# Sırörtülü Ses Dosyalarının Ki-Kare Ve Olasılıksal Sinir Ağları Yardımıyla Çözümlenmesinde İçeriğe Göre Performans Karşılaştırması

# A Performance Comparision About File Content For Steganalysed Audio Files Through Chi-Square And Artificial Neural Networks

[1]*Ali DURDU*, [2]*Ahmet Turan ÖZCERİT*

[1]Bilgisayar Mühendisliği, Bilgisayar ve Bilişim Bilimleri Fakültesi, Sakarya Üniversitesi, Türkiye
[2]Bilgisayar Mühendisliği, Teknoloji Fakültesi, Sakarya Üniversitesi, Türkiye

## Özetçe

Bu çalışmada, müzik sesi, insan sesi ve hayvan sesi içeren wav ses dosyalarına gizli veri gizlenmiş, gizlenen dosyalara uygulanan Ki-kare testi ile Olasılıksal Sinir Ağı(OSA) beraber kullanılarak çözümlenmesini sağlayan sıraçma tekniği üzerinde performans karşılaştırması yapılmıştır. Kullanılan sıraçma yönteminde gizleme algoritmasının bilinmediği varsayılmış ve En Önemsiz Bit(EÖB) sırörtme yöntemi kullanılarak oluşturulmuş sırlı nesnelere yönelik bir analiz yöntemi geliştirilmiştir. Geliştirilen sıraçma yönteminde, ses dosyalarının son bitlerine gömülmüş veriler Ki-kare testi ile analiz edilerek sonuçlar OSA yapay sinir ağı desteğiyle gerçeğe daha da yakınsanmıştır. Sonuç olarak ki-kare testinin farklı dosya içeriklerinde farklı sonuçlar verdiği görülmüştür. Özellikle insan sesi gibi karmaşık veriler içeren dosyalarda ki-kare testi başarısız olmuştur. Aksine hayvan ve müzik seslerinde başarılı sonuçlar elde edilmiştir.

**Anahtar Kelimeler**: Sıraçma, Sırörtme, Ki-kare, Olasılıksal Sinir Ağları(OSA), Sayısal Ses, En Önemsiz Bit (EÖB)

## Abstract

In this study, there has been carried a performance comparison on variety content hidden data of audio wav files by using the chi-square test and PNN with steganography technique that allows resolution of package. During performance of applied steganography method, it is assumed that hiding algorithm is known. It has been developed an analysis method for hidden objects created by using LSB steganography technique. LSB data hiding method that the hidden data embedded into last bits, has been strengthened by holding a performance comparison analysis with content by music sound, people sound and animal sound about steganography algorithms. Lastly results has been optimized as real as possible by training of PNN neural network.

**Keywords***:* Steganalysis, Steganography, Chi-square, Probably Neural Network (PNN), Digital Audio, Least Significant Bit (LSB)

## 1. Giriş

Teknolojinin gelişmesiyle iletişim olanakları son derece artmıştır. Bu kolay iletişimin yanında anlık olarak sürekli hızlı iletişim ortamlarının en büyük sorunu güvenlik olmuştur. İletişimde güvenlik unsuru üzerinde çalışan birçok çalışma vardır. Şifreleme veya sırörtme (steganography) yöntemleri bunlar arasında sayılabilir.

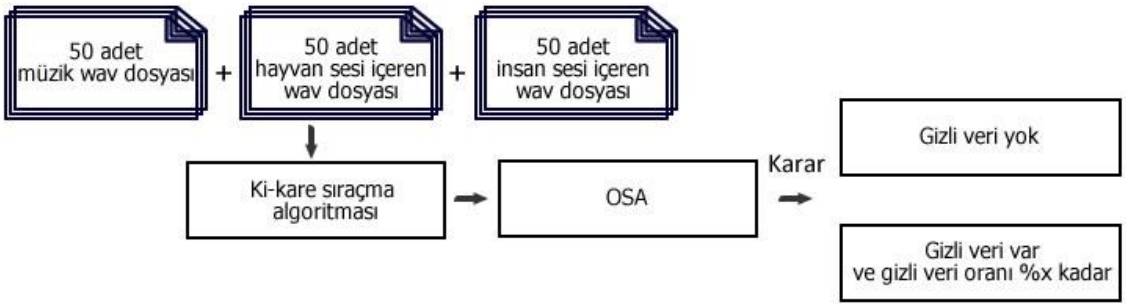
Şifreleme günümüzde de sıkça kullanılan bir güvenlik yöntemidir. Şifrelemede iletilecek veri iletim ortamında üçüncü kişilerin anlayamayacağı şekilde şifreleme algoritmasına bağlı olarak kodlanır. Şifreleme algoritmalarının bulunması ile şifre

