IMAGE CODING USING LAPLACE TRANSFORM

Muharrem Tuncay Gençoğlu[1] **Mehmet Vural**[2]

[1] Fırat University, Elazig/NationalDefenseUniversity, Ankara, Turkey, mtgencoglu23@gmail.com

[2] Fırat University,Elazığ,Turkey

Abstract

In this paper a different cryptographic method is introduced by using Power series transform. A new algorithm for cryptography is produced. The extended Laplace transform of the exponential function is used to encode an explicit text. The key is generated by applying the modular arithmetic rules to the coefficients obtained in the transformation. Here, ASCII codes used to hide the mathematically generated keys strengthen the encryption. Text steganography is used to make it difficult to break the password. The made encryption is reinforced by image steganography. To hide the presence of the cipher text, it is embedded in another open text with a stenographic method. Later, this text is buried in an image. For decryption it is seen that the inverse of the Power series transform can be used for decryption easily.

Experimental results are obtained by making a simulation of the proposed method. As a result, it is stated that the proposed method can be used in crypto machines.

Keywords: Cryptography, Power Series Transform, Data Encryption, Embedded Image

1.Introduction

Processed in this environment and protection of the transmitted information or security to provide is great importance. There are many threats such as unauthorized access, damage, etc. while data communication is being performed in the digital environment. In order to eliminate these threats many encryption techniques are developed [1-6].Cryptography is the whole mathematical technical work on information security. The cipher is often expressed with parameters called key which is as part of the external information. Decryption is almost impossible without an appropriate key. For the definition, theorem and mathematical transaction details used in this study, [3,7] can be looked at.

1.2. Our Contribution

We wrote a Power series transformation algorithm which can be used in the encryption methods existed in the literature. Next, we buried a hidden text into any image by cryptology and steganography. We suggested a hybrid method for crypto machines.

In this article, a new information security model based on the Taylor series for steganography is proposed. The proposed model is used for both cryptography and steganography. The characterization of the proposed model is given as follows.

- A new method in which steganography and cryptography reused together, is proposed.
- The proposed steganography method is a media independent steganography method. This method is used for both in image steganography and text steganography.
- A Taylor series based coding method is defined mathematically and practically.
- The method is simulated and the simulation results are shown in the experimental results clearly

2.The Proposed Method

Combining cryptography and steganography methods, the application stages that increase the data security and privacy of this proposed hybrid model are as follows.

2.1.Encryption

In this method, a new encryption method based on the Taylor series is proposed. The steps of the proposed method are as follows.

Step 1: The Taylor series is expanded withe^t. Then this value is multiplied by t^3 to generalize the mathematical relation to be used in the encryption algorithm.

Step 2: The number values corresponding to the letters in the alphabet is applied to the text to be encrypted.

Step 3: The numbers found are replaced in the generalized encryption algorithm.

Step 4: The Power series transform is applied to the function obtained from here.

Step 5: The obtained coefficients are found mod 28 values.

Step 6: Instead of these numbers, the encryption keys are found by taking the quotients in the mode operation.

Step 7: The text is encrypted by writing the letters corresponding to these keys.

Step 8: Encrypted text is converted to ASCII code and the corresponding numbers are found. Then these numbers are converted into a binary system.

Step 9: These numbers are hidden into any text by a method that the user will specify.

Step 10: The sender sends this embedded text along with the private key.

Example

Suppose that we want to send the message “FIRAT”. Firstly we take into accord extended Power series withe^t:

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

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

Then, if we expand;

$$e^t = 1 + \frac{t}{1!} + \frac{t^2}{2!} + \frac{t^3}{3!} + \cdots = \sum_{n=0}^{\infty} \frac{t^n}{n!} \quad (2.1)$$

With t³, then we get:

$$t^3 e^t = t^3 + \frac{t^4}{1!} + \frac{t^5}{2!} + \frac{t^6}{3!} + \cdots = \sum_{n=0}^{\infty} \frac{t^{n+3}}{n!} \quad (2.2)$$

Therefore, we obtain:

$$f(t) = \sum_{n=0}^{\infty} K_n \frac{t^{n+3}}{n!}. \quad (2.3)$$

If we enumerate letters of the alphabet from scratch "FIRAT” plain text be equal 6,9,19,0,22. If we write K_0 =6, K_1 =9, K_2 =19, K_3 =0, K_4 =22 in to (2.3), we get

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

$$= K_0 \frac{t^3}{0!} + K_1 \frac{t^4}{1!} + K_2 \frac{t^5}{2!} + K_3 \frac{t^6}{3!} + K_4 \frac{t^7}{4!} \quad (2.4)$$

