*Araştırma Makalesi / Research Article*

# Embedding Data Crypted With Extended Shifting Polybius Square Supporting Turkish Character Set

Hüseyin Bilal MACİT*[1], Arif KOYUN[2], Mehmet Erkan YÜKSEL[3]

*[1]Mehmet Akif Ersoy University, Tefenni MYO, Dept. of Computer Technologies, Burdur, Turkey*
*[2]Süleyman Demirel University, Engineering Faculty, Computer Engineering, Isparta Turkey*
*[3]Mehmet Akif Ersoy University, Engineering Faculty, Computer Engineering, Burdur, Turkey*

**Abstract**
The security of a message transmitted from one peer to another is a matter of many studies over centuries. Today, with digital communication, billions of data are transmitted from one point to another every milisecond. That is why data security has become one of the most studied topics. In this study, an ancient encryption method called Polybius square which has been a source of inspiration for today's encryption methods is introduced. In addition an expanded version of Polybius square was developed adding Turkish character support. An encryption key has also been added to the Polybius cipher. The entire message can be encrypted with a key or with different keys in each character of the message. The encrypted message is hidden within the pixels of the picture files using the LSB algorithm. Thus, when the message is transmitted to the other side, it is encrypted with a private key, hidden inside a cover data, and has become unsuspicious. To measure the change in cover data; MSE, PSNR and SSIM measurement methods are used. The method proposed in the study is coded with a visual programming language. The developed software has been introduced and its results are shown.

**Keywords**: Polybius cipher, Encryption, Decryption, LSB, Steganography.

# Türkçe Karakter Destekli Genişletilmiş Kayan Polybius Karesi ile Şifrelenmiş Veriyi Gömme

**Öz**
Bir yerden bir yere iletilen bir mesajın güvenliği, yüzyıllar boyunca yapılan pek çok araştırmanın konusudur. Bugün, dijital iletişim ile milyarlarca veri, her milisaniye bir noktadan diğerine iletilmektedir. Bu nedenle veri güvenliği, üzerinde en çok çalışılan konulardan biri haline gelmiştir. Bu çalışmada, günümüzdeki şifreleme yöntemlerine ilham kaynağı olmuş, Polybius karesi adlı eski bir şifreleme yöntemi tanıtılmıştır. Ayrıca Türkçe karakter desteği eklenerek, Polybius karesinin genişletilmiş bir versiyonu geliştirilmiştir. Polybius karesine ek olarak bir şifreleme anahtarı eklenmiştir. Tüm mesaj bir anahtar ile veya mesajın her bir karakteri farklı anahtarlar ile şifrelenebilmektedir. Şifrelenmiş mesaj, LSB algoritması kullanılarak resim dosyalarının pikselleri içinde gizlenmiştir. Böylece, mesaj karşı tarafa iletildiğinde, bir kapak verisinin içine gizlenmiş ve bir özel anahtarla gizlenmiştir ve varlığı şüphe çekmemektedir. Kapak verisindeki değişimi ölçmek için; MSE, PSNR ve SSIM ölçüm yöntemleri kullanılmıştır. Araştırmada önerilen yöntem görsel bir programlama dili ile kodlanmıştır. Geliştirilen yazılım tanıtılmış ve ürettiği sonuçlar gösterilmiştir.

**Anahtar kelimeler**: Polybius şifrelemesi, Şifreleme, Şifre çözme, LSB, Steganografi.

## 1. Introduction

Today; people, companies and corporations use the internet as their primary communication tool. Internet is the fastest and most wide platform for rapid transfer of information. One of the biggest problems on the Internet is ensuring the safety of transferring data [1]. Ensuring the security of

*Sorumlu yazar: hbmacit@mehmetakif.edu.tr
*Geliş Tarihi: 25.07.2018, Kabul Tarihi: 17.01.2019*

information can be described as to prevent the access, use, alteration, destruction and damage of information in an unauthorized way [2]. Three key elements of information security are; confidentiality, integrity and availability. Confidentiality is preventing unauthorized access to information or preventing knowledge of existence of the information. Integrity is preventing modification of information by unauthorized persons or software. Availability is to allow access of only authorized persons when they needed the information. The information is not secure even if one of these three basic elements is damaged [2, 3]. There are three basic ways of securing information. These are; prevention, restriction and encryption. Information is secured if access to information is prevented with any blocking access to network. Also information is secured if access to the network is restricted or insulated. If access to the network is not restricted, the most common way of ensuring information security is to encrypt it with information encryption algorithms [4].