*Corresponding author: Address: Sakarya University Esentepe Campus Serdivan Sakarya 54187 Turkey. E-mail address: adurdu@sakarya.edu.tr

çözme algoritmaları bulunmuş ve böylece birbirini sürekli geliştiren bir süreç başlamıştır. Şifreleme yönteminde en büyük açık gönderilen verinin anlamsızlığı nedeniyle şifreli olduğunun bilinmesi ve içerdiği bilginin önem taşıdığının anlaşılmasıdır. Bu nedenle şifreli veri çözülemese de iletişimin engellenebilmesi için iletim hattına saldırılarda bulunulabilir. Veri iletişiminin engellenmesi, şifreleme işlemini geçersiz ve yararsız kılacaktır.

Sırörtme de iletilen gizli veri açık bir şekilde sergilenmez. Gizli veri fark edilmeyecek bir ortamda gizli bir şekilde saklanır. İletilecek gizli veri herhangi bir dosyaya gömülerek masum bir şekilde transfer edilebilir. Sırörtmede iletilecek veri, ayrıca şifreleme mekanizmaları ile de desteklenerek iki boyutlu bir güvenlik sistemi oluşturulabilir. Sırörtme yöntemlerine karşı da geliştirilmiş bazı saldırı yöntemleri mevcuttur. Sıraçma olarak isimlendirilen bu yöntemler, taşıyıcı dosya içerisindeki gizli verinin algılanmasını amaçlayan birçok farklı mekanizmalar içerebilir. Yapılan çalışmalarda, sayısal ortamda sıraçma yöntemleri genellikle resim dosyaları üzerinde uygulanmıştır [1..6]. Resim dosyalarından farklı olarak hareketli görüntüler üzerinde çalışan Çetin ve Özcerit video dosyalarının içerisine gizleme yapacak renk histogramına dayalı yeni bir gizleme tekniği sunmuşlardır [7]. Ses dosyalarına yönelik yapılan sıraçma çalışmaları ise azda olsa vardır. Avcıbaş, ses ölçütlerdeki bozulma ile ses verilerinde sıraçma yöntemi önermiştir [8]. Özer, Sankur, Memon ve Avcıbaş istatiksel ayak izi yöntemiyle ses verilerinde sezme işlemi yapmaya çalışmışlardır [9].

Bu çalışmada, [10] numaralı yayında geliştirilmiş sıraçma yönteminin gizli bilgi içeren ses dosyasının içerik türüne göre performans değerlendirmesi yapılmıştır. Analiz yapılan ses dosyasının içeriğinin farklılığına göre sıraçma algoritmasının performansının değişimi ölçülmeye çalışılmıştır. Buna göre çalışmada, müzik, insan ve hayvan sesleri içeren üç farklı kategoriden sesler kullanılmıştır. Yapılan çalışmanın kısa bir özeti Şekil 1'de genel blok diyagramında gösterilmiştir. Geliştirdiğimiz sıraçma yöntemi, sırörtülü ses dosyasındaki gizli verinin ki-kare sezme algoritması ile olasılık değerlerinin hesaplanması ve bu değerlerin PNN yapay sinir ağı ile değerlendirilmesi esasına dayanır.




**Şekil 1.** Gizli veri sezme genel blok diyagramı

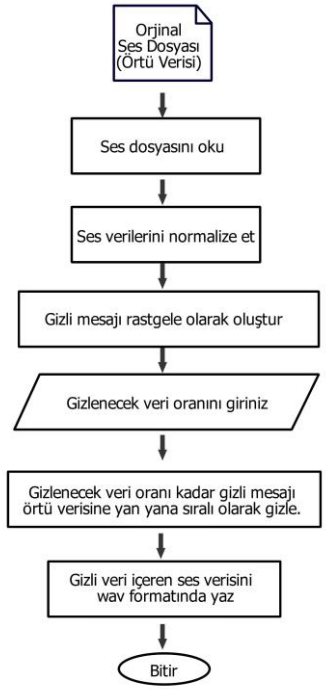
Bölüm 2'de sırörtme, Bölüm 3'de ise sıraçma kavramlarına yer verilmiştir. Elde edilen sonuçlar Bölüm 4'de sunulmuştur. Çalışmanın sonucu ise Bölüm 5'de verilmiştir.

