Gazi Üniv. Müh. Mim. Fak. Der.
Cilt 31, No 1, 129-144, 2016

Journal of the Faculty of Engineering and Architecture of Gazi University
Vol 31, No 1, 129-144, 2016

STEGANOGRAFİ TABANLI YENİ BİR KLASÖR KİLİTLEME YAKLAŞIMI VE YAZILIMI GELİŞTİRİLMESİ

Mehmet Ali ATICI, Şeref SAĞIROĞLU
Gazi Üniversitesi, Mühendislik Fakültesi, Bilgisayar Mühendisliği Bölümü, Ankara
mehmetaliatici34@gmail.com, ss@gazi.edu.tr

(Geliş/Received: 31.12.2014; Kabul/Accepted: 14.12.2015)

ÖZET

Bu makalede, steganografi tabanlı yeni bir kişisel güvenlik yaklaşımı sunulmuş ve pratik olarak kullanımı için ise bir klasör kilitleme yazılımı (STKK) geliştirilmiştir. Sunulan yaklaşım kullanıcılara, bilgisayardaki tüm dosyaların güvenliği için esnek ve güvenilir çözümler sunmaktadır. Steganografik çözümlerin yanı sıra AES, DES ve 3DES gibi bilinen kriptografik yaklaşımların da geliştirilen yazılıma eklenmesi ile güvenlik arttırılmıştır. Deneysel sonuçlar, geliştirilen çözümün steganalize karşı dayanıklı olduğunu ve tüm dosya tiplerini desteklediği için kişisel güvenliğin artırılmasına katkı sağlayacağını göstermektedir.

Anahtar Kelimeler: Steganografi, steganaliz, güvenlik, klasör kilitleme yazılımı, kriptografi, DES, 3DES, AES

DEVELOPMENT OF A NEW FOLDER LOCK APPRAOCH AND SOFTWARE BASED ON STEGANOGRAPHY

ABSTRACT

This paper introduces a new personal security approach based on steganography. In order to achieve the task, a folder-lock software (STKK) was developed. The proposed approach provides more flexible solutions to the users to secure all files in the computer. In addition to steganographic solutions, cryptographic approaches such as AES, DES and 3DES are also added to the developed software. The experimental results have shown that the developed solution is robust against steganalysis and might provide better personel security by supporting all file types.

Keywords: Steganography, steganalysis, security, folder lock software, cryptography, AES, DES, 3DES

1. GİRİŞ (INTRODUCTION)

Bilişim teknolojilerinin hayatımıza daha fazla girmesi ve yaygınlaşmasıyla birlikte yapılan iş ve işlemler dijital ortamlara kaymakta, bu ortamlarda bulunan, işlenen ve transfer edilen bilgilerin korunması veya güvenliğinin sağlanması çok büyük önem arz etmektedir. Dijital olarak veri iletişimi gerçekleştirilen bir ortamda, göndericiden alıcıya giden veriye yönelik izinsiz erişim, zarar verme, yok etme, değiştirme ve yeniden üretme gibi birçok tehdit mevcuttur. Bu tehditlerin ortadan kaldırılması için çeşitli şifreleme teknikleri geliştirilmiştir [1]. Şifreleme, veriyi anlaşılmaz bir formata dönüştürüp verinin aslına ulaşılmasını zorlaştırsa da iletişimin gizliliğini sağlamamaktadır. Örneğin aradaki trafiğe izinsiz erişim sağlanması durumunda gizli bir veri gönderimi yapıldığı anlaşılabilecektir. Bu noktada tamamlayıcı bir güvenlik çözümü olan steganografi gündeme gelmektedir. Steganografi kelime anlamı olarak gizli yazı veya örtülü yazı anlamına gelmekte olup bilginin varlığı tespit edilemeyecek şekilde saklanması sanatıdır [2]. Sayısal veri dosyası formatlarının çeşitliliği sayesinde birçok dosya türü içerisine steganografik yöntemlerle veri saklanabilmektedir [3-16]. Bunlardan [5] no'lu çalışmada resim, ses ve metin gibi dosya türleri içerisine veri saklama tekniklerini detaylı bir şekilde açıklanmıştır. Ses içerisine, düşük bit kodlaması (Low Bit Encoding), faz kodlaması (phase coding), yayılmış spektrum (spread spectrum) ve yankı veri saklaması (echo data hiding) yöntemleriyle veri saklanması ve metin içerisine boşluk kullanımı, konuşma dilinin yapısı ve eşanlamlı kelimelerden

faydalanarak veri saklama yöntemleri bu çalışmada ayrıntılı bir şekilde irdelenmiştir. En az Önemli Bit (LSB-Least Significant Bit) yöntemiyle resim içerisine veri saklama alanında çok sayıda çalışma yapılmıştır [4, 8, 11, 16]. LSB yöntemiyle ve anahtar kullanılarak, gri seviyeli resimlerde, piksel değerini oluşturan bitlerin ilk dördünün modifikasyonu ile %50 ye yaklaşan kapasiteyle veri saklanabilmiştir [8]. Gri seviyeli Bitmap resimleri içerisine, görsel olarak fark edilmeksizin, en önemsiz 4. bit seviyesine kadar, LSB modifikasyonu yöntemiyle veri saklanabileceğini gösteren Türkçe bir yazılım geliştirilmiştir [11]. Diğer bir çalışmada açık anahtar ve gizli anahtar çiftiyle çalışan bir şifreleme sistemiyle, resim dosyalarının en az önemli bitlerini değiştirerek veri saklayan bir yöntem önerilmiştir. AS knapsack ismi verilen şifreleme sistemi sayesinde göndericinin alıcıya yolladığı veriyi inkâr edememesi ve alıcının göndericinin ilettiği gerçek veriyi görebilmesi sağlanmıştır. Saklama sonrası oluşan resim dosyalarının fiziksel boyutunun, orijinal resim dosyasından farklı olduğu belirtilmiştir [4]. LSB yöntemiyle resim içerisine veri saklayan kriptoloji desteği de sunan bir araç geliştirilmiştir [16]. Palet tabanlı ve kayıplı sıkıştırmalı resim dosyaları içerisine de veri saklama çalışmaları yapılmıştır. Bit Düzlemi Karmaşıklık Bölümlemesi (BPCS- Bit Plane Complexity Segmentation) yöntemini temel alarak palet tabanlı resimler içerisine veri saklayan ve paletteki renk vektörlerinin sırasına bağlı olmayan bir metot geliştirilmiştir [9]. Kayıplı sıkıştırma gerçekleştiren resimler üzerinde BPCS yöntemiyle veri saklayan diğer bir çalışma yapılmıştır [10]. Sıkıştırma işlemi esnasında, küçük-dalga (wavelet) katsayılarının niceleme (quantization) işlemiyle bit düzlemine döndürülmüş hali üzerinde BPCS yöntemiyle veri saklama gerçekleştirilmiş ve %9 ile %15 arasında değişen kapasitelerde veri saklanabilmiştir. Birleşik Fotoğraf Uzmanları Grubu (JPEG- Joint Photographic Experts Group) resimleri içerisine, yine sıkıştırma işlemi esnasında daha fazla saklama kapasitesi ile veri saklayabilen bir yöntem geliştirilmiştir [15]. Palet tabanlı renkli resimler içerisine, veri saklama kapasitesini artırmasına rağmen şeffaflığı bozmayarak veri saklayabilen bir yöntem önerilmiştir [6]. Ses içerisine veri saklama kapsamında gerek LSB modifikasyonu gerekse dönüşüm vb. gibi diğer teknikler kullanılarak steganografi çalışmaları yapılmaktadır. Dönüştürme tekniklerini kullanarak, çalışmanın yapıldığı zamanda mevcut olan ses dosyaları içine veri saklama sistemlerinden daha fazla oranda veri saklanabileceğini tespit edilmiştir [17]. LSB modifikasyonu ile ses içerisine veri saklama kapasitesini %33 oranında arttıran bir yöntem geliştirilmiştir [18]. Ses dosyası içerisine, en az önemli bit modifikasyonu ile veri saklanması üzerine çalışma yapmış ve kokpit sesi gibi ses dosyaları içerisine daha fazla bit seviyesinde veri saklanabildiğini gösterilmiştir [7]. İnternette sıkça kullanılan küçük boyutlu midi ses dosyaları içerisine, LSB yöntemi, tekrarlanan komut kodları algoritması ve sistem harici kodları algoritmasını kullanarak veri saklayan bir çalışma sunulmuştur. Resim ve ses dışındaki dosya türleri de veri saklama çalışmalarında kullanılmaya başlanmıştır [3]. Ayrık Dalgacık Dönüşümleri (DWT- Discrete Wavelet Transforms) ve Hızlı Fourier Dönüşümü (FFT- Fast fourier Transform) tekniklerinden faydalanarak konuşma iletişiminin güvenliğini sağlamaya yönelik yeni bir yaklaşım sunulmuştur [19]. Mp3 dosyaları içerisine saklanacak veri bitine göre pencere tipi değerini ayarlayan ve değiştirme kuralına göre önceki pencere tipi değerini güncelleyen bir teknik sunulmuştur [12]. LSB modifikasyonu yöntemi ile gizli bilgiyi ses dosyasının birden fazla en az önemli bitlerine rastgele ancak anahtar kullanmadan saklayan ve veri saklama kapasitesini artıran bir teknik sunulmuştur [20]. Resim ve ses dosyalarının yanı sıra Yardımlı Metin Biçimleme Dili (HTML-HyperText Markup Language) dosyaları da veri saklama amacıyla kullanılmaktadır. Yardımlı metin (hypertext) içerisine, boşluklar ekleme yerine biçimleme (markup) etiketlerinin pozisyonlarını değiştirerek veri saklayan bir çalışma sunulmuştur [13]. Steganografinin gelişmesine paralel olarak gelişen diğer biri bilim dalı ise steganalizdir. Steganalizin amacı ise steganografinin tam tersine bir resim, ses veya herhangi bir dosyadaki gizli verinin varlığını ortaya çıkarmaktır. Steganaliz, taşıyıcı nesnelerle stego nesneleri ayırt etmek üzere tasarlanmış teknikler bütünü olup saklanan verinin taşıyıcı nesne üzerinde bir takım parmak izleri bıraktığı düşüncesini temel almaktadır [21]. Yani saklama işlemi sonrasında oluşan stego nesne görsel, işitsel veya işlevsel olarak orijinalinden ayırt edilemez olsa da istatistiksel olarak belirgin farklılıklar taşımaktadır. Resim steganalizi konusundaki kadar çok olmasa da ses steganalizi konusunda da bazı çalışmalar yapılmıştır [21-23]. Saklama algoritmasının bilinmesine gerek duyulmaksızın, ses dosyaları içerisinde saklı mesajın varlığını evrensel bir şekilde tespit etmeye yönelik yapılan çalışmada %75 ile %90 arasında değişen bir başarı elde edilmiştir [21]. Mevcut bazı steganografi yazılımlarıyla WAV dosyaları içerisine yapılan gömme işlemini tespit etmeye yönelik bir yöntem geliştirilmiştir [22]. Yapay sinir ağlarıyla Dalga Şekli Ses Dosya Biçimi (WAV- Waveform Audio File Format) dosyalarındaki anormallikleri analiz ederek %75 başarı oranıyla steganografik içerik olup olmadığını tespit eden bir sistem sunulmuştur [24].

