iletişim güvenlik sisteminde kullanılabilirliğini göstermiştir.

Anahtar kelimeler: Kriptografi, Ses Steganografisi, Veri Steganografisi, Metin Steganografisi.

1. Introduction

Security is considered as the most basic factor in any communication system. This issue poses an important threat, as failure to ensure the confidentiality of information will negatively affect individuals, communities and states. For this reason, new applications and new system protection mechanisms have emerged along with the developing technology to prevent data hiding and changing. In these applications, many encryption algorithms have been created and existing algorithms continue to be developed to further increase the security of the data, and even new algorithms are being created.

The main purpose of cryptographic protocols is to ensure the integrity and confidentiality of the data. While examining a protocol, just like algorithms, we are concerned with basic operating principles rather than what kind of device we will implement[1].

Data we want to be protected; It is sent after being rendered incomprehensible with the aid of a key and the specified encryption algorithm. However, the fact that encrypted data in this way can be cracked by crypto analysts over time indicates that encryption alone is not sufficient for secure communication. For this reason, encryption and information hiding methods have started to be used as hybrid with encryption algorithms. It has been shown that it is possible to provide secure communication, especially using Steganography[6,10,14,16,17].

Data hiding and data communication security is a very important issue. The purpose of hiding data is the third person noticing during communication. In cryptographic encryption, the third party is aware of the secret data being sent. However, when data communication is made between the two people using steganographic methods, the third person cannot realize that there is a hidden communication between them. Steganography is the art of

* Corresponding author: mt.gencoglu@firat.edu.tr. ORCID Number of authors: ¹ 0000-0002-8784-9634, ² 0000-0003-1768-5117

hiding information with other information. Encryption turns data into an incomprehensible format, making it difficult to access real data, but cannot ensure the privacy of communication. In that case, we can express the difference between steganography and cryptography as follows; While cryptography scrambles the data, steganography completely hides the data[3-7].

Steganography, which is very important in hiding information, has been frequently used in recent years to protect the data in digital media by embedding it in text, audio, video and image files. In some techniques, the hybrid model is used[2].

Steganography started to use many methods with the development of technology. With this development, many steganographic methods started to need different algorithms. A different algorithm and a different method are used in each steganographic method. Each steganographic method has a distinctive steganalysis method. Steganography is done by hiding data into text, sound, picture, video files[12-15,17-24]. Similarly, a text file can also be stored in an audio or video file[8-10]. Therefore, steganography is not an encryption method, but a complementary element to encryption[11].

1.1. Motivation and Contribution

In this study, encryption and data hiding techniques are used to ensure the security of communication. A Taylor series based encryption algorithm, previously developed by Gençoğlu, was used to demonstrate that mathematical functions can be used to increase the robustness of the algorithms used in encryption[17]. Then, sound steganography, one of the steganography techniques, was used to hide the presence of data encoded with the proposed algorithm.

1.2 Organization

In the second chapter of this study, brief information about the necessity of the proposed method was given. Then, information was given about the proposed algorithm technique and comparison was made. In the third chapter, the application steps of the proposed algorithm technique are shown. In the fourth chapter, experimental results are given. In the fifth chapter, the performance analysis of the proposed method was made. In the sixth chapter, the obtained results and suggestions were included.

2. Proposed Method

Initially, with an eight-character key, the message is encrypted, subject to several rules and using the Taylor series in the encryption algorithm. Then, the obtained data is sent to the most meaningless bit of the voice by hiding with a proprietary code that will receive the encrypted message. The encryption diagram is shown in Fig. 1 and the decryption diagram is shown in Fig. 2.

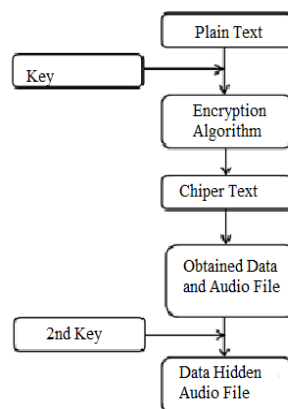


Fig. 1 The encryption diagram of the proposed model.

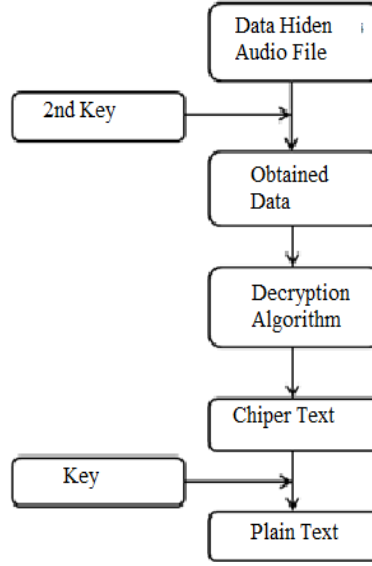


Fig. 2 The decryption diagram of the proposed model.