Most popular ways of securing information for centuries are cryptography and steganography. The aim of steganography is to hide the existence of information. The steganographic method keeps the secret information embedded in another ordinary information in transmission [5]. Steganography is the best way to transmit information without any doubt, but as the size of the secret information grows, the size of the carrier information must grow [1]. Cryptology uses many disciplines such as mathematics, physics, statistics, computer science and electronics [6]. The aim in cryptography is transforming an important piece of information into a form that can not be understand by third parties [5, 7]. The cryptography word is the combination of two Greek words; “crypto,” which means hidden and “graphos” which means writing [8] and steganography word is the combination of two Greek words; “stego” which means covered and protected and “graphos” which means writing [9].

There are terms as open information, cipher text, key, method name and algorithm in a cryptography method. M is open information (message to be sent), C is encrypted information, K is key, E is encryption method and D is encryption method as it is shown in Figure 1 [10].

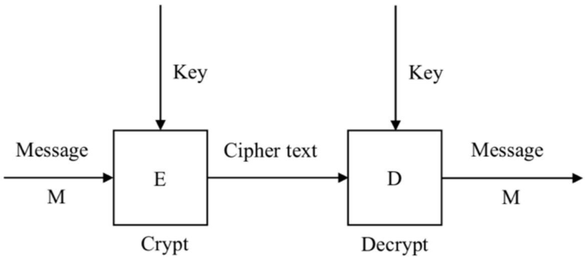


**Figure 1.** Common method of cryptology

According to Figure 1, encryption basicly can be shown as;

$$C = E_K(M) \tag{1}$$

and decryption can be shown as [10];

$$M = D_K(C) \tag{2}$$

As it is shown in Figure 2; cryptography methods are examined in two categories according to the type of the key they use; symmetric cryptography, which uses private key and asymmetric cryptography which uses public key for encryption and decryption [5].

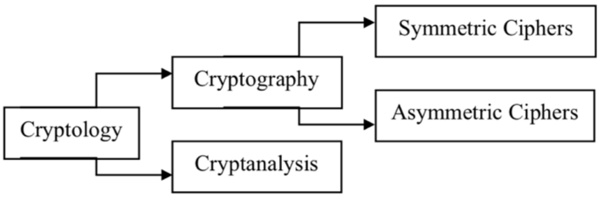


**Figure 2.** Cryptology overview [4]

The most common type of encryption is symmetric encryption which is also called as traditional or single key method and uses the same key for encryption and decryption, that is why the third person should not know the key value. An example to this method can be given as DES [10]. In asymmetric encryption methods; encryption and decryption are performed using two different keys [4]. It's not enough to decrypt the ciphertext when third parties capture the open key. Cryptanalysis is the method of obtaining the true information from a coded, meaningless data [6].

## 2. Material and Method

The Greek historian Polybius, who lived between the years of 203 and 120 BC, invented a ciphering table, which is called by his name. He has placed a square matrix consisting of 5 rows and 5 columns, as every cell shows one of the 26 letters of the Latin alphabet as it is shown in Table 1. The goal is to encrypt the Latin alphabet using only 5 characters which are the numbers of rows and columns [7].