Ses steganalizi çalışmaları kapsamında görsel steganaliz teknikleri de geliştirilmiştir. LSB yöntemiyle 1, 2 ve 3. seviyede ses dosyalarına veri saklanmış ve stego wav dosyalarının spektrogram görüntüleri ile taşıyıcı dosyalara ait spektrogram görüntüleri arasındaki farklar nedeniyle veri saklandığı görsel steganalizle kolayca tespit edilmiştir [25]. Yukarıda anlatılan literatür çalışmalarına ilişkin,

Tablo 1. Steganografi ve Steganaliz çalışmalarının karşılaştırma sonuçları (Comparison results of steganography and steganalysis works)

Kaynak	Bilim Dalı	Kullanılan Teknikler	Dosya Tipi
[3]	Steganografi	LSB yöntemi, tekrarlanan komut kodları algoritması ve sistem harici kodları algoritması	Midi ses dosyaları
[4]	Steganografi	Açık anahtar ve gizli anahtar çiftiyle çalışan bir şifreleme sistemi	Resim
[5]	Steganografi	Ses için, Düşük bit kodlaması, faz kodlaması, yayılmış spektrum ve yankı veri saklaması, Metin için boşluk kullanımı, konuşma dilinin yapısı ve eşanlamlı kelimeler, resim için düşük bit oranı kodlaması, metin blok kodlaması vs.	Ses, Resim, Metin
[17]	Steganografi	Dönüşüm teknikleri	Ses
[18]	Steganografi	LSB modifikasyonu	Ses
[7]	Steganografi	LSB modifikasyonu	Ses
[8]	Steganografi	LSB yöntemiyle ve anahtar kullanılarak	Gri seviyeli resimler
[10]	Steganografi	BPCS yöntemi	Resim (JPEG2000)
[11]	Steganografi	LSB modifikasyonu	Gri seviyeli Bitmap resimler
[12]	Steganografi	Pencere değiştirme kuralından faydalanma	Ses (mp3)
[13]	Steganografi	Biçimleme (markup) etiketlerinin pozisyonlarını değiştirerek	Hypertext
[15]	Steganografi	Düşük ve Yüksek ölçeklendirme faktörü uygulanarak oluşan hataya göre Ayrık Kosinüs Dönüşümü (DCT-Discrete Cosine Transformation) katsayılarına saklama tekniği	Jpeg resimler
[19]	Steganografi	DWT ve FFT	Konuşma sesleri
[16]	Steganografi	LSB modifikasyonu	Resim
[24]	Steganaliz	yapay sinir ağlarıyla anormallik analizi	Ses (WAV)
[20]	Steganografi	LSB modifikasyonu	Ses
[25]	Steganaliz	Spektrogram görüntü farklılıklarının analizi	Ses (WAV)
[21]	Steganaliz	Saklı mesajın varlığını evrensel bir şekilde tespit etme	Ses
[22]	Steganaliz	mevcut bazı steganografi yazılımlarıyla yapılan saklamanın tespiti	Ses (WAV)
[23]	Steganaliz	İçerikten bağımsız bozukluk ölçütlerinden faydalanma	Ses

çalışmanın konusu, kullanılan teknikler ve dosya biçimlerini gösteren özet bilgiler Tablo 1'de sunulmuştur. Bu çalışmanın sağladığı temel katkılar, geliştirilen STKK yazılımının steganografi tekniklerini yeni bir alanda uygulayarak klasör kilitleme yazılımlarının işletim sistemi fonksiyonlarına ihtiyaç duyulmaksızın daha güvenli geliştirilebileceğini göstermesi, İleri Şifreleme Sistemi (AES-Advanced Encryption System), Veri Şifreleme Standardı (DES-Data Encryption Standart) ve Üçlü Veri Şifreleme Standardı (3DES-Triple Data Encryption Standart) gibi kriptografik algoritmaları da uygulayarak tüm dosya tiplerini WAV ses dosyaları içerisine ses kalitesini bozmadan 100 kbps gibi yüksek bir kapasiteye kadar saklayabilmesidir.

Makalenin bundan sonraki kısmı şu şekilde organize edilmiştir: 2. bölümde ses dosyaları içerisine veri saklanması anlatılmış, 3. bölümde önerilen yaklaşım ve geliştirilen STKK yazılımı tanıtılmış, 4. bölümde önerilen yaklaşım değerlendirilmesi gerçekleştirilerek son bölüm olan 5. bölümde sonuçlar tartışılmış ve ileride yapılacak çalışmalar hakkında bilgiler verilmiştir.

2. SES DOSYALARI İÇERİSİNE VERİ SAKLAMA (DATA HIDING INTO AUDIO FILES)

Steganografide sayısal bir verinin başka bir sayısal veri içerisine fark edilebilir değişikliklere sebep olmadan saklanması söz konusudur. Veri saklama yöntemlerinin temel mantığı, sayısal veri dosyası formatlarındaki gereksiz veya önemsiz kısımların kullanılmasına veya insan duygularının istismar edilmesine dayanmaktadır. Mesela bir wav dosyasında ses örneği değerlerindeki küçük değişiklikler kulak tarafından fark edilemez. Steganografi teknikleri işitme sisteminin bu özelliğinden faydalanarak wav dosyalarının ses örneği değerlerini veri saklamak amacıyla değiştirebilirler. Ses dosyaları steganografi uygulamalarında veri saklama amacıyla kullanılabilmektedir. Ses içerisine veri saklama yöntemleri düşük bit kodlaması, faz kodlaması, yayılmış spektrum ve yankı veri saklaması olarak sınıflandırılmaktadır [5]. Bu konuda yapılan çalışmalarda genelde dönüştürme teknikleri [17] ve LSB modifikasyonu [7, 18] gibi yöntemler kullanılmıştır.

Düşük bit kodlaması ses örneklerinin son bitlerinin saklanacak veriye göre değiştirilmesi yani LSB modifikasyonudur. LSB modifikasyonu steganografide kullanılan en yaygın yöntemdir [26] ve büyük miktarda verinin saklanmasına izin vermektedir [27]. Faz kodlamasında ses dosyası bölümlere ayrılmakta ve bu bölümlere ait faz değeri veriyi saklayacak şekilde yeniden oluşturulmaktadır. Yayılmış spektrum yönteminde sese ait frekans spektrumu üzerinde veri gizlenmektedir. Yankı veri saklaması yönteminde ise ses sinyali üzerine yankı eklenmekte ve yankının farklı gecikme değerleri kodlanarak veri saklanabilmektedir [5]. Ses dosyasının format dönüşümü vb. nedenlerle yeniden örneklendirilmesi sonucu saklı verinin kaybedilmesine karşı dayanıklı olmaması LSB yönteminin temel dezavantajıdır [27-28]. Taşıyıcı dosyanın işitsel gürültüye sebep olmadan veri gömülecek maksimum bit sayısı veri saklama kapasitesini sınırlamaktadır [18, 20]. Veri saklama kapasitesi artırılırken şeffaflık bozulursa taşıyıcı ses sinyalinin sağlamlığı etkilenir ve bu durumda ataklar kolaylaşır [20].

Ses sinyalleri analog sinyallerdir. Sesi sayısallaştırma işlemi analog sinyalleri örneklendirerek PCM (Pulse Code Modulation) gibi bir yöntemle numerik değerlere dönüştürülerek gerçekleştirilir [29]. PCM gerçek ses sinyallerini tahminen en uygun numerik değere dönüştürmektedir [29]. Dolayısıyla PCM ile elde edilen ses örnekleri bir ses dalgasının belli bir andaki yaklaşık değerini ifade etmekte ve bu durum PCM ile sayısallaştırılmış ses örnekleriyle veri saklama amacıyla oynama imkânı sunmaktadır. WAV dosyaları sıklıkla kullanılan ses dosyası türlerinden birisidir. Wav dosyaları 8 veya 16 bit büyüklüğündeki değerlere sahip ses örneklerinden oluşabilmektedir [30]. Wav dosya formatı Şekil 1'de sunulmuş olup, bir wav dosyası temel olarak bir başlık bölümü ve bunu takip eden ve içerisinde iki adet alt veri parçası barındıran bir "WAVE" veri parçasından oluşmaktadır. Bu veri parçasının alt veri parçalarından birincisi "fmt" veri parçası olup WAV dosyasının veri biçimiyle ilgili bilgileri içermektedir. Diğer alt veri parçası olan "data" ise asıl ses örnekleri verisinden oluşmaktadır. Başlık kısmında yapılacak herhangi bir değişiklik dosyanın yapısını bozup çalışmaz hale getirecektir. Ancak veri bölümündeki ses örneklerinin en az önemli bitlerinin değiştirilmesi ses kalitesinde hissedilebilir bir fark oluşturmamaktadır. WAV dosyaları içerisine veri saklamak için veriye ait bit değerleri sırasıyla taşıyıcı WAV dosyasının "data" parçasındaki ses örneklerinin en az önemli bitlerine dağıtılmakta yani ses dosyasının belirlenen ses örneklerinin en az önemli bitleri saklanacak olan verinin bitlerine eşitlenmektedir.

Şekil 1. WAV dosya formatı (WAV file format) [30].

3. ÖNERİLEN YAKLAŞIM VE GELİŞTİRİLEN UYGULAMA (STKK) (PROPOSED APPROACH AND DEVELOPED APPLICATION)

Klasör kilitleme programları bir klasörü ve içeriğini başkalarına karşı görünmez ve erişilmez hale getiren programlar olup kendi başına ayrı bir güvenlik yazılımı alanı olarak değerlendirilebilir. Bu yazılımlar

genelde işletim sistemine ait fonksiyonları kullanarak çalışır ve aslında disk üzerinde bir yerlerde var olan bir klasörü kullanıcılara ve programlara karşı görünmez ve arama sonucunda bulunmaz hale getirmektedirler. Klasör kilitleme yazılımları klasörü sakladığında diskten silmemekte sadece kullanıcıya görme ve erişim izni vermemektedir. Dolayısıyla saklı klasörün boyutu kullanıcıya görünmediği halde kullanılan disk miktarının içerisinde yer alacaktır.

