T.C. İSTANBUL TİCARET ÜNİVERSİTESİ
MÜHENDİSLİK FAKÜLTESİ
BİLGİSAYAR MÜHENDİSLİĞİ BÖLÜMÜ

VERİ GİZLEME

ŞEVVAL YOĞURTCUOĞLU

Bilgisayar Mühendisliği Programında Hazırlanan

BİLİŞİM TASARIM PROJESİ

Proje Danışmanı: Dr. Öğr. Üyesi Mustafa Cem Kasapbaşı

İSTANBUL, 2019

ÖZET

Haberleşme de mesaj iletiminde mesajın güvenli ve gizli bir şekilde iletilmesinde iki farklı teknik kullanılır bunlar Kriptografi ve Stegonografidir. Kriptografi, gizli bir mesajı şifreler, Steganografi de ise mesaj , ses, görüntü veya video dosyalarının içine yerleştirilir. Bu çalışmada Stenografi yöntemi kullanılarak LSB metoduna göre mesaj lineer ve random yerleştirilerek gizlenmiştir. Stego görüntülerin kaliteleri Tepe Sinyal-Gürültü Oranı (PSNR) ve Yapısal Benzerlik Endeksi (SSIM) ölçüm kriterleri incelenmiş ve değerlendirilmiştir.

ABSTRACT

In communication, two different techniques are used in the transmission of messages in a secure and confidential manner: Cryptography and Stegonography. Cryptography encrypts a confidential message, while Steganography is embedded in a message, audio, image, or video file. In this study, using the Stenography method according to LSB method, the message was hidden by placing it linearly and randomly. The quality of the Stego images were evaluated and evaluated by measuring the Peak Signal-to-Noise Ratio (PSNR) and Structural Similarity Index (SSIM).

İçindekiler Tablosu

1.GİRİŞ

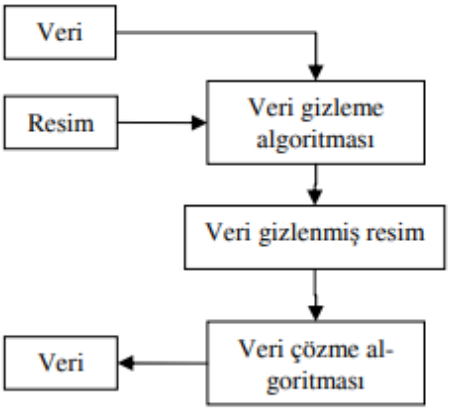
Veri, analiz edilmek üzere bir amaç için toplanan ve çevrilen karakter dizisidir. Bu karakterler metin, sayı, resim, ses veya video dâhil olmak üzere herhangi biri olabilir. Verinin anlam kazanmış durumuna ise bilgi denir.[2] Gelişen teknoloji ile internet kullanımının yaygınlaşması sonucunda elektronik iletişim artmıştır ve böylece elektronik ortamda yapılan işlemler için güvenlik önemli bir kavram haline gelmiştir. Bilgi güvenliğini tanımlamak gerekirse, bilginin izin alınmadan veya yetkisizce erişilmesi, kullanılması, değiştirilmesi, ifşa edilmesini önlemektir.

Günümüzde bilgi güvenliği önlemleri arasında en yaygın önlemlerden biri haberleşme güvenliğidir. Haberleşme, karşılıklı olarak bilgi alışverişinde gönderici ile alıcı arasında güvenli bir haberleşme ortamını oluşturmaktadır. Haberleşme esnasında 2 bilginin hedeflerine ulaşmadan önce 3. şahıslar tarafından ele geçirilmesi ve içeriğinin öğrenilmesi riski her zaman olabilecek bir durumdur. Haberleşme esnasında güvenliğini sağlamak için farklı teknikler sürekli gelişmiştir. iletişimde güvenliğinin ve gizliliğinin sağlanmasında iletilecek metnin şifrelenmesi için kullanılan iki önemli yaklaşımdan ilk metod metnin kendi içerisinde karıştırılarak anlaşılmaz hale getirilmesidir (kriptografi), ikincisi ise metnin bir başka yapı (ses, video, resim) içerisine gizlenmesi (steganografi) olarak tanımlanır.

Bu çalışmada verinin gizliliği ve güvenliğini korumak için steganografi ile bir mesajı resmin içine saklama yöntemi incelenecektir ve değerlendirilmesi yapılacaktır.