If we apply extended Taylor series transformation to both sides of (2.4), we get

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

$$= T[K_0 \frac{t^3}{0!} + K_1 \frac{t^4}{1!} + K_2 \frac{t^5}{2!} + K_3 \frac{t^6}{3!} + K_4 \frac{t^7}{4!}](h)$$

$$= 6.3!\, h^3 + 9.4!\, h^4 + 19.5! \frac{h^5}{2!} + 0.6! \frac{h^6}{3!} + 22.7! \frac{h^7}{4!}$$

$\sum_{n=0}^{\infty} K_n (n+3)! \frac{h^{n+3}}{n!} = 36h^3 + 216h^4 + 1140 \frac{h^5}{2!} + 0 \frac{h^6}{3!} + 4620 \frac{h^7}{4!}$. (2.5)

The equivalence of 36,216,1140,0,4620 in the modes (28) are(K_n) 8,20,20,0,0. If we write quotient in mode operation place of these numbers, we get the key ($K_n^{'}$) 1, 7,40,0,165. "FIRAT" plain text converts "HSSAA" by (2.2).

If we convert "HSSAA" encrypted text to 8-bit characters in the ASCII code we obtain 72, 83,83,65,65. If these codes are written in binary system we get the keys$(1001000)_2$,$(1010001)_2$,$(1010001)_2$,$(1000001)_2$, $(1000001)_2$. ASCII 8 bit keys are in the text as follows: A provision giving the binary number system in the space between each word of the text namely if the number between two words 1 then we get $(1)_2$ and we define 2 with $(0)_2$.

Sender also send this text clearly with (1, 7, 40, 0,165) secret key.

2.2. Decryption

Steps of the proposed decryption method are given below.

Step 1: Thereceiver writes hidden ASCII codes into the text.

Step 2: He finds the letters corresponding to these codes.

Step 3: He obtains the numbers corresponding to the letters.

Step 4: These numbers and the secret key are written in place of the inverse power series.

Step 5: The letters corresponding to the coefficients obtained here are written.

Step 6: The first clear text is obtained.

Example

The recipient receives a text message and by reading the spaces between words with software that will get the data buried create the necessary numerical equivalents. If these numbers are divided into 8-bit groups, the ASCII equivalence of the embedded data is obtained.

If we write H, S, S, A, A→8,20,20,0,0 andsecret key values (1,7,40,0,0,165) into

$$A_n = \frac{K_n - K_n^{'}}{28}$$

$\mathbf{36} = 28x1 + 8$

$\mathbf{216} = 28x7 + 20$

$\mathbf{1140} = 28x40 + 20$

$\mathbf{0} = 28x0 + 0$

$\mathbf{4620} = 28x165 + 0$ are obtained.

If we apply these values 36,216,1140,0,4620 to the

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

then, we get

$$\sum_{n=0}^{\infty} K_n (n+3)! \frac{h^{n+3}}{n!} = 36h^3 + 216h^4 + 1140\frac{h^5}{2!} + 0\frac{h^6}{3!} + 4620\frac{h^7}{4!}$$

$$= 6.3!\,h^3 + 9.4!\,h^4 + 19.5!\frac{h^5}{2!} + 0.6!\frac{h^6}{3!} + 22.7!\frac{h^7}{4!}. \qquad (2.6)$$

If we apply inverse Extended Power Series Transformation to both sides of the (3.7), then we get

$$T^{-1}\left[\sum_{n=0}^{\infty} K_n (n+3)! \frac{h^{n+3}}{n!}\right] = T^{-1}[6.3!\,h^3 + 9.4!\,h^4 + 19.5!\frac{h^5}{2!} + 0.6!\frac{h^6}{3!} + 22.7!\frac{h^7}{4!}]$$

$$\sum_{n=0}^{\infty} K_n \frac{t^{n+3}}{n!} = 6.t^3 + 9.t^4 + 19.\frac{t^5}{2!} + 0.\frac{t^6}{3!} + 22.\frac{t^7}{4!}.$$

If we convert the K_n coefficients we will get the first plain text 6,9,19,0,22→F,I,R,A,T.

The operations performed in this section is shown in Figure 1 and Figure 2.

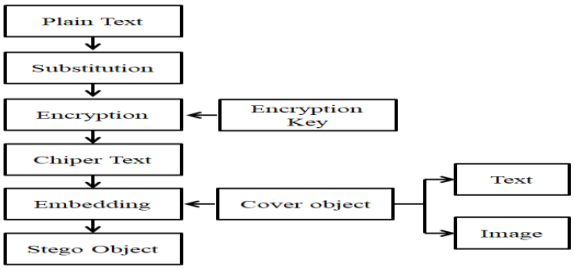

Figure-1. Flow Diagram of Encryption System

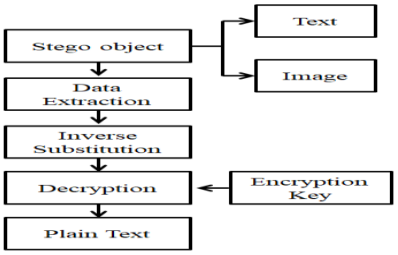

Figure-2. Flow Diagram of Decryption System

3.Experimental Results

In this article, recommended the method for both text and image media is applied. A simulation program is carried out to obtain experimental results. Text steganography and image steganography results are obtained in the performed simulation. Simulation of text steganography windows Fig.3 and4 'are shown.Fig.3 shows encryption method and data embedding window and Fig.4 shows the data extraction and decryption window, respectively.