Bu çalışmada işletim sistemi fonksiyonlarına ihtiyaç duyulmaksızın steganografi tekniklerinin klasör kilitleme yazılımı geliştirilmesinde kullanılabileceği gösterilmektedir. Geliştirilen bu yazılımın temel işlevi, belirlenen bir klasörü veya klasörler ve dosyalar setini tüm içeriğiyle birlikte yine belirlenen WAV formatındaki ses dosyaları seti içerisine şifreleme imkânı da sunarak saklamaktır. Saklama işleminin gerçekleştirilmesi için ikili (binary) veri içerisine başka bir veriyi, bir anahtar yardımıyla taşıyıcı dosyanın örneklerinin istenilen seviyesindeki bitlerine saklayan bir fonksiyon geliştirilmiştir. Ses örneklerin farklı seviyedeki bitlerine veri saklanması test edilerek ses dosyasındaki değişiklikler tespit edilse de klasör kilitleme uygulamasında WAV dosyalarının sadece en az önemli bitleri (LSB) kullanılmıştır. Saklanacak olan verinin bitleri, wav dosyalarının en az önemli bitlerine ardışık değil, anahtardan okunan pozisyonlara rastgele saklanmaktadır. Bu durum saklama kapasitesini düşürmektedir ancak saklama kapasitesi ile steganaliz ataklarına karşı dayanıklılık arasında bir ters orantı vardır. Saklama kapasitesinin düşmesine karşın steganaliz karşısındaki sağlamlık artmaktadır.

Geliştirilen uygulamada temel olarak dört java sınıfı bulunmaktadır. Bunlar wavReader, kripto, steganography ve folderLock sınıflarıdır. wavReader sınıfında taşıyıcı wav dosyalarının Şekil 1'de verilen formata göre başlık ve veri bilgilerine erişim sağlayan metotlar, kripto sınıfında şifreleme, çözümleme ve özet elde etmeye yönelik metotlar, steganography sınıfında veri saklama, saklı veriyi çıkarma ve saklama kapasitesinin hesaplanması gibi metotlar, folderLock sınıfında ise kullanıcı arayüz ekranlarının yanı sıra klasör içeriğinin ham veriye dönüştürülmesi, ham veriden klasör yapısının hiyerarşik olarak tekrar oluşturulması gibi metotlar tasarlanmıştır.

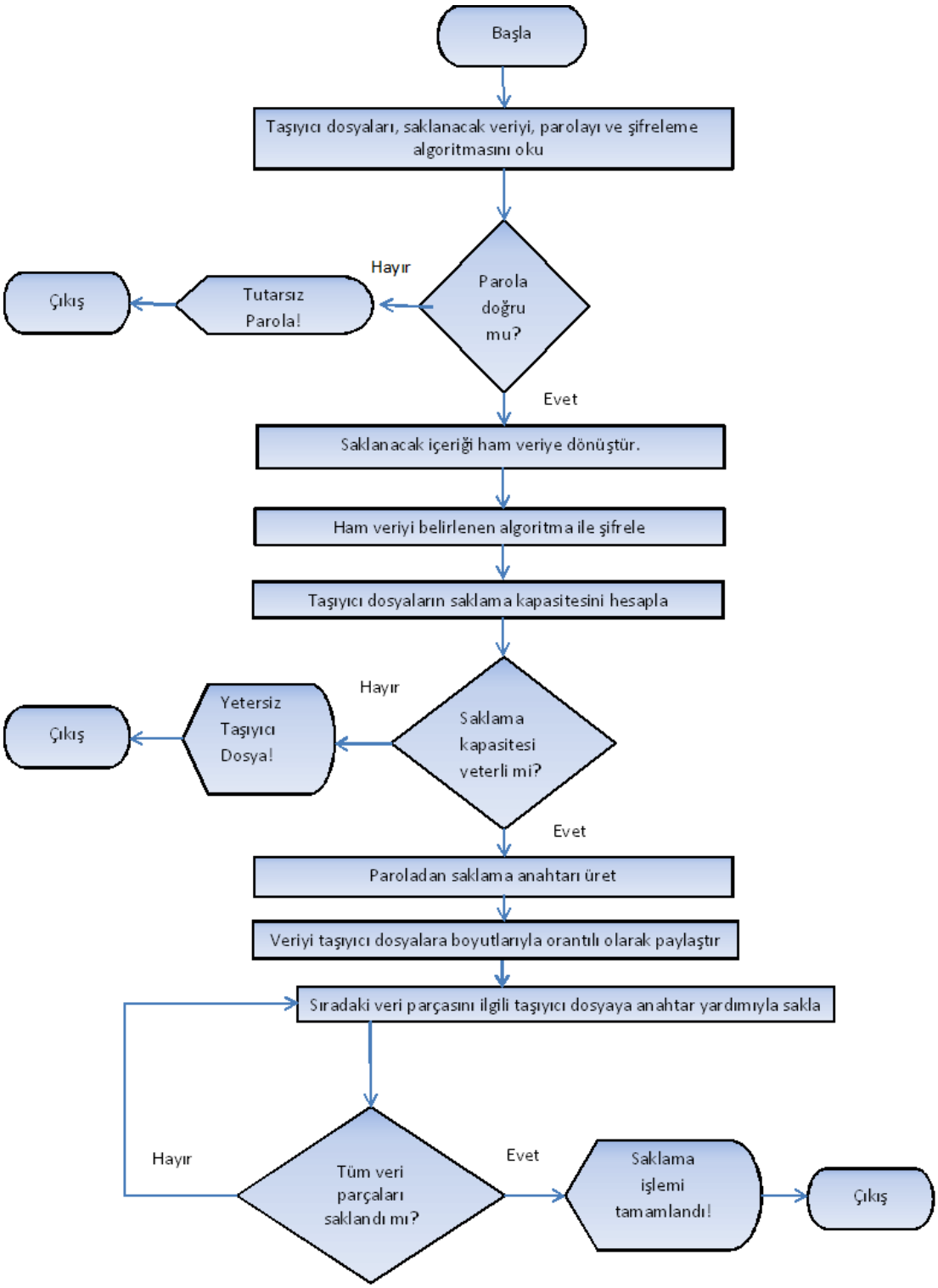
Klasör kilitleme işleminde öncelikle saklanacak klasör, taşıyıcı WAV dosyaları, parola ve şifreleme algoritması belirlenmekte, sonrasında belirlenen parola tutarlıysa saklanacak içerik yani klasör ve hiyerarşik olarak tüm alt klasör ve dosyaları ham veriye (byte dizisi) dönüştürülmektedir. Bu ham veride kilitlenen klasör ve alt klasörlerin isimleri, içerilen tüm dosyaların isim ve verileri ile hiyerarşik yapıyı tekrar sağlayacak bilgiler tutulmaktadır. Daha sonra oluşturulan ham veri belirlenen algoritma ile şifrelenmekte, taşıyıcı WAV dosyalarının saklama kapasitesi bu ham veri için yeterliyse, ham veri her bir taşıyıcı dosyanın saklama kapasitesiyle doğru orantılı olarak taşıyıcı dosya sayısı kadar parçaya ayrılmakta ve bu parçalar ilgili taşıyıcı WAV dosyası içerisine saklanmaktadır. Şekil 2'de klasör kilitleme işlemine ait iş akış diyagramı verilmiştir. Saklama işlemi öncesinde klasör ve hiyerarşik olarak tüm içeriği byte dizisine dönüştürülmektedir. Bu işlemin detayı Şekil 3'de anlatılmaktadır. Buna göre klasör kök dizini isminin uzunluğu ve ismi, klasör isminin uzunluğu ve ismi, içerdiği dosya sayısı, tüm dosyaların sırasıyla isminin uzunluğu, ismi, boyutu ve içeriği bir byte dizisine yazılmaktadır. Sonrasında içerdiği alt klasör sayısı ve tüm alt klasörler için bu işlemler özyinelemeli olarak tekrarlanarak byte dizisine ardışık olarak eklenmektedir. Geri getirme işleminde ise taşıyıcı dosyalardan çıkartılan veriler önce birleştirilmekte sonrasında ise Şekil 2'deki aşamalara göre ham veri okunarak klasör yapısı tekrar disk üzerinde oluşturulmaktadır. Saklanacak verinin ham veriye dönüştürülmesi işlemi Şekil 4'de örnekle de gösterilmektedir. Şekil 4'de öncelikle stego klasörünün bulunduğu dizinin isminin uzunluğu 50 olarak yazılmakta sonrasında dizin ismi eklenmektedir. Burada bu bilgilere gösterim için açıktan yazılmış olup aslında bu değerlerin byte karşılıkları yazılmaktadır. Diğer bilgiler de Şekil 3'de verilen akış şemasına göre diziye eklenmektedir. Klasör içeriği ham veriye dönüştürüldükten sonra birden fazla taşıyıcı WAV dosyası içerisine saklanacaksa bu veri taşıyıcı dosyalara saklama kapasiteleriyle dolayısıyla boyutlarıyla orantılı olarak bölüştürülmektedir. Son taşıyıcı dosyaya kadar olan taşıyıcı dosyalar için saklanacak verinin boyutu Eşitlik 1 ile hesaplanmaktadır.