2.STEGANOGRAFİ NEDİR?

Steganografi, verinin bir yapı içerisinde gizlenerek iletilmesidir. Bu yaklaşımla amaç, taşınmak istenen mesajın bir başka ortamda saklanarak 3. Şahıs kişilerin iletilen mesajın varlığından haberlerinin olmasını engellemektir. Bu yöntem ile ses, resim, video görüntüleri üzerine bilgi saklanabilir. Bu yaklaşımda içine bilgi gizlenildiği ortama cover-data, oluşan ortama da stego-text denilir. Daha sonra içerisine veri gizlenmiş olan resim anahtar yardımı ile alıcı tarafta decode edilerek içerisinde ki mesaja erişilebilir.



Şekil 1. Steganografi sistem yapısı

2.1.STEGANOGRAFİ TARİHÇESİ

MÖ 440 Antık Çağlar	- Antik Yunan'da ulakların saçlarının kazınıp, saç derisine mesajın yazılması, ulağın saçları uzayıp varacağı yere gitmesi ve saçların tekrar kazınması (Krenn,2004). - Antik Yunan'da balmumu kaplı tabletlerin kullanımı (Bender,Gruhl,Morimoto ve Lu, 1996). - Antik Çin'de meyve sepetinin kullanımı.Meyve sepetindeki her meyvenin birbirine göre pozisyonu farklı bir anlam ifade etmektedir (Petircolas,Anderson ve Kuhn,1999).
1650	- Gaspar Schott'un müzik notları ile bilgileri kodlaması (Bender,Gruhl,Morimoto ve Lu, 1996).
1918'e kadar	- Görünmez mürekkeplerin kullanımı. İlk olarak I Dünya Savaşında kullanılmıştır. - I. ve II. Dünya savaşları sırasında Semagram'ların kullanımı (Petircolas,Anderson ve Kuhn,1999).
1870-1945	- I. ve II. Dünya savaşları sırasında Microdot'ların kullanımı (Johnson ve Jajodia,1998)
Dijital Çağ	- Dijital çağda,sayısal (dijital) nesneler üzerinde steganografi uygulamaları yapılmaktadır ve gelişen teknoloji nedeniyle, verilerimizi korumak amacıyla son yıllarda sıklıkla kullanılmaya başlanmıştır. Gizli veri, yine masum içeriğe sahip olan bir dizi dosyanın içinde saklanabilmektedir.

Tablo 1.Steganografinin tarihsel gelişim süreci

2.2. STEGANOGRAFİNİN KULLANIM ALANLARI

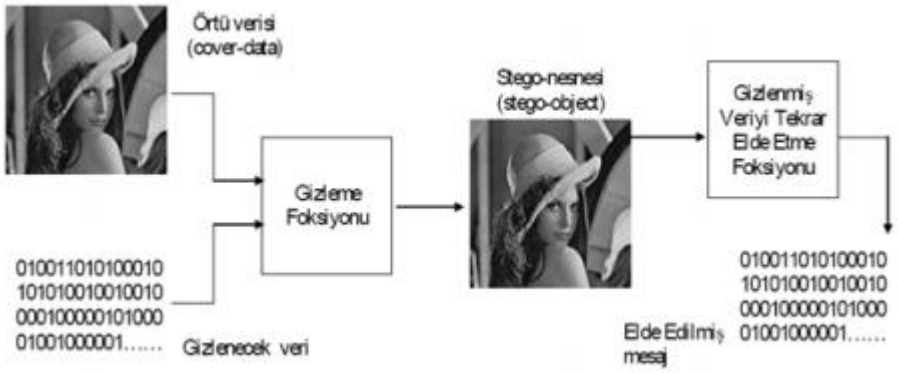
Kullanım alanları bakımından Sayısal Steganografi aşağıda verildiği gibi 4 e ayrılır.

- Metin steganografi
- Ses steganografi
- Görüntü steganografi
- Video steganografi

Bu çalışma Görüntü steganografi bakımından incelenecektir.

2.3.GÖRÜNTÜ(IMAGE) STEGANOGRAFİ

Steganografi uygulamalarında en çok tercih edilen yöntem görüntüdür. Bunun nedeni resimlerin küçük boyutlara sahip olmalarıyla beraber çok sayıda veri içermesinden dolayıdır.