**Table 1.** Polybius square

| | 1 | 2 | 3 | 4 | 5 |
|---|---|---|---|---|---|
| 1 | A | B | C | D | E |
| 2 | F | G | H | I/J | K |
| 3 | L | M | N | O | P |
| 4 | Q | R | S | T | U |
| 5 | V | W | X | Y | Z |

The letters 'I' and 'J' are combined into a single cell in the Polybius square. Mostly, it is possible to guess from the meaning of the text which letter will come in the solved text. To encrypt a word; every letter of the word is shown as number of the row and column in the square. For example; The letter 'D' is encrypted as '14' and the letter 'S' as '43' [4]. When the POLYBIUS word is encrypted, ciphertext string is created with the line and column numbers as in Table 2.

**Table 2.** Encrytping the word “POLYBIUS”

| Letter | P | O | L | Y | B | I | U | S |
|---|---|---|---|---|---|---|---|---|
| Sequence | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 |
| Cipher | 35 | 34 | 31 | 54 | 12 | 24 | 45 | 43 |

The dual number sets representing the row and column number for each letter are combined to form the ciphertext: “3534315412244543” which is going to transmit to the recipient. If the recipient knows the decryption method, he can easily decrypt the ciphertext, but he has to put the letter 'I' or ‘J’ through guessing. As it is seen; Polybius square does not offer secure encryption in today's conditions. However, it can be used combined with different methods such as steganography to provide a secure communication [11].

Polybius encryption is also the basis of many encryption methods used today. However, the Polybius cipher has weaknesses such as;

- It is easy to break because no key is used.

- It can only encrypt Latin alphabetic letters. Besides, it can’t encrypt any of the numbers, punctuation and space between words.
- Since the letters I and J are encrypted with the same code, the decoder must interpret them. For this reason, there is a possibility of error in decryption [4].

An impoved version of Polybius encryption is developed in this study which uses a shifting key to get rid of those weaknesses. This new square is an expanded 10x7 matrix to support all characters on the Turkish keyboard. Moreover, two different characters do not hold in the same cell, so there is no possibility of making mistakes decrypting the ciphertext. Also as it is shown in Table 3, the cell which is in the intersection of row number 8 and column number 2 contains the space character. Thus, the spaces between words and sentences can also be encrypted.

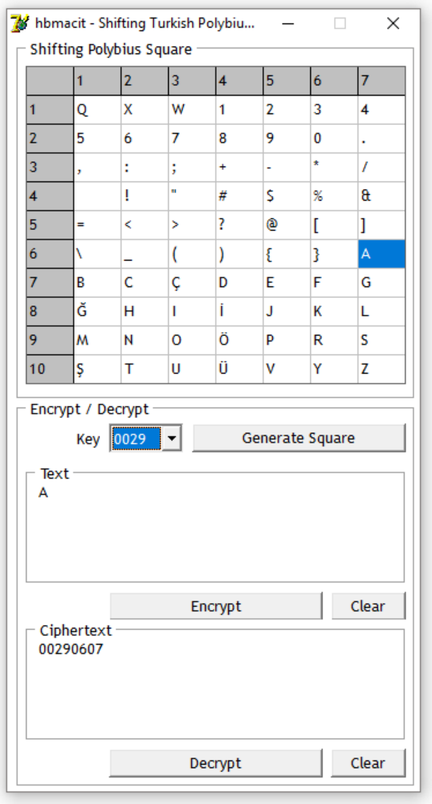
**Table 3.** Improved version of Polybius square (Key=0)

| | 1 | 2 | 3 | 4 | 5 | 6 | 7 |
|---|---|---|---|---|---|---|---|
| 1 | A | B | C | Ç | D | E | F |
| 2 | G | Ğ | H | I | İ | J | K |
| 3 | L | M | N | O | Ö | P | R |
| 4 | S | Ş | T | U | Ü | V | Y |
| 5 | Z | Q | X | W | 1 | 2 | 3 |
| 6 | 4 | 5 | 6 | 7 | 8 | 9 | 0 |
| 7 | . | , | : | ; | + | - | * |
| 8 | / | | ! | “ | # | + | % |
| 9 | & | = | < | > | ? | @ | [ |
| 10 | ] | \ | _ | ( | ) | { | } |