$$B.K_i\ /K_{total} \tag{1}$$

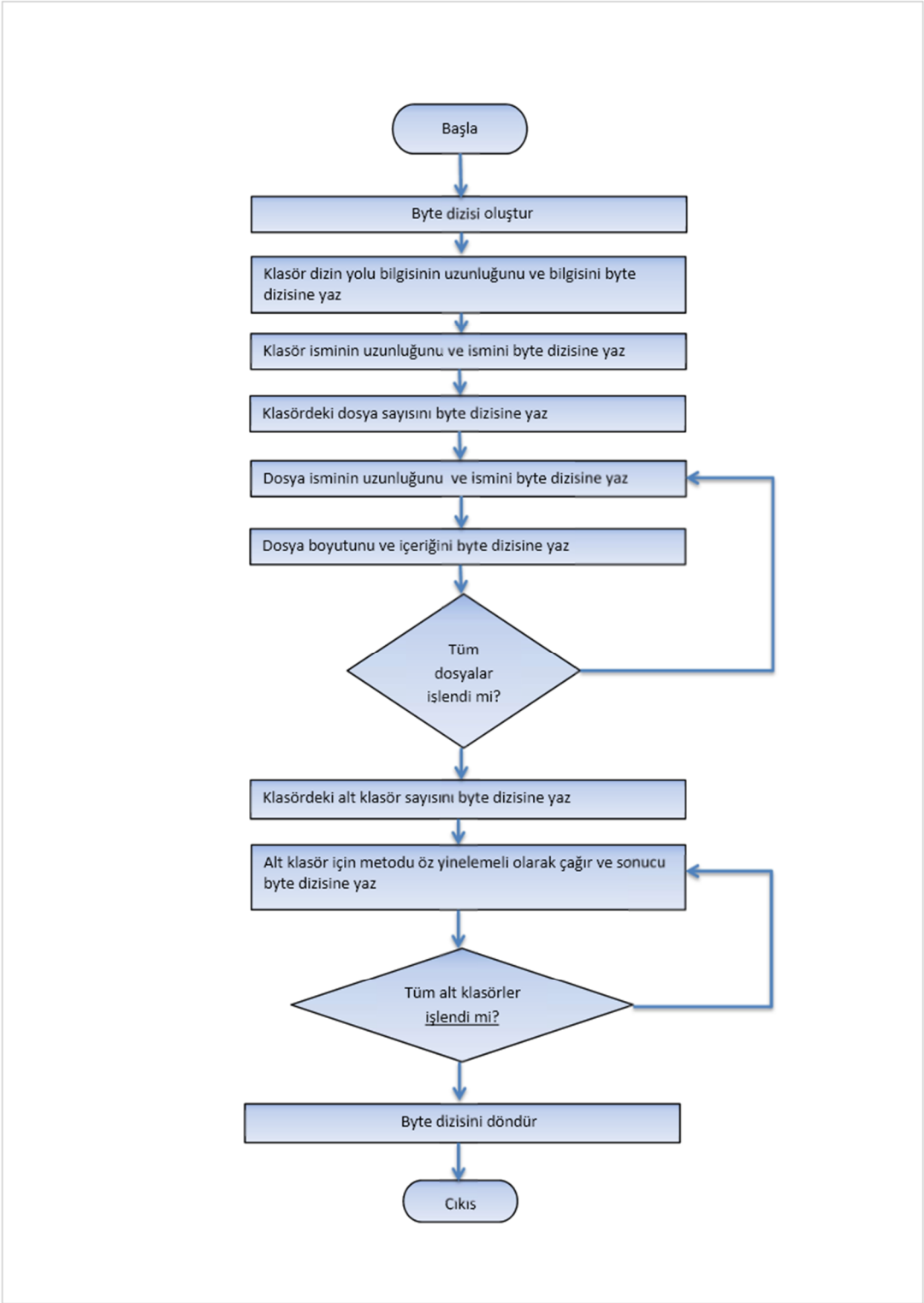
Bu eşitlikte B saklanacak ham verinin toplam boyutunu, K_i sıradaki taşıyıcı dosyanın saklama kapasitesini, K_{total} ise Eşitlik 2'de belirtildiği üzere taşıyıcı dosyaların toplam saklama kapasitesini göstermektedir.

$$K_{total} = \sum_{i=1}^{n} K_i \tag{2}$$

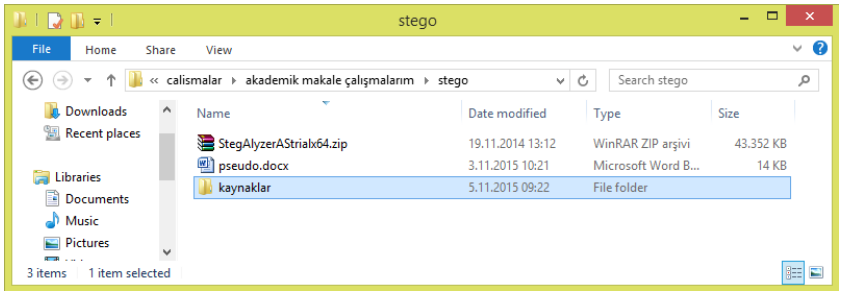
Buna ilişkin bir örnek Şekil 5'de sunulmaktadır. Bu örnekte saklanacak ham verinin (şifrelemiş halinin) toplam boyutu 500 byte, üç ayrı taşıyıcı WAV dosyalarının saklama kapasitelerinin ise sırasıyla 150, 250 ve 300 byte olduğu varsayılmaktadır. Bu durumda taşıyıcı dosyaların toplam saklama kapasitesi 700 byte olup veriyi saklamak için yeterlidir. Buna göre ilk dosya için saklanacak veri miktarı 500.150/700 = 107 byte olarak, ikinci dosya içinse 500.250/700 = 178 byte olarak hesaplanmaktadır. Son taşıyıcı dosyaya kadar 107 + 178 = 285 byte veri saklanmış olduğundan üçüncü dosyaya 500-285 = 215 byte veri saklanacaktır.



Şekil 2. Klasör kilitleme sistemi akış diyagramı (Work flow of folder lock system)



Şekil 3. Saklanacak içeriğin ham veriye dönüştürülmesi. (Transforming the content to be hidden into raw data)

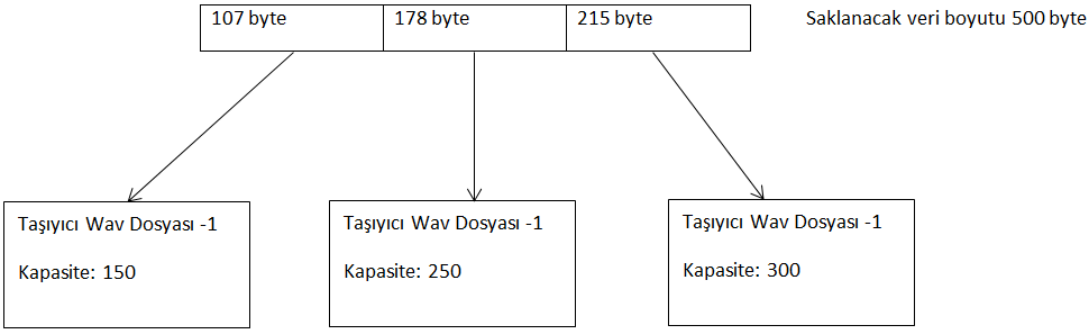


(a) Klasörün hiyerarşik yapısı (Hierarchical structure of folder)

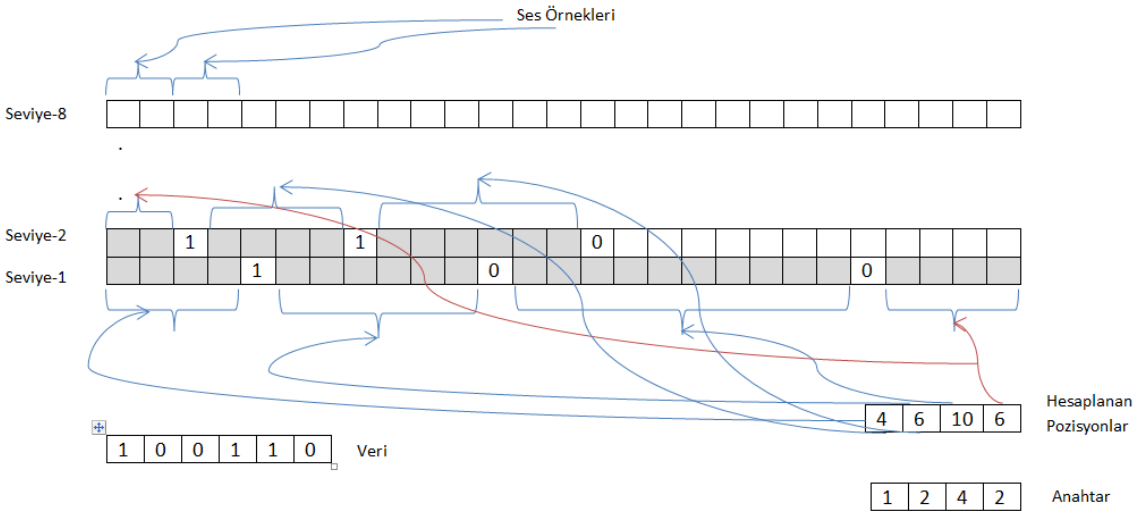
50	D:\doktora\calismalar \akademik makale çalışmalarım	5	stego	2	24	StegAlyzerAStrialx64.zip	44.391.656	Dosya içeriği	11	pseudo.docx	14.078	Dosya içeriği	1	....

(b) Byte dizisi içeriği (Byte array content)

Şekil 4. Saklanacak içeriğin ham veriye dönüştürülme örneği **(a)** klasörün hiyerarşik yapısı **(b)** byte dizisi içeriği (Example of transforming the content to be hidden into raw data **(a)** hierarchical structure of folder **(b)** byte array content)



Şekil 5. Saklanacak içeriğin taşıyıcı dosyalara bölüştürülmesi (Division of content into carrier files)



Şekil 6. Saklama işlemi (Hiding process)

Saklama işlemi öncesinde wavReader metotları kullanılarak taşıyıcı WAV dosyasının ses örneği oranı ve veri kısmına erişilmektedir. Saklama işleminde kullanılan anahtar değeri bir byte dizisidir. Saklanacak verinin okunan her biti, anahtardan okunan byte değeri kullanılarak Eşitlik 3'de hesaplanan ses örneği (audio sample) kadar atlanarak gelinen pozisyona gömülmektedir.

$$P = s.(anahtar[i]/k + 1) \quad (3)$$

Burada **s** wav dosyasından okunan ses örneği oranına göre 1 veya 2 byte değerini almakta, $\boldsymbol{anahtar[i]}$ anahtardan okunan sıradaki değeri, **k** veri saklama kapasitesini ayarlamada kullanılan katsayıyı ifade etmektedir. Saklama işleminde gömülmekten kasıt, belirlenen ses örneğinin en son bitinin saklanacak olan bite eşitlenmesidir. Anahtarda okunan byte değerleri bittiğinde, sıradaki saklanacak bitin saklanacağı pozisyonun bulunabilmesi için anahtardaki byte dizisinin başına dönülmektedir. En az önemli bit seviyesinde saklama yapılacak ses örneği kalmadığından bir üst bit seviyesine geçilerek aynı işlemler devam etmektedir. Bir ses örneğinin herhangi seviyedeki bir bitine sadece bir kez saklama yapılmaktadır. Ayrıca ses örneklerinin 4. LSB seviyesine kadar olan bitlerinin bazılarına veya tamamına veri saklanmış olabileceği gibi hiç veri saklanmamış ses örnekleri de olabilmektedir. Saklama işlemine ilişkin örnek gösterim Şekil 6' da sunulmaktadır. Veri saklama kapasitesinin artırılmasını ayarlamada bir **k** katsayısı kullanılmaktadır. Bu katsayı 1 ila 256 arasında değerler alabilmektedir. Veri saklanacak bir sonraki pozisyonun belirlenmesi anahtardan okunan sıradaki değerin bu katsayıya oranına bağlıdır. Katsayı değeri yükseldikçe saklama kapasitesi artırılmaktadır.