2.1. Encryption Algorithm

First of all in the encryption algorithm, after the message is encrypted using a set of rules with the key, the obtained data is subjected to hiding by sound steganography. The working principle of the encryption algorithm is as follows:

- The message to be encrypted is processed with the key in octal blocks.
- The key to be used must have eight characters.
- Taylor series is used in encryption, mod 256 is used in calculations.
- All of the key and the message are processed by converting them into Binary in octal blocks.
- Taylor series is used in the encryption algorithm for the Laplace transform to be used in the algorithm. The expanded Taylor series is taken with e^t .
- $f(x) = f(a) + \frac{f'(a)}{1!}(x-a) + \frac{f''(a)}{2!}(x-a)^2 + \dots + \frac{f^n(a)}{n!}(x-a)^n + \dots$

$$= \sum_{n=0}^{\infty} \frac{f^n(a)}{n!} (x-a)^n \text{ [16] and } f(t) \text{ is obtained;}$$

$$f(t) = \sum_{n=0}^{\infty} K_n \frac{t^{n+3}}{n!} .$$

From hence;

$$[f(t)](h) = T\left[\sum_{n=0}^{\infty} K_n \frac{t^{n+3}}{n!}\right](h)$$

$$= T\left[K_0 \frac{t^3}{0!} + K_1 \frac{t^4}{1!} + K_2 \frac{t^5}{2!} + K_3 \frac{t^6}{3!} + K_4 \frac{t^7}{4!} + K_5 \frac{t^8}{5!} + K_6 \frac{t^9}{6!} + K_7 \frac{t^{10}}{7!}\right](h)$$

$$\sum_{n=0}^{\infty} K_n (n+3)! \frac{h^{n+3}}{n!} \tag{2.1}$$

From here, the dividend and remainder values of the coefficients according to mod 256 are found.

Step 1.

After the 1st character of the key and 1st character of the message has been converted to binary;

- a) If the number of 0 in the 1st character of the key is more than or equal to the number of 1;
 - The last bit, the 1st character of the key, is taken first (a_1).
 - The first bit, the 1st character of the message, is taken to the end.
- b) If the number 0 in the 1st character of the key is less than the number 1;
 - The leading bit, the 1st character of the key, is taken to the end (a_1).
 - The last bit, the 1st character of the message, is taken first (m_1).
 - The transformed version (a_1) of the 1st character of the key with the transformed version of the 1st character of the message (m_1) by XOR the first character of the message is encrypted in step 1 (x_1).

Step 2.

After the 2nd character of the key is converted into binary;

- a) If the number of 0 in the 2nd character of the key is more than or equal to the number of 1;
 - The last bit, the 2nd character of the key, is taken first (a_2).
 - The first bit(x_1), the 1st character of the message, the encrypted value at the end of step 1, is taken to the end (m_2).
- b) If the number of 0 in the 2nd character of the key is less than the number of 1;
 - The leading bit, the 2nd character of the key, is taken to the end (a_2).
 - The last bit (x_1), the 1st character of the message, the encrypted value at the end of step 1, is taken first (m_2).
 - The transformed version (a_2) of the 2nd character of the key with the transformed version of the 2nd character of the message in step 2 (m_2) by XOR the first character of the message is encrypted in step 2 (x_2).

Step 3.

After the 3rd character of the key has been converted to binary;

a) If the number of 0 in the 3rd character of the key is more than or equal to the number of 1;

- The last bit, the 3rd character of the key, is taken first (a_3).
- The first bit of the encrypted value at the end of step 2(x_2), the 1st character of the message, is taken to the end (m_3).

b) If the number of 0 in the 3rd character of the key is less than the number of 1;

- The leading bit, the 3rd character of the key, is taken to the end (a_3).
- The last bit of the encrypted value at the end of step 2(x_2), the 1st character of the message, is taken to the top (m_3).
- The transformed version (a_3) of the 3rd character of the key with the transformed version of the message in step 3 (m_3) by XOR the first character of the message is encrypted in step 3 (x_3).

By doing similar operations in steps 4,5,6,7 and 8, x_4, x_5, x_6, x_7 and x_8 encrypted values are found.

- At the end of step 8, the encryption process is completed in the first character of the message. Other characters of the message are similarly encrypted, but before processing, each character is subjected to XOR processing by the encrypted format of the previous character. In this way, the message is encrypted in octal blocks.
- Encryption is completed by taking from previously random generated Tab. 1 the equivalent of the value obtained at the end of each step (first 4 numbers rows, last 4 numbers columns).

Table. 1 S-box List

	0000	0001	0010	0011	0100	0101	0110	0111	1000	1001	1010	1011	1100	1101	1110	1111
0000	1	181	120	169	38	245	76	242	230	39	72	78	47	33	239	249
0001	49	7	37	64	68	160	237	32	58	48	14	203	35	114	110	143
0010	119	23	6	12	220	109	44	61	215	202	159	45	29	250	157	235
0011	24	184	170	22	150	28	149	133	129	198	219	13	145	56	63	204
0100	212	97	201	5	15	177	234	122	50	0	113	102	253	106	36	168
0101	192	65	57	104	226	3	174	101	84	151	42	128	140	60	224	112
0110	207	53	46	95	131	243	87	118	175	164	69	55	178	247	79	126
0111	158	134	217	229	139	73	93	30	254	92	142	59	27	52	248	153
1000	240	121	189	196	138	165	130	228	11	144	34	147	25	194	137	100
1001	180	135	99	222	156	241	161	208	18	20	80	197	67	105	244	124
1010	221	74	211	167	85	115	183	251	111	51	16	108	200	233	205	66
1011	41	152	214	125	163	31	86	62	155	166	176	26	75	21	188	172
1100	232	96	4	216	238	54	107	210	171	9	195	103	8	88	141	10
1101	117	2	91	123	154	43	191	236	162	116	185	81	127	19	173	193
1110	82	252	246	83	190	187	186	136	223	71	70	218	182	225	89	146
1111	40	209	98	179	255	132	17	199	77	231	213	206	227	90	94	148

The parties are previously recorded by agreement a standard value of the person, who will receive the message, into the file with the extension *.txt and use this file as the second key. Using audio steganography's LSB (Least Significant Bit) most meaningless bit technique, they hide the obtained dividend-remainder values in any sound file. Since the hidden data is hidden in the most meaningless bit of the audio file, the changed audio will not display a frequency feature that can be heard with the ear. Besides, any change in sound frequency will be observed(Fig. 3 and Fig. 4)

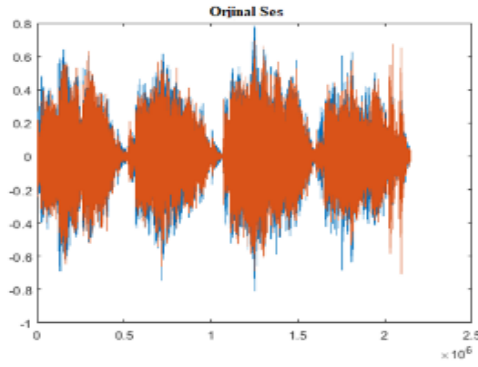


Fig. 3 A sample sound of the used dataset.