Şekil 2.Steganografik Sistem

Görüntü steganografisinde veriyi resmin içine gizlemek için veriyi en önemsiz bite ekleyerek veya maskeleme ve filtreleme yaparak iletilmesi sağlanır. Verinin saklanmasında göz önünde bulundurulması gereken faktörler; değişimin 3. Şahıslar tarafından fark edilmemesi, saklanacak verinin boyutu ve dayanıklılıktır.

Steganografi üzerine yapılan çalışmalar şu şekildedir;

Yer değiştirmeye yönelik yöntemde, pikseller üzerinde çalışılır. Pikselin rengi bir baytlar ile ifade edilmektedir. Bu baytların en anlamsız bitlerinin değişmesi resim görüntüsünde göz ile farkedilmesini zorlaştırır. Mesaja ait karakterleri temsil eden baytların her bir bitinin farklı bir pikselin en önemsiz bitine kaydedilmesiyle iletilir. Ortaya çıkan resimde renk değerleri olduğu gibi kalır ya da bir artıp azalır. İşaret işlemeye yönelik yöntemlerde, image sıkıştırma algoritmaları kullanılmaktadır. Spektrum yayılmasına yönelik yöntemlerde, gönderilmek istenen mesaj ihtiyaç duyduğu frekans bandından çok daha fazlası kullanılarak bilgi buraya gizlenerek dağıtılmaktadır. . İstatistiksel yöntemlerde ise, bazı istatistiksel bilgilerin değiştirilmesi ile alıcıya gizli bir mesaj iletilebilmektedir. Alıcı taraf bu frekans bantlarındaki bilgiler ile iletilmek istenen mesajı elde edebilmektedir.

Bu çalışma da en anlamsız bite (msb) ekleme yapılırken random ve sıralı üretilerek veri gizleme işlemi yapılmaktadır.

3.EN ÖNEMSİZ BİTE (LSB) EKLEME YÖNTEMİ

Resmin içerisine veri gizlerken en çok kullanılan yöntem resmin piksellerin en anlamsız anlamlı bitine veriyi gizlemektir. Bu yöntemin tercih edilmesinin nedeni en anlamsız bitte yapılan değişiklik de gözle görülür bir farklılık oluşturmamasından dolayıdır. Önce sıkıştırma yapılıp daha sonra veri gizlenirse yüksek miktarda veri gizlenebilir.

3.1.LİNEER LSB YÖNTEMİ

Bu yöntemde amaç , gizlenecek verinin resmin bitlerinin ilk baytından başlanarak sırayla en anlamsız bitlere konulmasıdır.

Örneğin, 'S' harfi gizlemek istersek; 'S' nın değeri 01010011 dir. Veri gizlenmemiş haldeki resimdeki bitler : 00100111 11001001 10001000 00100111 11001000 11101001 11001000 00100111 11101101 şeklindedir .

'S' nin gizlenmiş haldeki resimin bitleri şöyle olur;

00100111 11001001 10001000 00100111 11001000 11101000 11001001 00100111 11101101

Bu yapmakta olunan çalışmada resmin içine veri gizlenerek daha sonra bu resmin iletimi sağlanmıştır. Bu yöntemde veriyi gizleme işlemi aşağıdaki algoritmada belirtildiği gibidir.