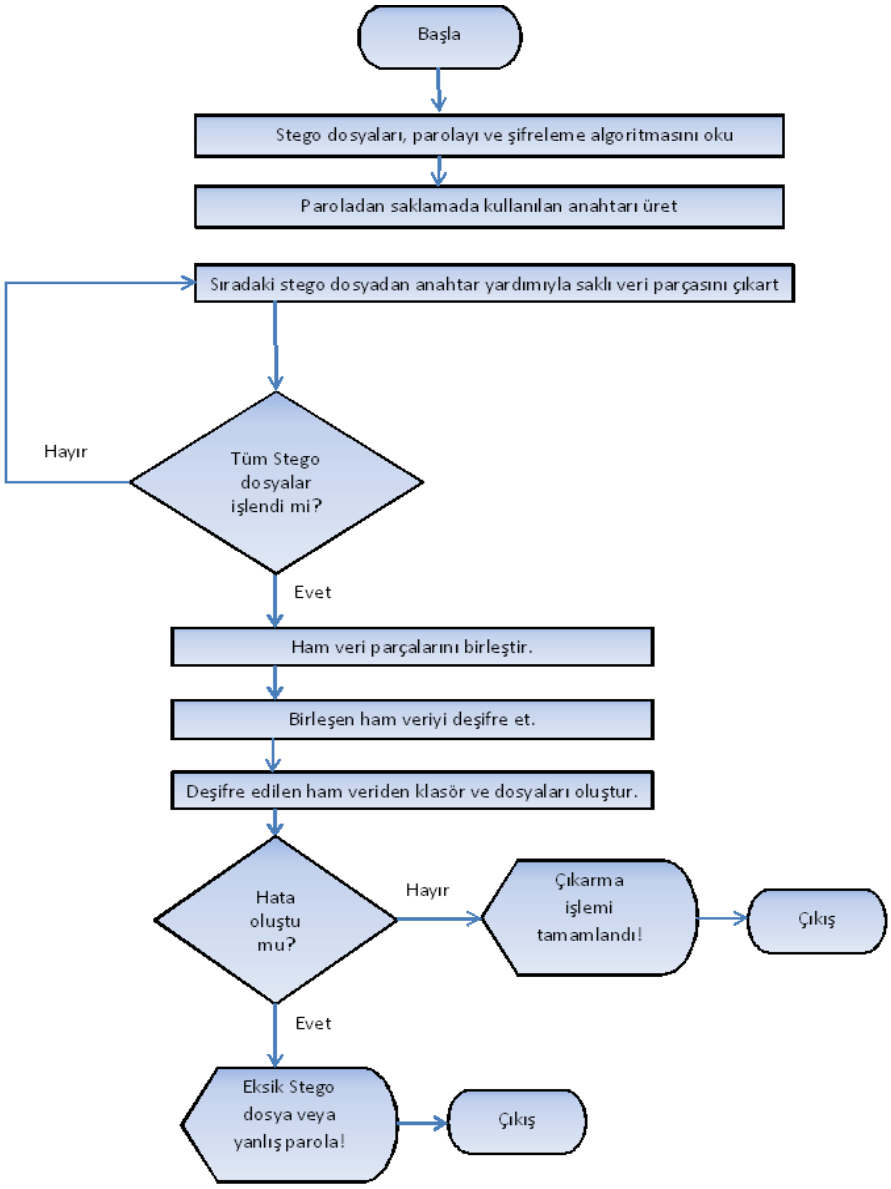
Şekil 6'da verilen örnekte k değeri 1 olarak alınmış taşıyıcı dosyanın ses örnekleri ise 2 byte olarak tespit edilmiştir. Bu örnekte anahtardan okunan ilk değer 1 dir. Eşitlik 3'e göre atlanacak pozisyon sayısı 2.(1/1 + 1) = 4 olarak hesaplanmıştır. Benzer işlemle diğer pozisyon bilgileri sırasıyla 6, 10 ve 6 olarak belirlenmiştir. Şekil 6'da koyu renkli kutucuklar bu değerler göre atlanan byte değerlerinin yerlerini göstermektedir. Saklanacak verinin 4. Bitine sıra geldiğinde 6 byte atlanması gerekmiş ancak en az önemli bit seviyesinde 4 byte veri kaldığından ikinci bit seviyesine çıkılarak 2 byte daha atlanmış ve sıradaki pozisyona veri saklanarak işleme ikinci bit seviyesinde devam edilmiştir. Hesaplanan pozisyon dizisinin sonuna gelindiğinde ise tekrar başa dönülerek veri saklama pozisyonları tespit edilmektedir.

İçerisinde veri saklı ses dosyalarından saklı klasörü geri getirme işlemi, klasör kilitleme işlemindeki aşamaların tersten yapılmasıyla gerçekleştirilmektedir. Geri getirme işleminin başarıyla sonuçlanması için saklama sonucu oluşan stego dosyalarının eksiksiz olması gerekir. Her bir stego dosyadan, paroladan oluşturulan anahtar yardımıyla saklı ham veri parçası çıkartılmakta, daha sonra ham veri parçaları birleştirilmekte ve şifreleme algoritmasına göre deşifre edilmektedir. Deşifre sonucu elde edilen byte dizisi kilitlenen klasör verisidir. Bu veriden klasör ve içeriği hiyerarşik bir şekilde tekrar oluşturulmaktadır. Bu işlem esnasında bir hata oluşması, stego dosyalarda eksik olması veya parolanın yanlış girilmesinden kaynaklanmaktadır. Klasörü geri getirme işlemine ait iş akış diyagramı Şekil 7'de verilmiştir. Bu çalışma kapsamında geliştirilen klasör kilitleme uygulaması, steganografi temelli olması sayesinde bilgisayarımız veya taşınabilir herhangi bir medya üzerinde yer alan ses dosyaları koleksiyonumuzun bitleri içerisinde işitsel açıdan fark oluşturmaksızın önemli ve kritik dosyalarımızın güvenli bir şekilde barındırılmasını sağlamaktadır. Klasör kilitleme uygulaması platform bağımsız bir programlama dili olan Java ile geliştirilmiştir. Dolayısıyla WAV dosyalarının çalıştırılabildiği tüm platformlarda kullanılabilecektir. Örneğin Windows ortamında harici bellek üzerindeki WAV dosyaları içerisine saklanan bir klasöre Linux ortamında tekrar erişilebilecektir. Klasik klasör kilitleme yazılımları işletim sistemi çekirdeğinin özelliklerini kullandığından klasörün gizlenmesi ve tekrar erişime açılması aynı işletim sisteminde gerçekleşebilir.

Steganografi tabanlı klasör kilitleme uygulaması başarı bir steganografi yazılımı için iki temel gereksinim olan saklama işleminin şeffaf bir şekilde gerçekleştirilip oluşan stego dosyalardaki farklılığın hissedilmemesi ve saklanan verinin tam ve düzgün bir şekilde tekrar geri getirilmesi gereksinimlerinin ikisini de karşılamaktadır. Oluşan stego müzik dosyaları dinlendiğinden orijinaliyle arasındaki fark anlaşılamamaktadır. Ayrıca yazılımın geri getirme modülü tam ve düzgün bir şekilde saklanan tüm dosyaları hiyerarşisine uygun bir şekilde geri getirebilmektedir. Steganografi uygulamalarının steganaliz ataklarına karşı dayanaklı olması gerekmektedir. Steganalizde amaç sadece saklanan veriyi ortaya çıkarmak değil, bir dosya içerisinde veri saklı olup olmadığını da anlamaktır. Veri saklama işleminin yapıldığı bit seviyesi arttıkça ses dosyası içerisine eklenen hata/gürültü yükü de artmaktadır. Bu durum steganografi uygulamalarında saklama kapasitesi ile istatistiksel steganalize dayanıklılık arasında ters orantı olduğunu göstermektedir. Ayrıca bir ses veya resim dosyasının en az öneme sahip bitlerine (LSB) ardışık bir şekilde veri saklama yöntemlerinin de steganalizde kullanılabilecek istatistiksel izler bıraktığı belirtilmektedir [27].

Geliştirilen steganografi tabanlı klasör kilitleme uygulaması klasörler ve dosyalar setini, WAV ses dosyaları setine şeffaf bir şekilde saklayabilmekte ve geri getirmektedir. Saklama işleminin yanı sıra AES, DES ve 3DES algoritmalarından birisiyle şifreleme imkânı da sunmaktadır.

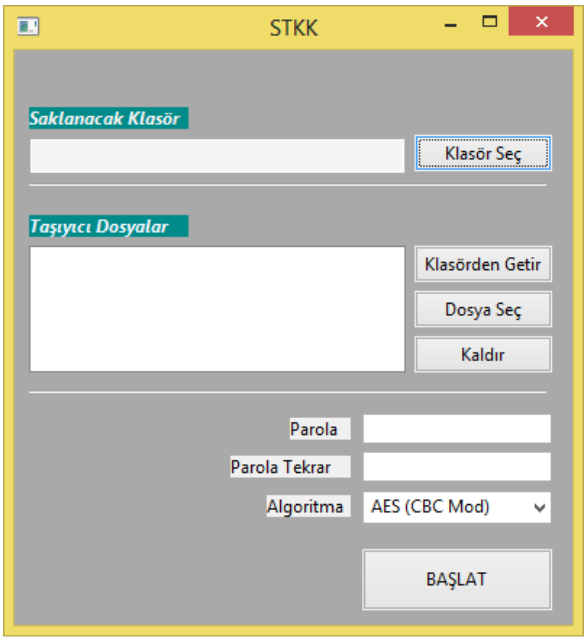
Saklama işlemini sadece bilgisayar üzerindeki değil, herhangi bir harici medya üzerindeki WAV dosyaları seti içerisine saklayabilmekte, saklanan klasörü de başka bir bilgisayar üzerinde geri getirebilmektedir.