## 2. Lsb Yöntemi ile Sırörtme Algoritması

Veri gizleme algoritması olarak LSB(Least Significant Bit) en önemsiz bit algoritması kullanılmıştır. Her 1 baytlık verinin son biti en önemsiz bittir. LSB yönteminde gizli

verilerin her bir biti ses dosyasını oluşturan baytların son bitlerine yerleştirilmektedir. Buna göre 8 baytlık bir ses örneğine 1 bayt veri gizlenebilir. Bu yöntemde gizli veri bit bit son bitlere gizlenmektedir. Gizli verinin bitleri sırasıyla yerleştirilebileceği gibi rastgelede yerleştirilebilir. Bu çalışmada son bitlere gizli bitler sıralı olarak yerleştirilmiştir. Fakat gizleme işlemi 50 müzik sesi, 50 insan sesi ve 50 hayvan sesi içeren wav dosyalarına yapılmıştır. Böylece gizleme yöntemi sabit tutularak dosya içerikleri değiştirilmiştir. Buradaki amaç sıraçma yöntemimizin farklı dosya içeriklerindeki performanslarını ölçmektir. Şekil 2'de gösterilen sırörtme algoritması LSB yöntemi ile ses dosyasına rasgele oluşturulan mesajı gizlemektedir. Gizli mesajın rastgele oluşturulmasındaki amaç, mesajın içeriğinin her seferinde farklı olmasını sağlamaktır. Böylece sıraçma yönteminin farklı mesajlarda da iyi sonuçlar verdiğini gösterilmektedir. Ayrıca aynı veri gizlenmesindeki oluşacak monoton bit dizilişinin de oluşmasını engellemektir. Şekil 2'de gizleme işleminin algoritması verilmiştir. Ses örnekleri sayısal olarak çok küçük değerler içerdiği için normalize edilerek istenen sayılara büyültülür. Rasgele oluşturulan mesaj istenilen gizli veri oranı kadar ses dosyasına gizlenir. Daha sonra normalize işleminin tersi yapılarak ses örnekleri gerçek değerine döndürülür. Sonra sırlı ses dosyası wav formatında tekrar oluşturulur.

Ses örnekleri 8 veya 16-bit uzunluğunda olmaktadır. Ses örneklerinin bir kanalda bulunduğu ses dosyalarına mono, çift kanalda bulunduğu ses dosyalarına ise stereo ses dosyaları denir. Stereo ses dosyalarında bilgi iki kanalla çoğaltılır ve daha kaliteli ses çıkışı sağlanır. Başlık kısmındaki bilgiler ses dosyasının temel yapısı hakkında bilgi verdiği için buradaki herhangi bir değişiklik doğrudan ses dosyasında yapısal olarak bozulmalara neden olmaktadır. Bu nedenle veri gizleme işlemi başlık kısmında yapılmaz. Data adı verilen yerde ses verileri sıkıştırılmamış halde bulunur. 8 bitlik mono ses dosyalarında tek kanal olduğu için veri gizleme kapasitesi stereo ses dosyalarına göre yarı yarıya düşüktür. Stereo dosyada her iki kanala birden veri gizlemek mümkündür.




**Şekil 2.** LSB yöntemi ile sırörtme algoritması

## 3. Sıraçma Yöntemi

Veri gizleme sonrasında oluşan sırlı dosya görsel işitsel anlamda orijinalinden ayırt edilemese de birtakım istatiksel izler bırakmaktadır. Bu izleri tespit edebilmek için kullanılan bazı saldırı yöntemleri vardır [11]: χ2 Testi (Ki-Kare), Görsel tespit (Görsel saldırılar), Histogram analizleri, RQP Yöntemi, RS analizi (İkili istatistik yöntemi), JPEG Sıraçma, Evrensel tespit sistemleri. Bu yöntemlerin bir kısmı sadece resim verilerine uygulanabilirken bir kısmı ise hem resim hem de ses verilerine uygulanabilmektedir.