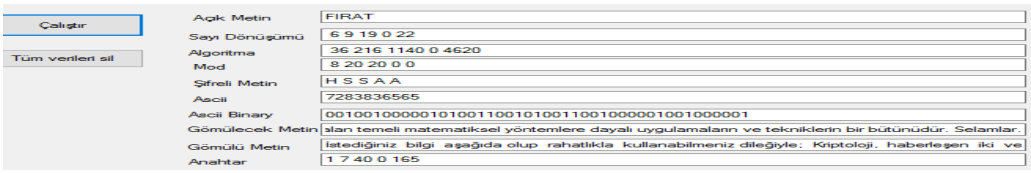

Figure-3. Encryption window of the simulation

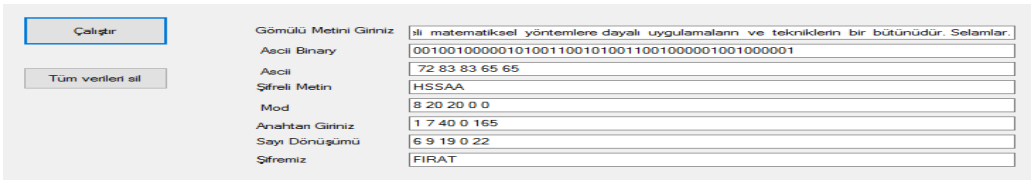

Figure-4. Decryption window of the simulation

In this part of the simulation, images are used as data hiding media.Data encryption and embedding window is shown in Fig. 5.

Figure-5. Data encryption and embedding windowfor image.

Data extraction window for images is shown in Fig. 7.

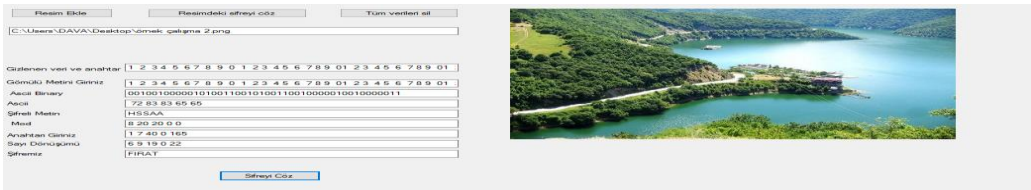

Figure-6. Data extraction window for image.

Data decryption window for images is shown in Fig. 7.

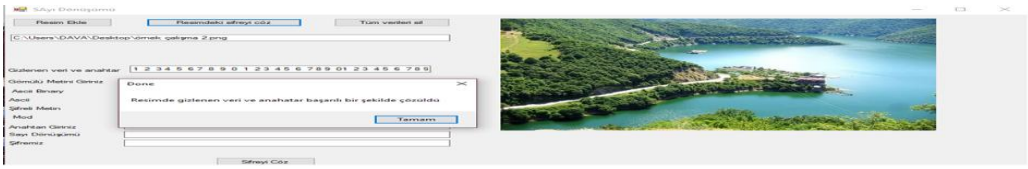

Figure-7. Data decryption window for image.

4. Conclusion and Recommendations

The proposed algorithm is created by using the power series transformation. Keys generated using this algorithm is applied to the method known as substitution method in the literature. In our practice, the keys obtained by the proposed method that aroused as an end result of digitization are used. A hybrid model is developed by using steganography to provide high security and explained in detail. The user can hide this massage which is obtained by taking the coefficient q_n instead of the coefficient $(K_n^{'})$

andalso presence of this message is hidden with ASCII code.Then, using another password, an encrypted text can be hidden into a text by the proposed method. In this way, by using the steganography approach, the security level of the data can be increased.It is verydifficulttofindtheprivatekeybythebrutefarceattackorbyanyotherattack. Finally; the written program can be used in crypto machine.

References

[1]Koç, Ç.K. (2009). Cryptographic Engineering, Springer. PP 125-128.

[2]Gençoğlu, M.T. (2016). Use of Integral Transform in Cryptology. Science and Eng. of Fırat Univ.,**28** (2), 217-220.

[3]Martin, K.M. (2012). Everyday Cryptography Fundamental Principles and Applications, Oxford University Press.

[4]Delfs, H.andKnebl, H. (2007). Introduction to Cryptography Principles and Applications, Springer.

[5]Paar, C.andPelzl, J. (2010). UnderstandingCryptography, Springer.

[6] Gençoğlu, M.T. (2017). Combining Cryptography with Steganography. ITM web of Conferences,**13**, 01010.