The main goal of this improved version is the ability of shifting all the cells of the matrix with the value of a shift key. The pseudo code of the process of creating the polybius square with the shifting key is;

```
for ( i = 1 to 70)
{
    read( shiftvalue )
    mypointer ← (( shiftvalue + i ) mod 70 ) + 1
    newarray ← newarray + oldarray [ mypointer ]
}
for ( i = 1 to 7 )
    for ( j = 1 to 10 )
    {
        Polybius.cells[i, j] ← newarray[ ((j - 1)*7)+i ]
    }
```

To implement the extended Polybius cipher, a software is developed with the a visual programming language. Figure 3 shows developed application encrypting of letter ‘A’ when shifting key is equal to 29 as an example. As it is seen, the cell values of the Polybius square are shifted to the left by the size of the key value.



|  | 1 | 2 | 3 | 4 | 5 | 6 | 7 |
|---|---|---|---|---|---|---|---|
| 1 | Q | X | W | 1 | 2 | 3 | 4 |
| 2 | 5 | 6 | 7 | 8 | 9 | 0 | . |
| 3 | , | : | ; | + | - | * | / |
| 4 |  | ! | " | # | $ | % | & |
| 5 | = | < | > | ? | @ | [ | ] |
| 6 | \ | _ | ( | ) | { | } | A |
| 7 | B | C | Ç | D | E | F | G |
| 8 | Ğ | H | I | İ | J | K | L |
| 9 | M | N | O | Ö | P | R | S |
| 10 | Ş | T | U | Ü | V | Y | Z |

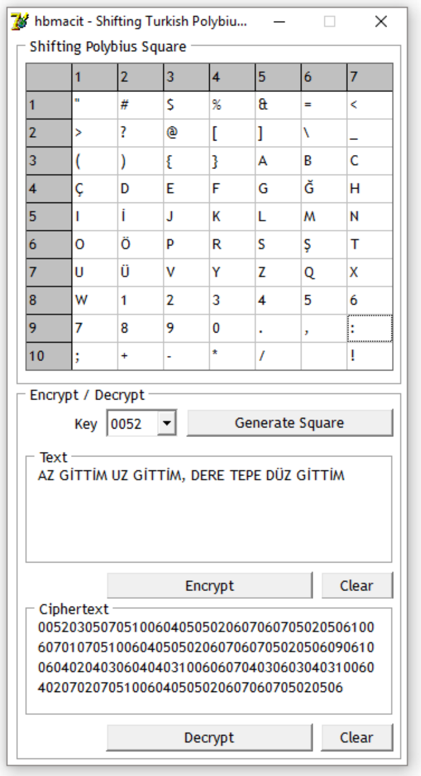
Key 0029

Text
A

Ciphertext
00290607

**Figure 3.** The matrix created with Key value 29 and letter 'A' encryption in developed application

Shifting key value can be used between 0 and 69. After 70 time shifts, the matrix gets to the non-shifted situation. The sentence "AZ GİTTİM UZ GİTTİM, DERE TEPE DÜZ GİTTİM" is encrypted with the proposed method as it is seen in Figure 4. As it is seen, the sentence includes Turkish characters and punctuation.



|  | 1 | 2 | 3 | 4 | 5 | 6 | 7 |
|---|---|---|---|---|---|---|---|
| 1 | " | # | $ | % | & | = | < |
| 2 | > | ? | @ | [ | ] | \ | _ |
| 3 | ( | ) | { | } | A | B | C |
| 4 | Ç | D | E | F | G | Ğ | H |
| 5 | I | İ | J | K | L | M | N |
| 6 | O | Ö | P | R | S | Ş | T |
| 7 | U | Ü | V | Y | Z | Q | X |
| 8 | W | 1 | 2 | 3 | 4 | 5 | 6 |
| 9 | 7 | 8 | 9 | 0 | . | , | : |
| 10 | ; | + | - | * | / |  | ! |

Key 0052

Text
AZ GİTTİM UZ GİTTİM, DERE TEPE DÜZ GİTTİM

Ciphertext
```
0052030507051006040505020607060705020506100
```

**Figure 4.** A Turkish punctuated sentence encrypted with shifting key value 52

First 6 characters of generated ciphertext shown in Figure 5 is analysed in Table 4 as an example. First four digits of ciphertext shows the key value. Then every 4 digits define a segment which represents a cell in the Polybius square. For example, the cell which contains letter ‘A’ is at the intersection of row 3 and column 5 when the key value is 0052. So the segment representing letter ‘A’ is generated as “0305”.