Sıraçma yöntemi olarak χ2 testi yöntemi kullanılmıştır. Taşıyıcı verilerdeki her bir bayt ses örneğinin sayısal değerinin ardışık değerli ses örneği ile çift oluşturmasına PoVs (Pair of Values) değer çifti denilmektedir. Ki-kare, taşıyıcı verilerdeki değer çiftlerinin istatiksel analizine dayanan bir sıraçma tekniğidir.

LSB yöntemi ses dosyasında çok küçük de olsa farklılıklar oluşturmaktadır ve bu farklar ses örneğinin ses kalitesinde insan kulağının algılayacağı ölçüde bir bozulma oluşturmaz. Fakat Westfeld ve Pfitzmann yaptıkları çalışmada içerisine veri gizlenmemiş ses verilerinin tek ve çift değerli frekansları düzgün bir şekilde dağılım göstermezken, LSB yöntemi ile veri gizlendiğinde sırlı dosyanın ses örneklerinin her değer çiftinin tek ve çift değerli frekansları eşit çıktığını tespit etmişlerdir[12]. Ki-kare algoritmasının çalışma prensibi bu eşitlik durumuna dayanmaktadır.

χ2 istatistik testinde k tane kategoriden ve gözlemlerden oluşan rastgele bir örnekleme varsayılır. Her gözlem sadece ve sadece bir kategoriye girmektedir. Araştırmada gizli bilginin PoVs'lerinin tek değerlerine önem verilmektedir. Sıralı bir şekilde dağılmış bir mesajın gizlenmesinden sonra, i kategoride teorik olarak beklenen frekans şöyledir:

$$n_i^* = \frac{|\{SÖ\ (SÖ)'nün\ sıralanmış\ indeksi\ \in\{2i,\ 2i+1\}\}|}{2} \qquad (1)$$

(1) ve (2) numaralı denklemde SÖ ses örneğini temsil etmektedir [2]. (1) denklemine göre her bir ses örneği mutlaka bir kategoriye girmiştir. Rastgele şekilde dağılmış bir mesajın gizlenmesinden sonra, ölçülen olasılık frekansı aşağıdaki gibidir.

$$n_i = |\{SÖ\}|(SÖ'nün\ sıralanmış\ indeksi\ \in\{2i,\ 2i+1\})| \qquad (2)$$

(2) numaralı denklemden de anlaşılacağı üzere rastgele dağılmış gizli mesaj iki katı sayıda kategori oluşturacaktır [2].

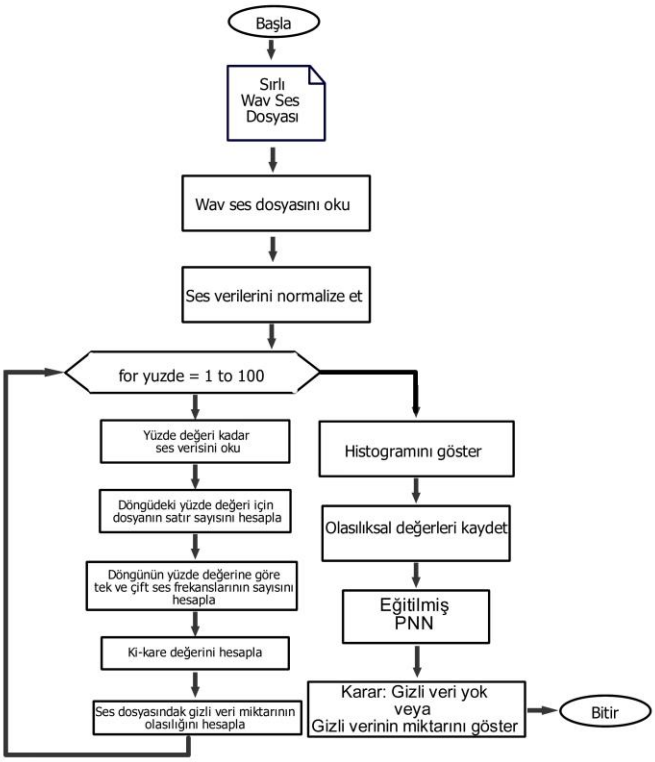
$$X_{k-1}^2 = \sum_{i=1}^{k} \frac{(n_i - n_i^*)^2}{n_i^*} \qquad (3)$$

(3) numaralı denklemde $x^2$ istatistiğinin k-1 bağımsızlık dereceleri hesaplanmaktadır [2].

$$P = 1 - \frac{1}{2^{\frac{k-1}{2}}\Gamma(\frac{k-1}{2})} \int_0^{x_{k-1}^2} e^{\frac{x^2}{2}} .x^{\frac{k-1}{2}-1} d \qquad (4)$$

(4) numaralı denklemde ise $n_i$ ve $n_i^*$ dağılımları eşit olduğu durumda, p mesaj gömme olasılığıdır [2]. $\Gamma$ , Euler'in gama fonksiyonudur[9]. Ki-kare p olasılık değerine göre veri gizleme oranını hesaplamaktadır.