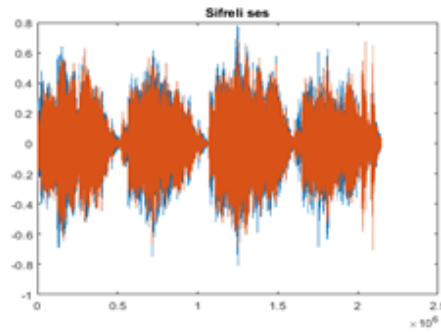


Fig. 4 The stego sound.

2.2. Decryption Algorithm

The decryption process is to decipher by applying in the reverse direction of steps in the encryption algorithm. The working principles of the decryption algorithm are as follows:

- The encrypted message is processed by the key in octal blocks.
- The entire key is implemented by converting the encrypted message into Binary in octal blocks.
- Using the LSB technique, to reach the hidden dividend - remainder values, the previously agreed standard value is saved in the file with the extension *.txt and the second key is entered into this file.

$$\text{➤ } A_n = \frac{K_n - K'_n}{256}$$

$$\begin{aligned} x_1 &= 256 * dividend_1 + remainder_1 \\ x_2 &= 256 * dividend_2 + remainder_2 \\ x_3 &= 256 * dividend_3 + remainder_3 \\ x_4 &= 256 * dividend_4 + remainder_4 \\ x_5 &= 256 * dividend_5 + remainder_5 \\ x_6 &= 256 * dividend_6 + remainder_6 \\ x_7 &= 256 * dividend_7 + remainder_7 \\ x_8 &= 256 * dividend_8 + remainder_8 \end{aligned}$$

$$\sum_{n=1}^{\infty} K_n (n+3)! \frac{h^{n+3}}{n!} [16] \tag{2.1}$$

$$\sum_{n=1}^{\infty} K_n (n+3)! \frac{h^{n+3}}{n!} = x_1 h^4 + x_2 h^5 + x_3 h^6 + x_4 h^7 + x_5 h^8 + x_6 h^9 +$$

$$x_7 h^{10} + x_8 h^{11} [16] \tag{2.2}$$

For each value obtained from the Taylor equation above, their equivalents in Tab. 1 are found.

Step 1.

After the 8th character of the key is converted to binary (a_8), it is processed with the value (m_8) from Tab. 1;

a) If the number of 0 in the 8th character of the key is more than or equal to the number of 1;

- The last bit, the 8th character of the key, is taken first (a_8).
- The 1st value from Tab. 2.1 with the key is XOR (m_8).
- The transformed version (a_8) of the 8th character of the key and the transformed version (m_8) of the 1st value from Tab. 1 is XOR. Taking the last bit of the found value first, the 1st character of the message (1st step) is decoded (m_7).

b) If the number of 0 in the 8th character of the key is less than the number of 1;

- The leading bit of the 8th character of the key is taken to the end (a_8).
- With the key, XOR is applied to the first value from Tab.4 (m_8).
- The transformed version of the key's 8th character (a_8) and the transformed version of the 1st value from Tab. 1 (m_8) is XOR. Taking the first bit of the found value last, the 1st character of the message(1st step) is decoded (m_7).

The first character of the message is reached by performing similar operations with the other characters of the key.

After reaching the 1st character of the message, before the above steps are applied to the characters 2,3,4,5,6,7 and 8, XOR is performed with the value of the previous character from Tab. 1. Then, if the above steps are applied, the message is reached.

2.3. Comparison of Embedding and Decoding Time

The time analysis of the messages with AES into the audio file and embedding/decoding of the messages encrypted with the proposed method (PM) into the audio file and embedding/decoding was made according to the file sizes, the results are given in Tab. 2 and Tab. 3.

The graphics of these data are shown in Fig. 5 and Fig. 6.

Tab. 2 Data Embedding Time Analysis

File Name	File Size (Byte)	Embedding Time (Sec)	
		AES	PM
Test-1	50	50	80
Test-2	150	170	210
Test-3	300	440	460

Tab. 3 Audio decoding Time Analysis

File Name	File Size (Byte)	Decoding Time (Sec)	
		AES	PM
Test-1	50	161	140
Test-2	150	260	277
Test-3	300	392	365