for $i = 1, \ldots, l(c)$ do

$s_i \leftarrow c_i$

$s_{ji} \leftarrow c_{ji} \quad m_i$

end for

$l(c)$ = esas resmi oluşturan baytların uzunluğu

s_i = steganografik anahtarın bitlerinin gösterimi

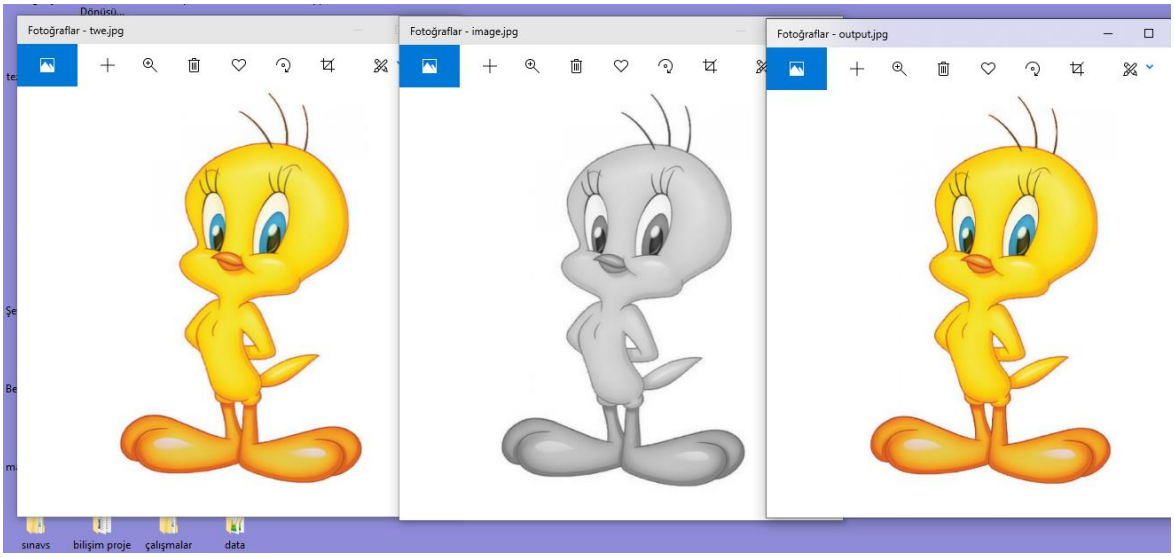
c_i = esas resmin bitlerinin gösterimi

m_i = esas resme gizlenecek verinin bitlerinin gösterimi

ji = esas resmin hangi bitlerine gömülüm yapılacağının gösterimi

Kodlama aşağıdaki adımlar kullanılarak yapıldı;

1. Resmi gri tonlamaya dönüştürme
2. Görüntüyü yeniden boyutlandır
3. Mesajı ikili(binary) formata dönüştür
4. Çıkış görüntüsünü giriş görüntüsü ile aynı olarak başlat
5. Resmin her pikseli boyunca gezin ve aşağıdakileri yap:
   i. Piksel değerini binary e dönüştür
   ii. Gizlenecek iletinin bir sonraki bitini alın
   iii. Değişken temp oluşturun
   iv. Mesaj biti ve pikselin LSB'si aynıysa, temp = 0 olarak ayarla.
   v. Mesaj biti ve pikselin LSB'si farklıysa, temp = 1 olarak ayarla.
   vi. temp, mesaj bitinin XOR'si ve pikselin LSB'si alınarak yapılır.
   vii. Çıktı görüntünün pikselini giriş görüntüsü piksel değeri + temp değerine eklenir
6. Mesajdaki tüm bitler gizleninceye kadar çıkış görüntüsü güncellenmeye devam edilir
7. Son olarak, girdi ve çıktı resimleri gösterilir.



Şekil 3. lsb yöntemi ile gizlenmiş mesaj öncesi ve sonrası image (kodu aşağıda verilmiştir)

Spyder (Python 3.7)

File Edit Search Source Run Debug Consoles Projects Tools View Help

Editor - C:\Users\TOSHIBA\Desktop\data\untitled0.py

ödev.py | datasetlwe.py | untitled0.py - proje | dateset.py | LİN.py | untitled0.py - data*

```
import cv2
import numpy as np
image=cv2.imread("twe.png")
gray = cv2.cvtColor(image, cv2.COLOR_BGR2GRAY)
resize=cv2.resize(gray, (512,512))
#%% mesajın ascii ye dönüştürülmesi
c = 0
for s in "sevvalyogurtcuoglu":
    c += 1
print(c)
b=c*8

ascii_value=[ord(ch) for ch in "sevvalyogurtcuoglu"]
print(ascii_value)
#%% binary sisteme dönüstürme
aa=bin(115)
result = []
for i in ascii_value:
    result.append(bin(i))

bin_message = [int(x) if x.isdigit() else x
          for z in result for x in str(z)]
n = 0
for d in bin_message:
    n += 1
print(n)
#%%
output=resize
h, w = resize.shape
bbb=[h,w]
embed_counter = 1

for e in range(h):
    for j in range(w):
        if(embed_counter <= b):
            LSB =np.mod((bbb), 2)
            temp1=LSB^LSB
            g=[n*embed_counter]
            temp = (LSB ^ g)
            output = resize[e][j]+temp
            embed_counter = embed_counter+1
 #%%
cv2.imwrite('image',resize)
cv2.imwrite('output',output)
```