Şekil 7. Geri getirme işlemi iş akış diyagramı (Extraction process work flow diagram)

Saklama işlemi sonrasında oluşan ses dosyaları diskteki boyut ve işitsel ses kalitesi yönüyle orijinalinden farksızdır. Yeterince ses dosyası olduğu müddetçe saklanacak verinin boyutunda herhangi bir sınırlama yoktur. Bu durum saklama kapasitesinin ayarlanması konusunda kullanıcıya esneklik sağlamaktadır. Hangi tipten olduğu fark etmeksizin her türlü dosya saklanabilmektedir. Belirlenen bir anahtar yardımıyla rastgele saklama yapılarak istatistiksel steganalize karşı dayanıklılık sağlanmaktadır. Saklama işleminin güvenliği saklama algoritmasının bilinmesine değil anahtar değerine bağlıdır.

Saklama işlemi sonrasında kullanım özelliğine göre saklanan verinin boyutu kadar alan diskten boşaltılmaktadır. Yani saklanan klasör disk monitör yazılımları tarafından saklı değil silinmiş olarak görülecektir. Saklama işlemi sonrasında saklanan klasör ve dosyaları işletim sisteminin arama araçları kullanarak bulmak mümkün değildir. Şekil 8'de geliştirilen yazılımın ekran görüntüsü verilmiştir. Şekil 8'de girilen bilgilere göre Şekil 2'de verilen iş akışı çalıştırılarak klasör kilitleme işlemi gerçekleştirilmektedir. Bu çalışmada farklı güvenlik yazılımları da incelenmiştir. Bunlardan ilki Steganos Safe [31] uygulamasıdır. Bu uygulama şifre ile açılabilen güvenli bir sürücü oluşturarak içerisine önemli verinin saklanmasını sağlamaktadır. Oluşturulan sürücünün video, ses veya çalıştırılabilir bir dosya içerisine saklanma özelliği de mevcuttur. Ancak bu saklama işlemi steganografik bir teknik olmayıp ses veya video dosyasının sonuna eklenmesi şeklinde gerçekleştirilmektedir. Steganos Crypt&Hide modülü [32] ise bir klasörün sadece bir tek taşıyıcı dosya içerisine steganografik yöntemle arşivlenerek yedeklenmesini gerçekleştirmekte, mevcut klasöre erişim devam etmektedir.



Şekil 8. Geliştirilen stego tabanlı klasör kilitleme yazılımı ara yüzü (Interface of the developed stego based folder lock software)

QuickCrypto [33] yazılımı ise bir klasörü saklamak yerine bir klasör içerisindeki dosyaları topluca saklama özelliğine sahiptir. Ancak içerisindeki dosyalar saklandıktan sonra içi boş görünen klasörün özellikleri incelendiğinde boyutu değişmemektedir. Yazılımın stego modülünde [34] ise tek bir taşıyıcı dosya içerisine tek bir dosya saklanması gerçekleştirilmektedir. FolderGuard [35] yazılımı belirlenen bir klasörü tüm içeriğiyle saklayabilmektedir. Klasör sanal olarak Windows Explorer, MS-DOS gibi programlardan saklanmaktadır. Ancak saklama işleminden sonra klasörün yer aldığı sürücü özellikleri incelendiğinde kullanılan alan boyutu değişmemektedir. Saklama yöntemi olarak steganografi tekniği kullanılmamaktadır.

GiliSoft File Lock Pro [36] yazılımı bir klasörü veya dosyaları kullanıcı ve programlardan saklayabilmektedir. Bir klasörün içindeki bir dosya saklandıktan sonra klasörün özellikleri incelendiğinde klasör boyutunda saklanan dosya boyutu kadar azalma olduğu görülmektedir. Ancak saklama işleminden sonra klasörün yer aldığı sürücü özellikleri incelendiğinde kullanılan alan boyutu değişmemektedir. Saklama yöntemi olarak steganografi tekniği kullanılmamaktadır.

Steganografi alanında çoğu ücretsiz birçok yazılım geliştirilmiştir. Bunlardan bazılarına ve yukarıda bahsedilen yazılımlara ilişkin özellikleri içeren karşılaştırma tablosu Tablo 2'de verilmiştir:

Tablo 2. STKK yazılımının mevcut yazılımlarla karşılaştırılması (Comparison of STKK software against available ones)

Kaynak	Uygulama	Taşıyıcı dosya türü	Saklanan dosya türü	Dosya setine saklama özelliği	Saklama kapasitesi	Steganografi tekniği kullanımı	Klasör saklama özelliği
[37]	OpenPuff	Bmp, jpg, pcx, png, tga, aiff, mp3, wav vb.	Hepsi	Var	256 mb.	Uygulanıyor	Yok
[38]	Mp3stego	mp3	Metin	Yok	taşıyıcı boyutuyla sınırlı	Uygulanıyor	Yok
[33]	QuickCrypto	N/A	Hepsi	N/A	N/A	Uygulanmıyor	Yok
[32]	Steganos Crypt&Hide	Jpeg, bmp, wav	Hepsi	Yok	taşıyıcı boyutuyla sınırlı	Uygulanıyor	Yok
[39]	stegHide	jpg, bmp, wav,au	Hepsi	Yok	taşıyıcı boyutuyla sınırlı	Uygulanıyor	Yok
[40]	Invisible Secrets	Jpg,png,bmp,html,wav	Hepsi	Yok	taşıyıcı boyutuyla sınırlı	Uygulanıyor	Yok
[31]	Steganos Safe	Mp3,m4a, avi, wmv, exe	Hepsi	Yok	taşıyıcı boyutuyla sınırlı	Uygulanmıyor	Var
[34]	QuickCrypto (Stego)	Bmp, jpeg, gif, wav, mp3	Hepsi	Yok	taşıyıcı boyutuyla sınırlı	Uygulanıyor	Yok
[36]	GiliSoft File Lock Pro	N/A	Hepsi	N/A	N/A	Uygulanmıyor	Var
[35]	Folder Guard	N/A	Hepsi	N/A	N/A	Uygulanmıyor	Var
	STKK (Önerilen Yaklaşım)	Wav	Hepsi	Var	Taşıyıcı dosyaların toplam boyutuyla sınırlı	Uygulanıyor	Var

4. ÖNERİLEN YAKLAŞIMIN DEĞERLENDİRİLMESİ (EVALUATION OF PROPOSED APPROACH)

Ses içerisine veri saklamada kullanılan steganografi tekniklerinin sağladığı fark edilemezlik özelliğinin performansı SNR (Signal-to-Noise Ratio) değerleriyle ölçülebilmektedir [41]. SNR değerinin hesaplanması Eşitlik 4'de gösterilmiştir [41-42]. Bu formülde $S_s(m,n)$ stego ses dosyası sinyalini, $S_c(m,n)$ taşıyıcı ses dosyası sinyalini ifade etmektedir. SNR değerinin 30 dB veya yukarı olması ses dosyası kalitesinin bozulmadığı anlamına gelmektedir [41].

$$SNR_{dB} = 10*\log_{10}\left(\frac{\sum_{n=1}^{N}(|Sc(m,n)|^2)}{\sum_{n=1}^{N}(|Sc(m,n)-Ss(m,n)|^2)}\right) \quad (4)$$

Ses steganografi veya filigran tekniklerinin sağladığı fark edilemezlik özelliğinin performansının ölçülmesinde PSNR (Peak Signal-to-Noise Ratio) değeri de kullanılmaktadır [20, 42-43]. PSNR değerinin hesaplanması Eşitlik 5'de gösterilmiştir [42]. PSNR değerinin hesaplanmasında saklama sonucu oluşan hataların kareleri toplamının ortalaması yani MSE (Mean Squared Error) değeri kullanılmakta olup Eşitlik 6'de gösterilmiştir [42].

$$PSNR = 10*\log_{10}(\frac{65535}{MSE}) \quad (5)$$

$$MSE = \frac{(\sum_{m=1}^{M}\sum_{n=1}^{N}[Sc(m,n)-Ss(m,n)]^2)}{M*N} \quad (6)$$

PSNR değerinin yüksek olması sesin kalitesinin korunması anlamına gelmektedir [43]. Önerilen tekniğin müzik dosyası içerisine veri saklama kapasitesinin yaklaşık değeri Eşitlik 7'de gösterilmiştir. Bu eşitlikte B, wav dosyasının veri alanının byte cinsinden boyutunu, S, veri saklanan toplam LSB seviye sayısını, s, wav dosyası ses örneğindeki byte sayısını, k, veri saklama kapasitesinin artırılmasını ayarlamada kullanılan katsayıyı, anahtar [i] değeri ise anahtarı oluşturan byte dizisindeki her bir byte değerini ifade etmektedir.

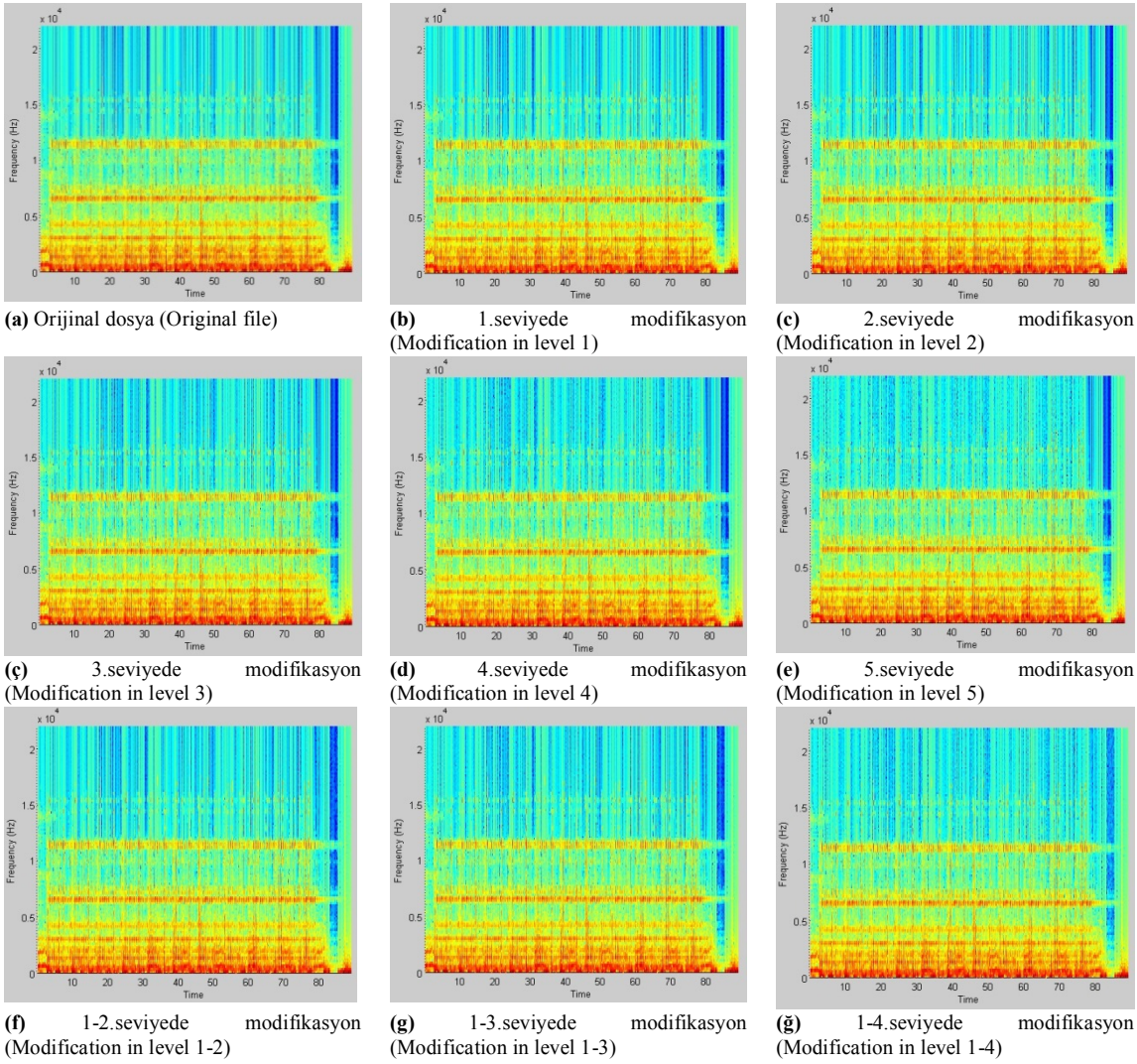
$$K = \frac{B*S}{s*\sum_{i=1}^{n}(anahtar[i]/k+1)} \quad (7)$$