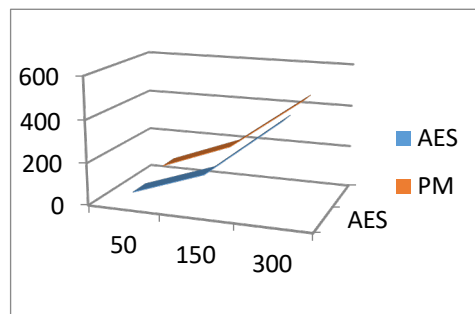


Fig. 5 Embedded Time/File Size

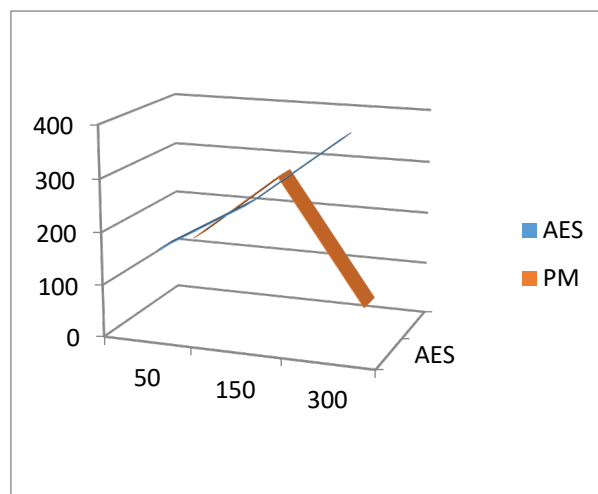


Fig. 6 Audio Decoding/File Size

2.4. Encryption

Key = Flr@tb3y Message = Steganog

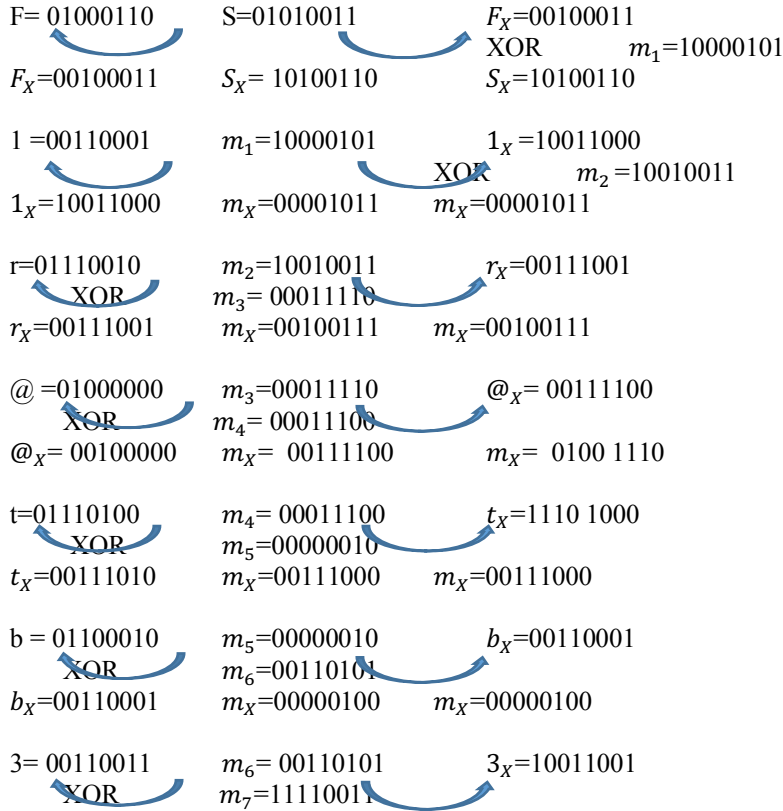
F=01000110 1=00110001 r =01110010 @=01000000
 t=01110100 b=01100010 3=00110011 y=01111001
 S=01010011 t=01110100 e=01100101 g=01100111
 a=01100001 n=01101110 o=01101111 g=01100111

The number of 0 and 1 numbers in the characters used as keys in the application is shown in Tab. 4.

Tab. 4 Number of 0 and 1 numbers in the key

		0 Number	1 Number
F	01000110	5	3
1	00110001	5	3
r	01110010	4	4
@	01000000	7	1
t	01110100	4	4
b	01100010	5	3
3	00110011	4	4
y	01111001	3	5

Step 1.



	0000	0001	0010	0011	0100	0101	0110	0111	1000	1001	1010	1011	1100	1101	1110	1111
0000	1	181	120	169	38	245	76	242	230	39	72	78	47	33	239	249
0001	49	7	37	64	68	160	237	32	58	48	14	203	35	114	110	143
0010	119	23	6	12	220	109	44	61	215	202	159	45	29	250	157	235
0011	24	184	170	22	150	28	149	133	129	198	219	13	145	56	63	204
0100	212	97	201	5	15	177	234	122	50	0	113	102	253	106	36	168
0101	192	65	57	104	226	3	174	101	84	151	42	128	140	60	224	112
0110	207	53	46	95	131	243	87	118	175	164	69	55	178	247	79	126
0111	158	134	217	229	139	73	93	30	254	92	142	59	27	52	248	153
1000	240	121	189	196	138	165	130	228	11	144	34	147	25	194	137	100
1001	180	135	99	222	156	241	161	208	18	20	80	197	67	105	244	124
1010	221	74	211	167	85	115	183	251	111	51	16	108	200	233	205	66
1011	41	152	214	125	163	31	86	62	155	166	176	26	75	21	188	172
1100	232	96	4	216	238	54	107	210	171	9	195	103	8	88	141	10
1101	117	2	91	123	154	43	191	236	162	116	185	81	127	19	173	193
1110	82	252	246	83	190	187	186	136	223	71	70	218	182	225	89	146
1111	40	209	98	179	255	132	17	199	77	231	213	206	227	90	94	148

- 1st Character = 00001011 - 78
- 2nd Character = 00000000 - 1
- 3rd Character = 10000110 - 130
- 4th Character = 10100111 - 251
- 5th Character = 01101110 - 79
- 6th Character = 11011111 - 193
- 7th Character = 11110011 - 179
- 8th Character = 11111010 - 213

Step 10.