Ses örnekleri sayısal değerlerine bakılarak tekler ve çiftler olarak ayrıştırılır. Ses dosyasının tamamı incelenir ve aynı sayısal değerlere sahip olan ses örnekleri sayılarak her biri için PoVs frekansları(sayıları) bulunur.




**Şekil 3.** Ki-kare steganaliz algoritması akış diyagramı

Bu çalışmada, sırörtme ve sıraçma işlemleri Matlab ortamında gerçeklenmiştir. Matlab ortamının sunduğu PNN sınıflandırıcı giriş ve çıkış verileri ile eğitilir. PNN sınıflandırıcısı, verdiğiniz verilerin içeriklerini araştırır ve öğrendiği bilgilerdeki en yakın olan çıkış değerini sonuç olarak verir. Taşıyıcı dosyada gizli veri sezimi yapılırken gizli verilerin boyutu da olasılıksal olarak hesaplamaktadır. Oluşan bu olasılık değerleri PNN kullanılarak doğru sonuca yakınsanmaktadır.

Çalışmamızda, taşıyıcı dosya kullanıcıdan istenmekte ve dosyanın Wav dosyası formatına uygunluğu kontrol edilmektedir. Ses dosyası okunduktan sonra dosyadaki ses örnekleri çalışılabilecek değerlere normalize edilir. Dosyanın başından başlanarak %1'den % 100'üne kadar okuma yapacak bir döngü ile tüm yüzdesel değerler için ki-kare istatiksel hesaplaması yapılmaktadır. Şekil 3'deki akış diyagramında görüldüğü gibi döngünün her çevriminde döngü değişkeninin belirlediği oran kadar ses verisi üzerinde çalışılır. Döngü içerisinde yapılan tüm işlemler sadece ses dosyasının o anki döngü değeri kadar yüzdesi için hesaplanır. Her bir adımda incelenen ses verilerinde gizli veri olma olasılığı Ki-kare olasılık formülü ile hesaplanır[10]. Hesaplanan değer 0 ile 1 arasındadır. Değer 1'e yaklaştıkça gizli veri olma olasılığı artar. Bu şekilde incelememizin nedeni ki-kare testi bütünsel olarak çalıştığından dosya parçalara

bölünerek her parça ayrı ayrı incelenmiş ve sadece o parça için olasılık tespiti yapılmıştır. Böylece gizlenen verinin konumu tespit edilmiştir.

PNN ağının sınıflandırabilmesi için olasılık değerleri öznitelik vektörleri olarak kullanılmıştır. Her dosyaya hangi oranda veri gizlendiği de PNN ağına öğretilmiştir. Böylece PNN ağının ilgili dosyanın her gizleme oranındaki olasılık durumunu öğrenmesi amaçlanmıştır. Her dosya için 100 adet olasılık değeri PNN ağına bir giriş olarak verilirken PNN ağından bir çıkış değeri(veri gizleme oranı %) elde edilir.

## 4. Deneysel Bulgular Ve Tartışma

Dosya içeriğinin sıraçma algoritmasının başarımına etkisini kıyaslayabilmek için müzik sesi, insan sesi ve hayvan sesi olmak üzere üç kategoride 50'şer dosyaya %40, %70, %100 oranında veri gizlenmiş ve sıraçma algoritmasından geçirilmiştir. Toplamda 450 dosya(3 kategori * 50 dosya * 3 oranda gizleme) sıraçma algoritmasından geçirilmiş ve sıraçma algoritmasının oluşturduğu olasılık değerleri ile PNN ağı eğitime tabi tutulmuştur. Test için her kategoriden eğitimde kullanılandan farklı olarak 10 dosya seçilmiş ve aynı oranlarda veri gizlenmiştir. Sonuçları analiz edebilmek için (5) ve (6) numaralı başarım denklemi kullanılmaktadır.