Bu çalışmada k katsayısının değeri 80 olarak belirlenmiştir. Anahtar dizisindeki byte değerleri 0 ile 255 arasında değişebilmektedir. Bu durumda veri saklanan iki ses örneği arasındaki mesafe 1 ile 4 arasında bir değer olacaktır. Yapılan çalışmada 16 bitlik stereo WAV dosyalarına ait ses örneklerinin her bir bit seviyesinde veri saklanması ve 2 ile 8. bit seviyeleri için birikmiş veri saklanması ayrı ayrı test edilerek dosyada oluşan değişimler incelenmiştir. Ses örneklerinin 1. Seviye ile 9. Seviye arasındaki tüm bit seviyelerine ayrı ayrı yapılan saklama işlemi ile 2. seviye ve 8. seviye arasındaki seviyeler için birikmiş veri saklanması işitsel olarak fark edilebilir bir gürültü oluşturmamıştır. Wav dosyası içerisinde farklı ses seviyeleri için ayrı ayrı ve birikmiş veri saklaması sonucu oluşan stego dosyalara ilişkin SNR ve PSNR değerleriyle, saklama kapasitesinin saniye başına kilo bit değeri Tablo 3'de gösterilmiştir. SNR değerleri incelendiğinde stereo wav formatındaki müzik dosyalarının LSB 1. Seviye ile 4. Seviye arasındaki bitlerine ayrı ayrı veya kümülatif olarak sesin kalitesi korunarak veri saklanabilmektedir. Veri saklama seviyesi yükseldikçe PSNR değerleri artmakta, oluşan stego ses dosyasının taşıyıcı ses dosyası ile benzerliği azalmaktadır. Sadece bir bit seviyesine veri saklandığında 35,36 kbps saklama kapasitesi oluşmaktadır. Kullanılan wav dosyası 16 bitlik ses örneklerinden oluşan 44,1 KHz ses örneği oranına sahip stereo müzik dosyasıdır. Ses örneklerinin tamamına ardışık veri saklanması durumunda saklama kapasitesi 44,1 kbps olacaktır. Ancak ardışık saklama yerine belirli bir anahtara göre rastgele saklama yapıldığından bu kapasite 35, 6 kbps olmuştur. Tablo 3'deki SNR ve PSNR değerleri incelendiğinde belirli bir bit seviyesine yapılan saklama sonucu oluşan stego dosyanın kalitesi, bu bit seviyesinin bir altındaki bit seviyesine yapılan birikmiş saklama sonucu oluşan stego dosyanın kalitesinden düşük olduğu görülmektedir.

Tablo 3. Stego dosyaların SNR, PSNR ve saklama kapasitesi değerleri (SNR, PNR and hiding capacity values of stego files)

Saklanan Bit Seviyesi	SNR	PSNR	Saklama kapasitesi (kbps)
LSB-1	**51,8823**	52,0369	35,36
LSB-2	**45,8594**	46,0136	35,36
LSB-3	**39,8404**	39,9948	35,36
LSB-4	**33,8174**	33,9719	35,36
LSB-5	27,7955	27,9500	35,36
LSB-6	21,7758	21,9304	35,36
LSB-7	15,7502	15,9048	35,36
LSB-8	9,7315	9,8860	35,36
LSB-9	6,7199	6,8745	35,36
LSB-1-2	**44,3208**	44,4754	80,72
LSB-1-3	**40,0334**	40,1879	102,12
LSB-1-4	**32,0571**	32,2116	161,12
LSB-1-5	26,8650	27,0196	192,20
LSB-1-6	21,1303	21,2849	229,85
LSB-1-7	16,0506	16,2052	262,27
LSB-1-8	9,0247	9,1792	314,65

Örneğin sadece 5. bit seviyesinde saklama yapıldığından oluşan SNR ve PSNR değerleri sırasıyla 27,7955 ve 27,9500 iken 1.seviye ile 4.seviye arasındaki tüm seviyelere veri saklandığından bu değerler 32,0571 ve 32,2116 olmuştur. Yani sadece 5. bit seviyesine veri saklandığında ses kalitesi kabul edilebilir SNR değerinin altına düşerken, PSNR değerinin daha



(a) Orijinal dosya (Original file) **(b)** 1.seviyede modifikasyon (Modification in level 1) **(c)** 2.seviyede modifikasyon (Modification in level 2)

(ç) 3.seviyede modifikasyon (Modification in level 3) **(d)** 4.seviyede modifikasyon (Modification in level 4) **(e)** 5.seviyede modifikasyon (Modification in level 5)

(f) 1-2.seviyede modifikasyon (Modification in level 1-2) **(g)** 1-3.seviyede modifikasyon (Modification in level 1-3) **(ğ)** 1-4.seviyede modifikasyon (Modification in level 1-4)

Şekil 9. Stego ses dosyalarının spektrogram grafikleri (a) Taşıyıcı dosya (b) En az önemli bit seviyesinde veri saklı stego dosya (c) 2.seviyede modifikasyon (ç) 3.seviyede modifikasyon (d) 4.seviyede modifikasyon (e) 5.seviyede modifikasyon (f) 1-2.seviyede modifikasyon (g) 1-3.seviyede modifikasyon (ğ) 1-4.seviyede modifikasyon (Spectrograms of stego audio files (a) Carrier file (b) Stego file that data hidden in least siginificant bit (c) Modification in level 2 (ç) Modification in level 3 (d) Modification in level 4 (e) Modification in level 5 (f) Modification in level 1-2 (g) Modification in level 1-3 (ğ) Modification in level 1-4)

düşük olmasıyla da oluşan stego dosyanın taşıyıcı ses dosyasıyla benzerliği azalmıştır. Bu durum beklenen bir sonuçtur. Çünkü herhangi bir bit seviyesine kadar kümülatif saklama yapıldığında ses örneğindeki tüm bitler değişse bile oluşan toplam değişim bir üst seviyedeki tek bir bit değişiminden bir eksik olmaktadır. Buna ilişkin gösterim Eşitlik 8'de verilmiştir.

$$2^{n+1} = 1 + \sum_1^n 2^n \quad (8)$$

Ses içerisine veri saklamada kullanılan steganografi tekniklerinin sağladığı fark edilemezlik özelliğinin performansı spektrogram grafikleri yardımıyla da değerlendirilebilmektedir [25, 44]. Spektrogram sinyalin spektral yoğunluğunun zamana göre değişimini göstermekte olup resim halinde bu değişikliği ifade etmektedir. Spektrogram grafikleri müzik, konuşma işleme, sismoloji gibi değişik alanlarda analiz amacıyla kullanılmaktadır. [44]. Spektrogram resimlerinde oluşan değişimler steganalizde kullanılmaktadır [25]. Şekil 9'da orijinal ses dosyasına ve 1. seviyede veri saklama sonucu oluşan stego ses dosyasına ait spektrogram grafikleri verilmiş olup bu grafiklerde belirgin bir farklılık gözlenmemektedir. Ayrıca diğer bit seviyelerine yapılan farklı saklama işlemleri sonucu oluşan stego dosyaların spektrogramları da gösterilmektedir. Spektrogram grafikleri incelendiğinde 5. seviyede veri saklanması sonucu fark edilir değişiklikler oluşmaya başlanmıştır. 1-4. Seviyeler arasındaki tüm bitlere yapılan birikmiş saklama sonucu da spektrogram bozulmaları grafiğin üst kısmındaki mavi bölgelerden fark edilmektedir.

5. SONUÇLAR (CONCLUSIONS)

Bu çalışmada steganografik yaklaşımlar incelenmiş, sunulan çalışmalar karşılaştırılmış, steganografi yaklaşımı kullanılarak daha yüksek güvenliği sağlamak amacıyla klasör kilitleme uygulaması geliştirilmiş ve bunun nasıl geliştirilebileceği detaylı olarak açıklanmıştır. 16 bitlik ses örneklerinden oluşan WAV formatındaki ses dosyalarının steganografide veri saklama amacıyla kullanılabileceği ve yüksek saklama kapasitesi sunabileceği anlaşılmıştır. Geliştirilen uygulamada bir anahtar yardımıyla belirlenen WAV dosyası seti içerisine LSB modifikasyonu yöntemiyle rastgele saklama gerçekleştirilmiştir. Belirli bir anahtara göre saklama işlemi ile güvenliği algoritmanın bilinmesinden bağımsız hale getirmiş, rastgele saklama yapmasıyla ise istatistiksel steganaliz ataklarına karşı dayanıklılık sağlamıştır. Birden fazla WAV dosyası içerisine saklama yapabilmesiyle de rastgele saklamanın getirdiği saklama kapasitesi sorununa dolaylı bir çözüm sunmuştur. Spektrogram grafikleri ve SNR değerleri incelendiğinde stereo WAV formatındaki müzik dosyalarının 1.seviye ile 3.seviye arasındaki tüm bitlerine birikmiş olarak 100 kbps civarında kapasite ile veri saklanabileceği görülmüştür. Mevcut yazılımlar incelendiğinde, normal klasör kilitleme yazılımları, klasörü saklandığı diskten aslında silmemekte sadece kullanıcıya görme ve erişme iznini kısıtlamaktadır. Dolayısıyla saklı klasörün boyutu kullanıcıya görünmediği halde kullanılan disk miktarının içerisinde yer alacaktır. Ancak steganografik tabanlı geliştirilen uygulamada saklanacak klasör, bilgisayarın kendi diskindeki veya harici bir diskteki ses dosyalarına saklanacak ve silinecektir. Böylece disk üzerinde hem görünmeyip hem de yer kaplayan bir veri yer almamaktadır.