Taylor series is used in the encryption algorithm for the Laplace transform to be used in the algorithm. Firstly, the expanded Taylor series is taken with e^t .

$$f(x) = f(a) + \frac{f'(a)}{1!}(x - a) + \frac{f''(a)}{2!}(x - a)^2 + \dots + \frac{f^n(a)}{n!}(x - a)^n + \dots$$

$$= \sum_{n=0}^{\infty} \frac{f^n(a)}{n!}(x - a)^n \tag{3.1}$$

$$e^t = 1 + \frac{t}{1!} + \frac{t^2}{2!} + \frac{t^3}{3!} + \dots = \sum_{n=0}^{\infty} \frac{t^n}{n!} \tag{3.2}$$

Then, if it is expanded with t^3 , equation(3.3) is obtained;

$$t^3 e^t = t^3 + \frac{t^4}{1!} + \frac{t^5}{2!} + \frac{t^6}{3!} + \dots = \sum_{n=0}^{\infty} \frac{t^{n+3}}{n!} \tag{3.3}$$

As a result, $f(t)$ is obtained;

$$f(t) = \sum_{n=0}^{\infty} K_n \frac{t^{n+3}}{n!} .$$

The plain text "Steganag" to be encrypted corresponds to the numbers 78, 1, 130, 251, 79, 193, 179, 213.

$$K_0 = 78, K_1 = 1, K_2 = 130, K_3 = 251, K_4 = 79, K_5 = 193, K_6 = 179, K_7 = 213$$

$$\begin{aligned}
 f(t) &= \sum_{n=0}^{\infty} K_n \frac{t^{n+3}}{n!} \\
 &= K_0 \frac{t^3}{0!} + K_1 \frac{t^4}{1!} + K_2 \frac{t^5}{2!} + K_3 \frac{t^6}{3!} + K_4 \frac{t^7}{4!} + K_5 \frac{t^8}{5!} + K_6 \frac{t^9}{6!} \\
 &\quad + K_7 \frac{t^{10}}{7!}
 \end{aligned} \tag{3.4}$$

From hence;

$$\begin{aligned}
 [f(t)](h) &= T\left[\sum_{n=0}^{\infty} K_n \frac{t^{n+3}}{n!}\right](h) \\
 &= T\left[K_0 \frac{t^3}{0!} + K_1 \frac{t^4}{1!} + K_2 \frac{t^5}{2!} + K_3 \frac{t^6}{3!} + K_4 \frac{t^7}{4!} + K_5 \frac{t^8}{5!} + K_6 \frac{t^9}{6!} + K_7 \frac{t^{10}}{7!}\right](h) \\
 &= 78.3!h^3 + 1.4!h^4 + 130.5! \frac{h^5}{2!} + 251.6! \frac{h^6}{3!} + 79.7! \frac{h^7}{4!} + 193.8! \frac{h^8}{5!} + 179.9! \frac{h^9}{6!} + 213.10! \frac{h^{10}}{7!} \\
 &\quad \sum_{n=0}^{\infty} K_n (n + 3)! \frac{h^{n+3}}{n!} \\
 &= 468h^3 + 24h^4 + 7800h^5 + 30120h^6 + 16590h^7 + 64848h^8 + 90216h^9 + 153360h^{10}
 \end{aligned} \tag{3.5}$$

According to mod (256) in the series 468, 24, 7800, 30120, 16590, 64848, 90216, 153360;

Dividend; 1, 0, 30, 117, 64, 253, 352, 599

Remainder; 212, 24, 120, 168, 206, 80, 104, 16.

Step 11.

The obtained data is hidden in an audio file selected by LSB technique by using the 2nd key through a file with the extension * .txt.

2.5. Decryption

Step 1.

Using the 2nd key, the encrypted message is extracted from the audio file by the file with the * .txt extension.

As a result of the above steps, Dividends and Remainders are obtained as follow;

Dividend; 1, 0, 30, 117, 64, 253, 352, 599

Remainder; 212, 24, 120, 168, 206, 80, 104, 16.

Step 2.

$$\begin{aligned}
 A_n &= \frac{K_n - K'_n}{256} \\
 256 * 1 + 212 &= 468 \\
 256 * 0 + 24 &= 24 \\
 256 * 30 + 120 &= 7800 \\
 256 * 117 + 168 &= 30120 \\
 256 * 64 + 206 &= 16590
 \end{aligned}$$

$256 * 253 + 80 = 64848$
 $256 * 352 + 104 = 90216$
 $256 * 599 + 16 = 153360$
 468, 24, 7800, 30120, 16590, 64848, 90216, 153360 values are obtained.

$$\sum_{n=0}^{\infty} K_n(n+3)! \frac{h^{n+3}}{n!} \tag{3.6}$$

$$\begin{aligned}
 &= 468h^3 + 24h^4 + 7800h^5 + 30120h^6 + 16590h^7 + 64848h^8 + 90216h^9 + 153360h^{10} \\
 &= 78.3!h^3 + 1.4!h^4 + 130.5!h^5 + 251.6!h^6 + 79.7!h^7 + 193.8!h^8 + 179.9!h^9 + 213.10!h^{10}
 \end{aligned}$$

If we apply the Reverse Extended Force Series Transformation to both sides of the equation (3.6), equation (3.7) is obtained.

$$T^{-1} \left[\sum_{n=0}^{\infty} K_n(n+3)! \frac{h^{n+3}}{n!} \right] \tag{3.7}$$

$$= T^{-1} [78.3!h^3 + 1.4!h^4 + 130.5!h^5 + 251.6!h^6 + 79.7!h^7 + 193.8!h^8 + 179.9!h^9 + 213.10!h^{10}]$$

$$\sum_{n=0}^{\infty} K_n \frac{t^{n+3}}{n!} = 78.t^3 + 1.t^4 + 130.\frac{t^5}{2!} + 251.\frac{t^6}{3!} + 79.\frac{t^7}{4!} + 193.\frac{t^8}{5!} + 179.\frac{t^9}{6!} + 213.\frac{t^{10}}{7!}$$

Step 3.