**Table 4.** First digits of example ciphertext

| Shifting Key | A | Z | Space | G | İ | T |
|---|---|---|---|---|---|---|
| 0052 | 0305 | 0705 | 1006 | 0405 | 0502 | 0607 |

Many coding standarts such as UTF-8, Unicode, Big-5 developed to facilitate the expression of different language keyboards and alphabets. This study supposes a 8 bit coding system with a set of 255 characters. In the proposed method; each encrypted segment can be represented as a binary sequence. Since each segment is between 0101 and 1007, a character which encodes in 8 bits in can be encoded as a 10 bit binary string in the proposed method after encryption. Because 10 bit data represents numbers between 0 ($2^0$-1) and 1023 ($2^{10}$-1). It means a vectorel difference between crypted and uncrypted data size as it is shown in Figure 5.

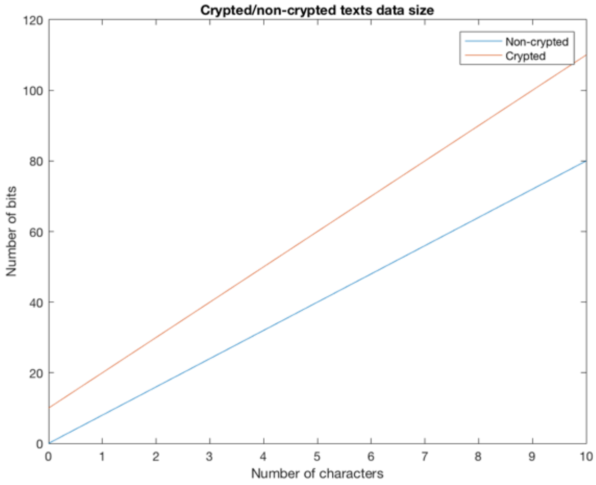


**Figure 5.** A comparison of data size of encrytped versus non-encrypted text

The second scope of this study is trasmitting the ciphertext without any doubt. The best way of unsuspicious transmission is using a steganography method. This study runs a Least Significant Bit algorithm to hide each ciphertext segments into an image file. LSB algorithm basicly runs as in Figure 6.

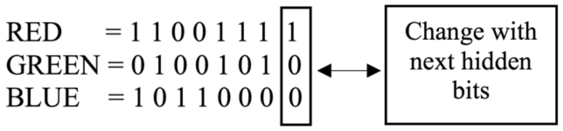
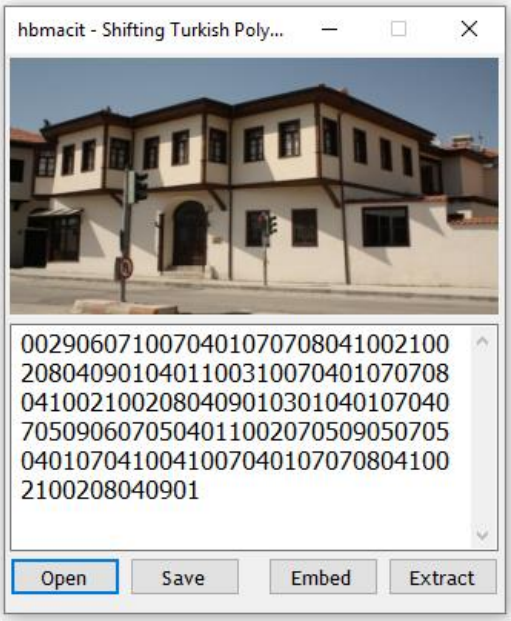