3.2. RASTGELE(RANDOM) LSB YÖNTEMİ

Linear yöntemin zayıf olmasının nedeni iletilmek istenilen mesajın 3. Şahıslar tarafından ele geçirilmesi ve anlaşılmasından dolayıdır. Bu ihtimali düşürmek için "Rastgele Aralık Yöntemi" algoritması geliştirilmiştir. Bu yöntem de lineer de olduğu gibi veriler sırayla en anlamsız bitten başlanarak yüklenmez. Hangi piksellere verinin saklanacağı denklemlere bağlıdır. Bu yöntemin veri saklanırken anahtar oluşturulması en önemli özelliğidir. Anahtar mesajın random olarak seçilen piksellerin en anlamsız bitlerine saklanacağını belirtir. Burada önemli olan alıcı ile verici arasında da aynı anahtar olmalıdır aksi takdirde veri gönderimi sağlanamaz.

for i=1,..., l(c) do

$s_i \leftarrow c_i$

end for

rastgele k_i değerleri üretilir.

$n \leftarrow k_1$

for i=1,...,$l(m)$ do

$s_n \leftarrow c_n \quad m_i$

$n \leftarrow n+k_i$

end for

$l(c)$ = esas resmi oluşturan baytların uzunluğu

$l(m)$ = gizlenecek veriyi baytların uzunluğu

s_i = steganografik anahtarın bitlerinin gösterimi

c_i = esas resmin bitlerinin gösterimi

m_i = esas resme gizlenecek verinin bitlerinin gösterimi

k = gizleyeceğim veri uzunluğunda belirlenen anahtarın gösterimi

Bu yöntemde saklanmak istenen mesajın uzunluğu ile anahtarın uzunluğu aynı olmadır. saklanılması istenilen mesaj yazılır ,bu kelimenin ascii karakter kodlamasında karşılığı bulunur. ilk bayttan başlanarak sırayla saklama işleminin yapılması yerine hangi baytlara verinin saklanacağını gösteren anahtarın kullanıldığı denklem aşağıda yer almaktadır . Bu bitler yine resmin piksellerinin en anlamsız bitlerine saklanacaktır.

Bu denklem;

$$j_1 = k_1$$

$$j_i = j_{i-1} + k_i, i \geq 2$$

j random belirlenmiş anahtara bağlı olarak denklemi kullanarak resmin hangi baytlarında mesajın saklanacağını belirten bir indistir.

4.DEĞERLENDİRME

Steganografi algoritması analiz edilirken orijinal resimdeki değişim oranı oldukça önemlidir. Resimdeki bu değişim ya da resimdeki bozulma oranını hesaplanması için farklı ölçme teknikleri mevcuttur. Steganografi algoritması analiz eden MSE ve PSNR teknikler arasındaki en çok bilinenleridir. PSNR, orijinal resim ile gizli mesaj içeren resim arasındaki benzerlik kalitesini hesaplar. PSNR değerinin hesaplanmasında saklanma sonucu oluşan hataların kareleri toplamının ortalaması (MSE) değeri kullanılmaktadır.

I_1 ve I_2 sırasıyla örtü orijinal resim ve stego resimlerini, M ve N resim boyutlarını göstermektedir.

$$MSE = \frac{\sum_{MN}[I_1(m,n)-I_2(m,n)]^2}{M*N} \quad (6.1)$$

R – resmin mümkün olan en yüksek piksel değeridir.

$$PSNR(dB) = 10*\log_{10}\left(\frac{R}{MSE}\right) \quad (6.2)$$

Şekil 6. Değerlendirme

Görüntü kalitesini anlamak için kullanılan diğer bir ölçü Yapısal benzerlik endeksi (SSIM) dir. SSIM, orijinal resim ile mesaj gizlenmiş resim arasındaki görsel kalitesinin ne kadar birbirine benzediğini gösterir.