Tahmin Edilen Gizleme Oranı > Gerçek Gizleme Oranı ise,

$$Başarım\ Oranı = \left| 100 - \frac{Gerçek\ Gizleme\ Oranı\ x\ 100}{Tahmin\ Edilen\ Gizleme\ Oranı} \right| \quad (5)$$

Tahmin Edilen Gizleme Oranı < Gerçek Gizleme Oranı ise,

$$Başarım\ Oranı = \left| 100 - \frac{Tahmin\ Edilen\ Gizleme\ Oranı\ x\ 100}{Gerçek\ Gizleme\ Oranı} \right| \quad (6)$$

Üç kategoriden 10 farklı wav ses dosyasına %40,%70 ve %100 oranlarında veri gizlenmiş ve oluşan sırlı ses dosyaları PNN ağında test edilerek analiz edilmiştir. Sonuçlar Tablo 1'de verilmiştir.

**Tablo 1.** Üç kategoriden on wav ses dosyasının üç farklı oranda veri gizlenmiş versiyonlarının PNN destekli ki-kare sıraçma algoritması başarım sonuçları

| Ses Dosyaları | Müzik Sesleri | | | İnsan Sesleri | | | Hayvan Sesleri | | |
|---|---|---|---|---|---|---|---|---|---|
| | Gizli Veri Oranları | | | | | | | | |
| | %40 | %70 | %100 | %40 | %70 | %100 | %40 | %70 | %100 |
| | PNN Gizli Veri Tahmin Performansı | | | | | | | | |
| Wav 1 | %98 | %99 | %100 | %35 | %30 | %34 | %97 | %97 | %98 |
| Wav 2 | %99 | %100 | %100 | %39 | %34 | %37 | %93 | %96 | %98 |
| Wav 3 | %97 | %98 | %99 | %43 | %42 | %44 | %95 | %94 | %96 |
| Wav 4 | %99 | %99 | %100 | %32 | %34 | %32 | %95 | %96 | %98 |
| Wav 5 | %100 | %100 | %100 | %43 | %34 | %38 | %100 | %100 | %98 |
| Wav 6 | %100 | %100 | %100 | %14 | %26 | %25 | %94 | %96 | %95 |
| Wav 7 | %97 | %99 | %99 | %16 | %36 | %26 | %96 | %96 | %96 |
| Wav 8 | %100 | %100 | %100 | %10 | %26 | %23 | %100 | %96 | %100 |
| Wav 9 | %98 | %99 | %99 | %14 | %18 | %21 | %96 | %94 | %96 |
| Wav 10 | %99 | %99 | %100 | %21 | %20 | %32 | %100 | %96 | %100 |

Ki-kare testi değer çiftlerinin frekanslarını analiz ederek sonuçlar üretmektedir. Değer çiftlerinin oluşması ile ki-kare sıraçma algoritması sağlıklı sonuçlar verir. Aksi halde düzgün sonuçlar vermemektedir. Müzik seslerinde belli bir ritim ve müzik tonu olduğu için sesler düzenli olarak artış ve azalış göstermektedir. Buda komşu ses sinyallerinin birbirine yakın değerler içermesine neden olur. Bu dosyalarda ki-kare sıraçma algoritması yüksek performans göstermektedir. Birbirini izleyen her baytın son bitine veri gizlenmesiyle değer çiftlerinin birbirine yakınlığı sağlanmış ve ki-kare doğru sonuçlar üretmiştir. Hayvan seslerinde de ses tonları düzenli artış ve azalış göstermektedir. Bu nedenle sıraçma algoritması bu tür seslerde de başarılı sonuçlar vermiştir. Fakat insan seslerinden konuşma sesleri anlık artış ve azalışlar göstermekte ve bu durum komşu piksellerin ses değerlerinin birbirinden çok farklı olmasına neden olur. Bu da değer çiftlerinin oluşmasını engeller. Bu tür veri gizlenmiş dosyalarda ki-kare sıraçma algoritması sağlıklı sonuçlar veremez. Komşu piksellerin birbirine yakın değerler içerdiği durumlarda ki-kare sıraçma algoritması başarılı sonuçlar verirken uzak değerler içermesi durumunda ki-kare başarılı olamamıştır.