**Figure 6.** Basic expression of LSB

An 8 bit color value is between 0 and 255. Each pixel of a 24 bit color bitmap image is represted with 3 x 8 bits of color sets, thus, changing of last bit of every set doesn’t make a visible change on the image [12]. LSB method can hide 3 bits to each pixel of an image. For example; a 320x240 pixels image can hide 320x240x3=230,400 bits without a remarkable change. Pseudo code of implemented algorithm in this study runs as;

```
bincipher ← bin(ciphertext)
pixelno ← 1
binpointer ← 0
while(1=1)
{
    bin(R) ← bin(R)+binary(bincipher[binpointer])
    binpointer ++
    if (ciphertext=length(binarycipher)) break
    bin(G) ← bin(G)+binary(bincipher[binpointer])
    binpointer ++
    if (ciphertext=length(binarycipher)) break
    bin(B) ←bin(B)+binary(bincipher[binpointer])
    binpointer ++
    if (ciphertext=length(binarycipher)) break
    pixelno++
}
```

Developed application for hiding ciphertext into an image is shown in Figure 7 with the obtained ciphertext from the sentence shown in Figure 4. The image can be selected in different resolutions. As it is mentioned before, higher resolution means higher embedding capacity in steganography.



```
002906071007040107070804100210020804090104011003100704010707080410021002080409010301040107040705090607050401100207050905070504010704100410070401070708041002100208040901
```

**Figure 7.** LSB application with generated ciphertext

7 different image files used to test LSB steganography for same ciphertext. Each image has different size and colors as it is shown in Table 5.

**Table 5.** Images implemented LSB

| Name | Landscape | Candy | Ball | Fruits | House | Feather | World |
|---|---|---|---|---|---|---|---|
| Picture | | | | | | | |
| Size | 217KB | 236KB | 36KB | 582KB | 256KB | 129KB | 152KB |
| Resolution | 320x240 | 320x240 | 320x240 | 525x525 | 470x314 | 397x640 | 225x225 |

## 3. Results

In the proposed method; each encrypted segment can be sent as a binary sequence. Since each segment is between 0101 and 1007, a character can be encoded in a 10 bit binary array in the proposed method after encryption. Although the decrypting process seems like simple, it is quite difficult for a user who does not know the method and key. Even if the encryption method alone does not provide high security, it is supported with a steganographic algorithm to establish a unsuspicious data transfer for higher security communication. The goal of a steganography algorithm is altering the cover as less as possible. Alteration measure can be divided into two categories as objective and subjective. Subjective measure depends to capacity of human visual system. Objective measure depends on some mathematical algorithms such as Peak Signal to Noise Ratio (PSNR) and Structural Similarity Index Measurement (SSIM) [13]. The performance of embedding method is measured by this methods.

PSNR is the noise ratio of an image before and after distortion. Higher PSNR means higher distortion. PSNR is calculated as;

$$PSNR = 20xlog_{10}(\frac{255}{\sqrt{MSE(I,I_o)}}) \tag{3}$$

I is image after distortion, $I_o$ is the original image. To calculate PSNR, first Mean Square Error value has to be calculated which has a inverse ratio to PSNR. Lower MSE means higher performance on the steganography method. MSE is calculated as [13];

$$MSE(I,I_o) = \frac{1}{MxN} x \sum_{y=1}^{M} \sum_{x=1}^{N} [I, I_o]^2 \tag{4}$$

SSIM is a method which considers the quality deterioration in the frames because it perceives the changes in structural information between them. SSIM of images I and Io is calculated as [14];

$$SSIM(I,I_o) = [l(I,I_o)]^{\alpha}.[c(I,I_o)]^{ß}.[s(I,I_o)]^{\gamma} \tag{5}$$

MSE, PSNR, SSIM calculations of 7 images shown in Table 5 which are coded and calculated in Matlab software before and after LSB application of generated ciphertext. Results of calculation is shown is Table 6.