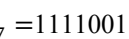






For each value obtained from the equation (3.7) equivalents in Table 3.2 are found.

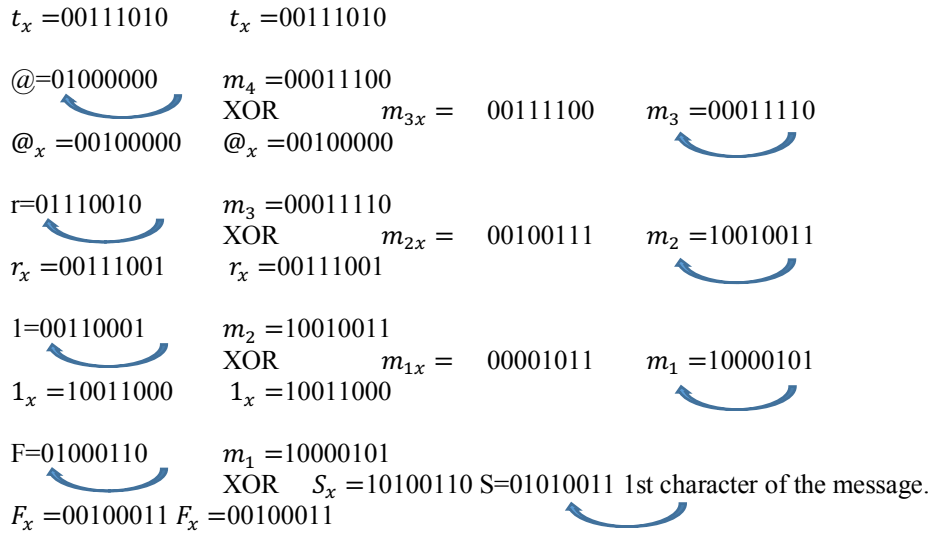
- 1st character = 78 - 00001011
- 2nd character = 1 - 00000000
- 3rd character = 130 - 10000110
- 4th character = 251 - 10100111
- 5th character = 79 - 01101110
- 6th character = 193 - 11011111
- 7th character = 179 - 11110011
- 8th character = 213 - 11111010

Step 4.

Key = Flr@tb3y

- 1st character = 00001011 2nd character = 00000000 3rd character = 10000110
- 4th character = 10100111 5th character = 01101110 6th character = 11011111
- 7th character = 11110011 8th character = 11111010

y=01111001	m ₈ = 00001011		
	XOR	m _{7x} = 11111001	m ₇ = 11110011
y _x = 11110010	y _x = 11110010		
3=00110011	m ₇ = 11110011		
	XOR	m _{6x} = 01101010	m ₆ = 00110101
3 _x = 10011001	3 _x = 10011001		
b=01100010	m ₆ = 00110101		
	XOR	m _{5x} = 00000100	m ₅ = 00000010
b _x = 00110001	b _x = 00110001		
t=01110100	m ₅ = 00000010		
	XOR	m _{4x} = 00111000	m ₄ = 00011100
			



Each character of the message is reached one by one by performing similar operations among other characters.

3. Experimental Results

Firstly, the message is encrypted then the encrypted message is hidden in the audio file. While the decryption process is being done, first the encrypted message is extracted from the audio file and then the encrypted message is decrypted. Data encryption based on the proposed algorithm has been performed in Fig. 7.

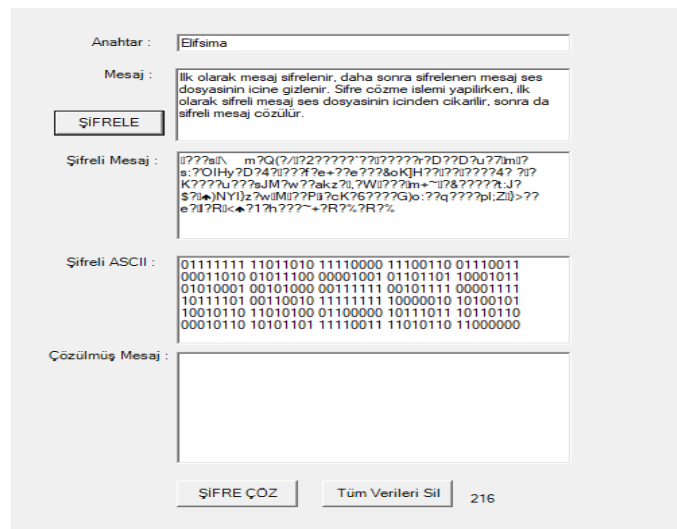


Fig. 7 Encryption screenshot

The encrypted data based on the proposed algorithm has been hidden in the audio file in Fig. 8.



Fig. 8 Screenshot of hiding encrypted data into audio.

4. Performance Analysis

In this technique, measures were taken against language frequency analysis attacks, which is one of the cryptanalysis techniques, by using the Taylor series. Various experimental attacks on the message encryption and hiding technique have been carried out. These attacks against the technique did not give any negative results. The equivalent of the same letter used in a word or a sentence is different values. Therefore, precautions were taken against the attacks of the language analysis method, which is one of the crypto attack techniques.

The encrypted data based on the proposed algorithm was attacked with the language analysis method in Fig. 9.