Farklı boyut ve dosya türleri için yapılan tablolar aşağıdaki gibidir;

RANDOM LSB

PNG için

Orijinal Resmin Boyutu	Saklanan Kapasite	Stego resmin boyutu	mse	PSNR	SSIM	Çözünürlük
19.7 kb	7 bayt	176 kb	0.26	53.86 dB	0.997	460
2150 kb	7 bayt	1060 kb	0.0012	77.26 dB	0.999	1380

JPEG için

Orijinal Resmin Boyutu	Saklanan Kapasite	Stego resmin boyutu	mse	PSNR	SSIM	Çözünürlük
19.7 kb	7 bayt	19.9 kb	0.19	55.20 dB	0.997	460
208 kb	7 bayt	95.6 kb	1.42	46.59 dB	0.998	1380

LSB

PNG için

Orijinal Resmin Boyutu	Saklanan Kapasite	Stego resmin boyutu	mse	PSNR	SSIM	Çözünürlük
19.7 kb	7 bayt	176 kb	0.25	54.04 dB	0.999	460
2150 kb	7 bayt	1060 kb	6,3	100.13 dB	0.999	1380

JPEG için

Orijinal Resmin Boyutu	Saklanan Kapasite	Stego resmin boyutu	mse	PSNR	SSIM	Çözünürlük
19.7 kb	7 bayt	19.7 kb	0.029	63.45 dB	0.999	460
208 kb	7 bayt	95.4 kb	1,39	46.67 dB	0.988	1380

5.SONUÇ

Bu çalışmadaki amacımız, iletilmek istenen mesajın güvenliğini sağlamakta kullanılan yöntemleri uygulayabilmektir. Kullandığımız yöntemler; Random LSB steganografi ve LSB steganografi yöntemleridir. Bu yöntemeler ile steganografinin çalışma prensibi ve verinin iletilmesi incelenmiş oldu. Her iki yöntemde de büyük ve küçük boyutlu olmak üzere PNG ve JPEG resimler üzerinde çalışılmıştır. LSB yönteminde ilk pikselin en anlamsız bitinden başlayarak daha sonra piksel konumu 1 arttırılarak yine o piksellerin en anlamsız bitine mesaj gizlenip iletilmiştir. Random LSB' de ise piksel konumlarının seçimi rastgele yapılmıştır ve mesaj rastgele seçilen piksellerin en anlamsız bitlerine gizlenip iletilmiştir. Random olarak gizlenen mesajın daha güvenli olduğu gözlemlenmiştir çünkü MSE değeri lineer yöntemde gözlemlenen değerden daha düşük çıkmıştır. (MSE değeri ne kadar düşük ise o kadar iyi gizlenmiştir.) Ayrıca yüksek boyutlu resimlerde PNG formatındaki resmin PSNR değeri JPEG formatındakine göre çok daha yüksek çıkmıştır bu da PNG formatının kayıpsız bilgi sakladığını kanıtlar. Bu yöntemlerin uygulamaları Python dili ile gerçekleştirilmiştir.

6.REFERANSLAR

[1] Johnson, N. F., Duric Z. ve Jajodia S., 2001. Information Hiding : Steganography and Watermarking - Attacks and Countermeasures, Boston.

[2]https://www.computerhope.com/jargon/d/data.htm [Ziyaret Tarihi:22.11.2019].

[3]https://www.tkdk.gov.tr/Kurumsal/BGYS [Ziyaret Tarihi:22.11.2019].

[4] Amin, M.M. and Salleh, M. and Ibrahim, S. and

[5] Chandramouli, R., Memon, N., 2001. Analysis of LSB Based Image Steganography Techniques, Proceedings of the International Conference on Image Processing, Thessalonica, Yunanistan, 1019-1022.

Katmin, 2003. Information hiding using steganography, 4th National Conference on Telecommunication Technology Proceedings, Shah Alam, Malaysia, Page(s):21 – 25.

Atıcı, M.A. 2007. Steganografik Yaklaşımların İncelenmesi, Tasarımı Ve Geliştirilmesi. Yüksek lisans Tezi, Gazi Üniversitesi, Fen Bilimleri Enstitüsü Bilgisayar Mühendisliği Anabilim Dalı, 109,Ankara

Khan, M.S. and Rai, S.S. 2014. Encryption Based Steganography- Modern Approach for Information Security. International Journal of Computer Science and Information Technologies, 5(3), 2914-2917.

https://www.geeksforgeeks.org/lsb-based-image-steganography-using-matlab/ [Ziyaret Tarihi:12.11.2019].