Tablo 1'de tüm gizleme oranlarında müzik ve hayvan seslerinde ki-kare algoritması yüksek performans değerleri göstermiştir. İnsan sesleri içeren dosyalarda tüm gizleme oranlarında algoritmanın performansı çok düşüktür. Ki-kare algoritmasının başarımı PNN ağını da doğru orantılı olarak etkilemektedir.

## 5. Sonuçlar

Ki-kare sıraçma algoritmasının farklı dosya içeriklerinde başarımları ölçülmüştür. Müzik sesi, hayvan sesi ve insan sesi içeren wav ses dosyaları üzerinde testler yapılmıştır. Ses tonlarının düzenli artış ve azalış gösterdiği dosya içeriklerinde sıraçma algoritması başarılı sonuçlar vermesine karşın ses tonlarının düzensiz artış ve azalışlar içerdiği dosyalarda sıraçma algoritması başarısız sonuçlar vermiştir. Müzik ve hayvan sesleri düzenli artış ve azalış içerir ve bu nedenle bu dosyalarda sıraçma algoritması başarılı sonuçlar vermiştir. İnsan sesi düzenli artış ve azalışlar içermediği için bu dosyalarda yapılan gizlemeler sıraçma algoritması tarafından sağlıklı olarak algılanamamıştır.

Sonuç olarak veri gizleme işlemi seçilen dosya içeriğine göre algılanamazlık açısından önemlidir. Karmaşık ses örnekleri içeren dosyalarda gizlenen veriler daha zor algılanabilirken düzenli ses örnekleri içeren dosyalarda gizlenen veriler daha kolay bulunabilir.

## Kaynakça

[1] Fridrich, J., "Minimizing the embedding impact in steganography", *Proceeding of the 8th Workshop on Multimedia and Security*, Geneva-Switzerland, 2-10, 2006.
[2] Stanley, C.A.,"Pairs of Values and the Chi-squared Attack", *Department of Mathematics*, Iowa State University, 2005.
[3] Bhattacharjee, J. B. Framework of LSB, Adaptive Steganalysis with IQM and Stegnography of Digital Media, 1(1), 39–49, 2010.
[4] Zhang, T., Li, W., Zhang, Y., Zheng, E., & Ping, X. Steganalysis of LSB matching based on statistical modeling of pixel difference distributions. Information Sciences, 180(23), 4685–4694, 2010. doi:10.1016/j.ins.2010.07.037
[5] Tan, S., & Li, B. Targeted Steganalysis of Edge Adaptive Image Steganography Based on LSB Matching Revisited Using B-Spline Fitting. IEEE Signal Processing Letters, 19(6), 336–339, 2012. doi:10.1109/LSP.2012.2194702

[6] Lerch-Hostalot, D., & Megías, D. LSB matching steganalysis based on patterns of pixel differences and random embedding. Computers & Security, 32, 192–206, 2013 doi:10.1016/j.cose.2012.11.005
[7] Cetin O., Ozcerit A., "A new steganography algorithm based on color histograms for data embedding into raw video streams", Sakarya University,Turkey,Elsevier, 2008.
[8] Avcibas, I., "Audio Steganalysis With Content Independent Distortion Measures," *IEEE Signal Processing Letters*, 13(2): 92-95, 2006.
[9] Ozer, H., Sankur, B., Memon, N., Avcibas, I., "Detection Of Audio Covert Channels Using Statistical Footprints Of Hidden Messages.", *Digital Signal Processing 16* (4): 389-401, 2006.
[10] Durdu A., Ozcerit A., Evirgen H. " Sırörtülü Ses Dosyalarının Yapay Sinir Ağları Yardımıyla Çözümlenmesi" *19. Sinyal İşleme Uygulamaları Kurultayı*, Antalya, 2011.
[11] Fridrich, J. and Goljan, M., "Practical steganalysis of digital images state of the art", *Proc. SPIE Photonics West*, 4675: 1-13, 2002.
[12] Westfeld, A. and Pfitzmann, A., "Attacks on Steganographic Systems", *Proceedings of the Third International Workshop Information Hiding*, Dresden, Germany, 61-76, 2000.
[13] Emil Artin, "The Gamma Function", in Rosen, Michael (ed.) Exposition by Emil Artin: a selection; *History of Mathematics 30. Providence*, RI: American Mathematical Society, 2006