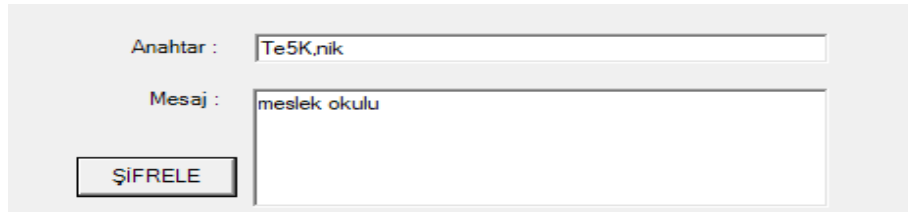


Fig. 9 Language analysis screenshot

12-3 | 104-7 | 92-28 | 56-64 | 2-73 | 224-301 | 40-179 | 112-413 | 64-866 | 112-1268 | 252-1038 | 72-213 | 32-853 | 192-2703 | 16-4064 | 32-478 as seen in the results of the examination, although the letters "e", "u", "l" are used twice in the sentence, all results show different values.

If against plain text attacks, which is another cryptanalysis method, first, the text is encrypted and then hidden in the audio, plain text attacks cannot be done. Even if the data hidden in the audio is reached, it has been tested that it is a powerful algorithm against plain text attacks thanks to the developed algorithm.

The encrypted data based on the proposed algorithm was attacked with plain text method in Fig. 10.

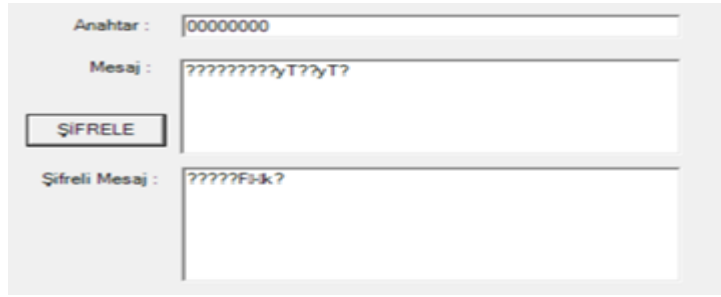


Fig. 10 Plain text attached screenshot

Since the encrypted message is concealed in the most meaningless bit of the sound, when the frequency analysis of the sound is made, no changes that can be seen with the eye as an image are encountered. This sentence is Turkish.

“Steganografinin amacı bilginin varlığını gizlemek veya bilgiyi fark edilmeden başka verinin içerisine yerleştirmektir. Güvenli şekilde gönderilmek istenen veriyi, dikkat çekmeyen görünüme sahip bir başka ortamda gizleyerek üçüncü şahısların gönderilen mesajın varlığından haberdar olması engellenir. Bu işlemler ile metin, ses, resim, video dosyaları içerisine veri gizleyebilmek mümkündür. Bu veriler herhangi bir metin dosyası olabileceği gibi, herhangi bir görüntü içerisine başka bir görüntüyü gizleme şeklinde de olabilmektedir. Yine aynı şekilde bir ses veya video dosyasının içine bir metin dosyası da saklanabilmektedir” text is encrypted as an application. Then this encrypted text is hidden in the audio file “ney sesi. wav”.

First, the data based on the proposed algorithm are encrypted and then hidden inside the sound using the LSB technique in Fig. 11.

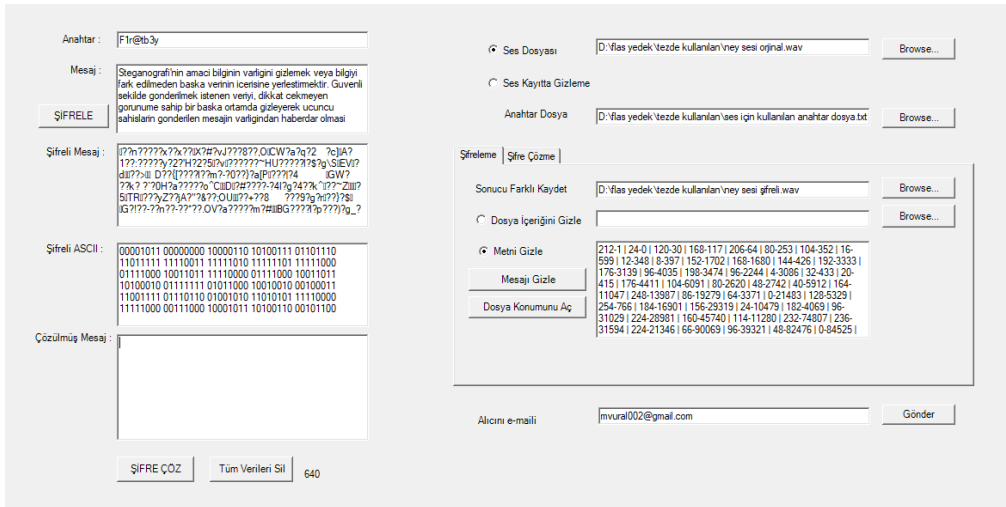


Fig. 11 Practice screenshot

The encrypted message can be hidden in the newly recorded audio file by opening the voice recorder instantly via the program as it is recorded in the audio file.

After saving the encrypted message in a file, optionally, the encrypted message can be hidden into sound in a file from (*.txt, *.xls, *.doc, etc.).

Thanks to the software written, when the program is taken over by unauthorized people, it can be determined who used the program and to whom the data was sent. This process has been added as a security measure. These follow-ups are performed only when used by unauthorized persons.