**Table 6.** Similarity results of I and $I_o$

| Name | MSE | PSNR | SSIM |
|---|---|---|---|
| Landscape | 0,0088 | 68,7125 | 0,999907 |
| Candy | 0,0029 | 73,5030 | 0,999977 |
| Ball | 0,0038 | 72,4195 | 0,999956 |
| Fruits | 0,0010 | 77,9690 | 0,999986 |
| House | 0,0015 | 76,2948 | 0,999974 |
| Feather | 0,0011 | 77,7689 | 0,999985 |
| World | 0,0057 | 70,6397 | 0,999957 |

As a result, a lower alteration with a LSB steganography method is implemented and tested in this study. Hidden data is encrypted before embedding with a private key and an ancient method. Similarity results show that an unsispicious text carrying method is generated with an encryption method which can be useful in real time applications.

## 4. References

[1] Manikandan G., Rajendiran P., Balakrishnan R., Thangaselvan, S. 2018. A Modified Polybius Square Based Approach for Enhancing Data Security, International Journal of Pure and Applied Mathematics, 119 (12): 13317-13323.

[2] Çek E. 2017. Kurumsal Bilgi Güvenliği Yönetişimi ve Bilgi Güvenliği İçin İnsan Faktörünün Önemi, Yüksek Lisans Tezi, İstanbul Bilgi Üniversitesi Sosyal Bilimler Enstitüsü, 1p.

[3] Baykara M., Daş R., Karadoğan İ. 2013. Bilgi Güvenliği Sistemlerinde Kullanılan Araçların İncelenmesi, 1'st International Symposium on Digital Forensics and Security, 231-239, Elazığ.

[4] Kondo T.S., Mselle L.J. 2013. An Extended Version of the Polybius Cipher, International Journal of Computer Applications, 79 (13): 30-33.

[5] Kumar P., Rana S.B. 2015. Development of Modified Polybius Technique for Data Security, Interntional Journal of Engineering and Technology, 5 (2): 227-229.

[6] Akleylek S., Yıldırım H.M., Yüce Tok Z. 2011. Kriptoloji ve Uygulama Alanları: Açık Anahtar Altyapısı ve Kayıtlı Elektronik Posta, Akademik Bilişim'11 - XIII. Akademik Bilişim Konferansı Bildirileri, İnönü Üniversitesi, Malatya.

[7] Maity M. 2014. A Modified Version of Polybius Cipher Using Magic Square and Western Music Notes, International Journal For Technological Research In Engineering, 1 (10): 1117-1119.

[8] Gualtieri D.M. 2014. Secret Codes & Number Games, Tikalon Press, ISBN: 978-1-942459-01-9, p:1.

[9] Sumathi C.P., Santanam T., Umamaheswari G. 2013. A Study of Various Steganographic Techniques Used for Information Hiding, International Journal of Computer Science & Engineering Survey, 4 (6): 9-25.

[10] Yerlikaya T., Buluş E., Buluş N. 2006. Kripto Algoritmalarının Gelişimi ve Önemi, Akademik Bilişim Konferansları, Denizli.

[11] Ismail M., Zarin T., Saqib N.U. 2014. Hiding Information Using Techniques of Polybius Square and Steganography to ensure Security, First International Conference on Emerging Trends in Engineering, Management and Scineces, Peshawar, Pakistan.

[12] Yalman Y., Ertürk İ. 2009. İmge Histogramı Kullanarak Geometrik Ataklara Dayanıklı Yeni Bir Veri Gizleme Tekniği, Akademik Bilişim Dergisi, Harran Üniversitesi.

[13] Kaş Ü., Tanyıldız E. 2017. Euler Renk ve Hareket Büyütme Yöntemlerinin Performans Analizi, Afyon Kocatepe University Journal of Science and Engineering, 17: 506-515.

[14] Wang Z., Simoncelli E.P., Alan C. 2003. Multi-scale Structural Similarity For Image Quality Assessment, The Thrity-Seventh Asilomar Conference on Signals, Systems & Computers, DOI: 10.1109/ACSSC.2003.1292216.