Klasör kilitleme yazılımlarında saklanacak klasör, özel bir klasör içine taşınmakta ve bu durum bazı saklanmış klasörler olduğunu belli etmektedir. Ancak önerilen uygulamada bilgisayar üzerinde saklı bir klasör olduğunun farkında olunmamaktadır. Yani steganografinin gücü sayesinde klasör kilitleme yazılımlarına ilave güvenlik sağlanmıştır. Geliştirilen yazılım mevcut çalışmalarla karşılaştırılmış ve Tablo 2'de sonuçları verilmiştir. Yapılan karşılaştırmada sunulan çalışmanın şu an için "wav" dosyalarıyla sınırlı olması bir dezavantaj gibi görünse de diğer özelliklerde daha iyi sonuçlar sunduğu görülmüştür. Ayrıca AES, DES ve 3DES gibi şifreleme özelliklerinin de geliştirilen yazılıma eklenmesiyle ekstra bir güvenlik sağlanmıştır.

Sonuç olarak sunulan yaklaşımda hem steganografik hem de kriptografik yaklaşımların birleştirilmesiyle yüksek seviyede güvenlik sağlayacak bir kişisel güvenlik çözümü sunulmuştur. Çalışmanın sonraki aşamasında steganografi tabanlı klasör kilitleme uygulaması saklama işlemi sonucu oluşacak değişimi azaltmaya yönelik en iyileme (optimizasyon) yapılarak daha güvenli hale getirilecektir. Ayrıca taşıyıcı dosya çeşitliliği artırılarak uygulamanın saklama kapasitesinin artması sağlanacaktır.

KAYNAKLAR (REFERENCES)

1. Sağıroğlu, Ş. ve Alkan, M., "Her Yönüyle Elektronik İmza (e-İmza)", Grafiker, Ankara, 2005.
2. Johnson, N.F. ve Jajodia, S., "Exploring steganography: Seeing the unseen", **Computer**, Cilt 31, No 2, 26-34, 1998.
3. Adli, A. ve Nakao, Z., "Three steganography algorithms for MIDI files", **Fourth International Conference on Machine Learning and Cybernetics,** Guangzhou, China, 2401-2404, 18-21 Ağustos 2005.
4. Akleylek, S. ve Nuriyev, U., "Steganography and new implementation of steganography", **Signal Processing and Communications Applications Conference,** Kayseri, TURKEY, 64-67, 16-18 Mayıs 2005.
5. Bender, W., Gruhl, D., Morimoto, N. ve Lu, A., "Techniques for data hiding", **IBM Syst. J.,** Cilt 35, No 3-4, 313-336, 1996.
6. Brisbane, G., Safavi-Naini, R. and Ogunbona, P., "High-capacity steganography using a shared colour palette", **IEE Proc.-Vis. Image Signal Process.,** Cilt 152, No 6, 787-792, 2005.
7. Gopalan, K., "Audio steganograph using bit modification" , **International Conference on Multimedia and Expo,** Baltimore, Maryland, 629-632, 6-9 Temmuz 2003.
8. Lee, Y.K. ve Chen, L.H., "High capacity image steganographic model", **Vision, Image and Signal Processing, IEE Proceedings-,** Cilt 147, No 3, 288-294, 2000.
9. Niimi, M., Noda, H., Kawaguchi, E. ve Eason, R.O., "High capacity and secure digital steganography to palette-based images", **International Conference on Image Processing**, Rochester, New York, USA, II-917-II-920, 22-25 Eylül 2002.
10. Noda, H., Spaulding, J., Shirazi, M.N. ve Kawaguchi, E., "Application of bit-plane decomposition steganography to JPEG2000 encoded images" **IEEE Signal Processing Letters,** Cilt 9, No 12, 410-413, 2002.
11. Sağıroğlu, Ş. ve Tunckanat, M., "A Secure Internet Communication Tool", **Turkish Journal of Telecommunications,** Cilt 1, No 1, 40-46, 2002.
12. Yan, D., Wang, R., Yu, X. ve Zhu, J., "Steganography for MP3 audio by exploiting the rule of window switching" **Computers & Security,** Cilt 31, No 5, 704-716, 2012.
13. Sui, X.G. ve Luo, H., "A new steganography method based on hypertext" **Asia-Pacific Radio Science Conference,** Qingdao, China, 181-184, 24-27 Ağustos 2004.
14. Swanson, M.D., Zhu, B. ve Tewfik, A.H., "Robust Data Hiding For Images", **Digital Signal**

Processing Workshop, Loen Norway, 37-40, 1-4 Eylül 1996.

15. Tseng, H.W. ve Chang, C.C., "Steganography using JPEG-compressed images" **International Conference on Computer and Information Technology,** Wuhan, China, 12-17, 14-16 Eylül 2004.

16. Habib, S., Parveen, A. ve Sarwar, S., "Secure Communication of Secret Data Using Steganography", **International Journal of Computer Science and Mobile Computing,** Cilt 2, No 5, 249-254, 2013.

17. Chou, J., Ramchandran, K. ve Ortega, A., "High capacity audio data hiding for noisy channels", **International Conference on Information Technology: Coding and Computing,** Las Vegas, NV, 108-112, 2-4 Nisan 2001.

18. Cvejic, N. ve Seppanen, T., "Increasing the capacity of LSB-based audio steganography", **IEEE Workshop on Multimedia Signal Processing,** St. Thomas, Virgin Islands, USA, 336-338, 9-11 Aralık 2002.

19. Rekik, S., Guerchi, D., Selouani, S. ve Hamam, H., "Speech steganography using wavelet and Fourier transforms" **EURASIP Journal on Audio, Speech and Music Processing,** Cilt 2012, No 1, 1-14, 2012.

20. Taruna ve Jain, R., "Message Guided Adaptive Random Audio Steganography Using LSB Modification", **International Journal of Computer Applications,** Cilt 86, No 7, 6-9, 2014.

21. Ozer, H., Sankur, B., Memon, N. ve Avcıbaş, İ., "Detection Of Audio Covert Channels Using Statistical Footprints Of Hidden Messages.", **Digital Signal Processing,** Cilt 16, No 4, 389-401, 2006.

22. Ru, X., Zhuang, Y. ve Wu, F., "Audio Steganalysis Based On 'Negative Resonance Phenomenon' Caused By Steganographic Tools.", **Journal of Zhejiang University Science A,** Cilt 7, No 4, 577-583, 2006.

23. Avcıbaş, İ., "Audio Steganalysis With Content Independent Distortion Measures", **IEEE Signal Processing Letters**, Cilt 13, No 2, 92-95, 2006.

24. Yavanoglu, U., Ozcakmak, B. ve Milletsever, O., "A New Intelligent Steganalysis Method for Waveform Audio Files", **International Conference on Machine Learning and Applications**, Boca Raton, FL, 233-239, 12-15 Aralık 2012.

25. Arslan, Y. ve Yalman, Y., "Visual Steganalysis of LSB-encoded Audio Data Based on Frequency Domain Characteristics", **International Conference on Security of Information and Networks,** Aksaray, Turkey, 359-362, 26-28 Kasım 2013.

26. Amin, M.M., Salleh, M., Ibrahim, S., Katmin, M.R. ve Shamsuddin, M.Z.I., "Information hiding using steganography", **4th National Conference on Telecommunication Technology,** Shah Alam, MALAYSIA, 21-25, 14-15 Ocak 2003.

27. Adhiya, K. P. ve Patil, S. A., "Hiding Text in Audio Using LSB Based Steganography", **Information & Knowledge Management,** Cilt 2, No 3, 8-14, 2012.

28. Meghanathan, N. ve Nayak, L., " Steganalysis Algorithms for Detecting the Hidden Information in Image, Audio and Video Cover Media", **International Journal of Network Security & Its Application (IJNSA)**, Cilt 2, No 1, 43-55, 2010.

29. Kessler, G.C., "An Overview of Steganography for the Computer Forensics Examiner", **Forensic Science Communications** , Cilt 6, No 3, 1-29, 2004.

30. İnternet: WAVE PCM soundfile format, https://ccrma.stanford.edu/courses/422/projects/WaveFormat/, 2014.

31. İnternet: Steganos, https://www.steganos.com/us/products/data-security/safe/features/, 2014.

32. İnternet: Steganos, https://www.steganos.com/us/products/data-security/privacy-suite/features/, 2014.

33. İnternet: Quickcrypto, http://quickcrypto.com/index.htm, 2014.

34. İnternet: Quickcrypto Steganography Software, http://quickcrypto.com/steganography-software.html, 2014.

35. İnternet: Winability, http://www.winability.com/folderguard/, 2014.

36. İnternet: Gilisoft, http://www.gilisoft.com/product-file-lock-pro.htm, 2014.

37. İnternet: OpenPuff, http://embeddedsw.net/OpenPuff_Steganography_Home.html, 2014.

38. İnternet: Mp3stego, http://www.petitcolas.net/steganography/mp3stego/, 2014.

39. İnternet: Steghide, http://steghide.sourceforge.net/, 2014.

40. İnternet: Invisiblesecrets Steganography Software, http://www.invisiblesecrets.com/steganography-software.html, 2014.

41. Djebbar, F., Ayad, B., Meraim, K.A. ve Hamam, H., "Comparative study of digital audio steganography techniques", **EURASIP Journal on Audio, Speech, and Music Processing,** Cilt 2012, No 1, 1-16, 2012.

42. Khan, S., Said, U., Ahmad, E., Ali, F. ve Ali, M., "The Effect of Various Number of Least Significant Bits substitution in Audio using Discrete Cosine Transform", **IJCSI**

International Journal of Computer Science, Cilt 10, No 4, 298-302, 2013.

43. Karthigaikumar, P., Kirubavathy, K.J. ve Baskaran, K., " FPGA based audio watermarking-Covert communication ", **Microelectronics Journal,** Cilt 42, No 5, 778-784, 2011.

44. Hussain, I., " A novel approach of audio watermarking based on S -box transformation ", **Mathematical and Computer Modelling,** Cilt 57, No 3-4, 963-969, 2013.