6. Conclusion and Discussion

By combining cryptography and steganography, a different perspective on cryptology has been introduced with this obtained hybrid model. In applications made with the proposed algorithm, it has been proven once again that mathematics is vital in the field of cybersecurity. Also, by expanding the proposed algorithm; It can be turned into an important defense system that can be used in cyber defense. Moreover, the mobile application of the proposed algorithm can be developed and presented as a commercial product, especially for use in instant communication. Plain text attacks have prevented with the proposed algorithm. Using the Taylor Series in the algorithm, the language analysis attack also has prevented.

Since the message encrypted with this developed algorithm is hidden, the data will not be available in the attacks. Even if hidden data are reached, meaningless values will be obtained because the data are encrypted using the mathematical function. This developed algorithm will make a significant contribution to data security. This is a hybrid model and is open to development. An attack was made with language frequency attack, explicit text attack and sound analysis methods to a text that was encrypted and hidden with the proposed method, as a result, our method was observed to be resistant to these attacks. Other attack techniques can be used to test the reliability of the algorithm. A new crypto device can be produced using the proposed method. Also, the developed algorithm can be used in biometric encryption or decryption.

Ethical approval: This article does not contain any studies with human participants performed by any of the authors.

References

- [1] Yıldırım M. Kriptolojiye Giriş Ders Notları, Uygulamalı Matematik Enstitüsü, 2004.
- [2] Vural M, Gençoğlu MT. Embedded Audio Coding Using Laplace Transform For Turkish Letters. Journal of the Technical University - Sofia Plovdiv branch, Bulgaria “Fundamental Sciences and Applications”,2018; 24:109-116.
- [3] Gençoğlu MT. Importance of Cryptography in Information Security. IOSR Journal of Computer Engineering, 2019; 21(1): 65-68.
- [4] Murray AH, Burchfield RW. The Oxford English Dictionary: Being a Corrected Re-issue. Clarendon Press, Oxford, 1933.
- [5] Weiss M. Principles of Steganography, Math 187: Introduction to Cryptography Professor Kevin O’Bryant, 2004.
- [6] Kadry S, Nasr S. New Generating Technique for Image Steganography. Lecture Notes on Software Engineering, 2013; 1(2):190-193.
- [7] Gençoğlu MT, Baleanu D. [Nonlinear Systems and Complexity](#) book series. In: Power Series Transform In Cryptology and ASCII, *Mathematical Methods In Engineering*. Springer, pp 67-74, 2018.
- [8] Memon N, Wong P. Protecting digital media content. Communications of the ACM 41(7): 34–43,1998.
- [9] Wang H, Wang S. Cyber Warfare: Steganography vs. Steganalysis, Communications of the ACM, 2004; 47(10): 6-82. <https://doi.org/10.1145/1022594.1022597>
- [10] Gençoğlu MT. Programming Encryption Algorithms with steganography. International Conference on Engineering Technology and Innovation, Sarajevo, 2017; 22-26 march, 58.
- [11] Anderson RJ, Petitcolas FAP. On the Limits of Steganography. IEEE Journal of Selected Areas in Communications, 1998; 16(4):474-481.
- [12] Bennett K. Linguistic steganography- survey, analysis and robustness concerns for hiding information in text. Tech Report, Purdue University, 2004.
- [13] Shahreza MS, Shahreza, MHS. Text steganography in SMS. International Journal of Network Security & Its Applications, 2007; 5(1): 2260-2265.
- [14] Gençoğlu MT. Combining Cryptography with Steganography. ITM Web of Conferences, 2017; <https://doi.org/10.1051/itmconf/01010>
- [15] Bhattacharyya S, Banerjee I, Sanyal G. A Novel Approach of Secure Text-Based Steganography Model using Word Mapping Method (WMM). International Journal of Computer and Information Engineering, 2010; 4(2): 96-103.
- [16] Gençoğlu MT. Embedded image coding using Laplace Transform for Turkish letters. Multimedia Tools and Applications, 2019; 78(13): 17521–1753.

- [17] Sellars D. An Introduction to Steganography, 1999. <http://www.cs.uct.ac.za/courses/CS400W/NIS04/papers99/dsellars/index.html>. Date of access: 01 January 2020.
- [18] Petitcolas FAP, Anderson RJ, Kuhn MG. Information Hiding- A Survey. *Process of IEEE*, 1999; 87(7): 1062-1078.
- [19] Huang X, Kawashima R, Segawa N, Abe Y. The Real-Time Steganography Based on Audio-to-Audio Data BitStream. Technical report of IEICE, ISEC, 2006; 106:15-22.
- [20] Jayaram P, Ranganatha HR, Anupama HS. Information hiding using audio steganography – a survey. *The International Journal of Multimedia & Its Applications*, 2011; 3(3):86-96. <https://doi.org/10.5121/ijma.2011.3308>
- [21] Cvejic N, Seppben T. Increasing the capacity of LSB-based audio steganography. Media Team Oulu Information Processing Laboratory University of Oulu FIN- 90014 Finland, 2002.
- [22] Qi YC, Ye L, Liu C. Wavelet domain audio steganalysis for multiplicative embedding model. *Proceedings of the International Conference on Wavelet Analysis and Pattern Recognition*, 2009; 429-432. <https://doi.org/10.1109/ICWAPR.2009.5207432>
- [23] Shahreza SS, Shalmani MTM. High capacity error-free wavelet domain speech steganography. *Acoustics, Speech and Signal Processing IEEE International Conference*, 2008; 223-227. <https://doi.org/10.1109/ICASSP.2008.4517963>
- [24] Choudry KN, Akash W. A Survey Paper on Video Steganography. *International Journal of Computer Science and Information Technologies*, 2015; 6 (3):2335-2338.