Düzce Üniversitesi
Bilim ve Teknoloji Dergisi

Araştırma Makalesi

Gizlilik Paylaşımı Yöntemini Kullanan Ses Dosyası Arşivleme Programı

Ersan YAZAN[a,*], Yetkin TATAR[b]

[a]*Bilgisayar Teknolojileri Bölümü, Besni Meslek Yüksekokulu, Adıyaman Üniversitesi, Adıyaman, TÜRKİYE*
[b]*Bilgisayar Mühendisliği Bölümü, Mühendislik Fakültesi, Fırat Üniversitesi, Elazığ, TÜRKİYE*
** Sorumlu yazarın e-posta adresi:eyazan@adiyaman.edu.tr*

ÖZET

Günümüz dünyasında her sektörde sayısal teknoloji ürünlerinin kullanımı hızla yaygınlaşmaktadır. Bunlardan birisi de sayısal ses iletişim teknolojisidir. Gerek kaydedilmesi gerekse iletişim sürecinde analog sistemlere göre önemli üstünlüğü olan bu teknolojide, tedbir alınmazsa sayısal ses dosyalarının dinleme, değiştirme, ekleme v.b saldırılara karşı savunmasız olduğu da bilinmektedir. Bu bildiride sayısal seslerin arşivlenip sonradan tekrar dinlenmesi gereken uygulamalarda kullanılabilecek bir yazılımsal aracın geliştirilme süreci açıklanmıştır. Yazılımsal araçta, orijinal ses dosyasının şifrelenip arşivlenmesi yerine, Shamir'in gizlilik paylaşım yöntemine dayanarak orijinal ses dosyasından elde edilen pay dosyalarının arşivlenmesi sağlanmıştır. Böylece hem dosyaların gizliliği korunmuş olup hem de tek bir kişinin yerine birkaç yetkilendirilmiş kişinin bir araya gelmesiyle dinleme işleminin gerçekleştirilmesine olanak sağlanmıştır. Ayrıca tek bir pay dosyasının kaybolması durumunda bile orijinal ses dosyasının yeniden elde edilmesi mümkündür. Yazılımsal araç, dinleme teşebbüslerini ve dinleme kayıtlarını tutabilmekte olup bu konudaki ihtiyacı giderecek şekilde tasarlanmış ve test edilmiştir.

Anahtar Kelimeler: *Gizlilik paylaşımı, Ses şifreleme, Güvenli ses dosyası arşivleme*

Audio File Archiving Program Which Uses Secret Sharing Method

ABSTRACT

In today's world, the use of digital technology products is becoming increasingly common in all sectors. One of them is the digital audio transmission technology. In this technology, which has more significant advantages than analog systems, digital audio files are vulnerable to threats of listening, changing, adding and so on if necessary precautions are not taken. In this paper, the process of developing a software tool to be used in applications when there is a need to re-listen archived digital audio files was explained. By the software tool, instead of encrypting and archiving the original audio files, archiving of share files derived from the original audio file based on Shamir's secret sharing method is provided. Thus, not only the privacy of files is protected, but also instead of a single person, a few authorized persons gather to make it possible to develop listening process. Also, in case of loss of a single share file, the original file audio file can be recovered. The software tool was designed and tested in a way that it can meet the needs of keeping listening attempt and listening.

Keywords: *Secret sharing, Audio encryption, Secure audio file archiving*

Geliş: 12/11/2015, Düzeltme:27/12/2015, Kabul: 02/02/2016

I. GİRİŞ

SAYISAL teknolojinin gelişmesiyle birlikte insanların günlük hayatlarını kolaylaştıracak birçok teknolojik aygıtın her alanda kullanıma girmesi sonucu; üretilen, saklanan ve iletilen veri miktarı da hızla artmaktadır. Ancak bu durum gerek sabit haldeki gerekse iletim halindeki metin, görüntü, ses gibi sayısal verilerin güvenliği ile ilgili sorunu da beraberinde getirmektedir. Veri güvenliği, gerek durağan haldeki gerekse iletim halindeki verilerin gizlilik, bütünlük ve erişilebilirliğinin garantili bir şekilde gerçekleştirilmesi olarak tarif edilebilir. Bu alanda geliştirilen tekniklerin bir kısmı verinin istenmeyen kişilerin eline geçmesini engellemeye yönelik olmakla birlikte, kriptografi gibi verinin içeriğinin gizlenmesine yönelik çalışmalar da mevcuttur. Verinin içeriğinin gizlenmesinde kullanılan birçok kriptografik yöntem geliştirilmiştir ve bu konuda yapılan çalışmalar halen devam etmektedir. Bu alanda geliştirilen tekniklerden bir tanesi de Gizlilik Paylaşımı Yöntemi (GPY)'dir. Gizlilik Paylaşımı ilk olarak Shamir [1] ve Blakley [2] tarafından bir birinden bağımsız olarak ortaya atılmıştır. Şifrelemede kullanılan anahtarın alıcıya güvenli bir şekilde ulaştırılmasını sağlamak amacıyla geliştirilen bu yöntem (k, n) eşik şeması olarak da adlandırılmaktadır [3]. Yönteme göre gizlenmek istenen veri n tane alıcıya pay edilerek gönderilir ve verinin tekrardan elde edileceği ortamda $k \leq n$ olmak üzere en az k tane pay bir araya getirilerek orijinal veri elde edilebilir. $k - 1$ ya da daha az payın bir araya getirilmesiyle gizlenen veri hakkında bir bilgi sahibi olunamaz dolayısıyla gizlenmiş olan veri elde edilemez. GPY'nin en önemli özelliği geleneksel şifreleme tekniklerinin içerdikleri karmaşık hesaplamaları içermemesidir.

GPY üzerine birçok araştırma yapılmış ve uygulamalar gerçekleştirilmiştir. Bir seferde paylaşılacak gizli veri sayısının arttırılması [4, 5], paylarda bir bozulma ya da hile olup olmadığının tespiti [3, 6, 7] gibi yöntemin geliştirilmesine yönelik çalışmalar bunlardan bazılarıdır. Ayrıca, alıcıların yetkilendirilerek payların dağıtılması ve gizli verinin elde edilmesinde sadece yetkili payların bir araya getirilmesi [8, 9] gibi veya daha farklı yeni yaklaşımların önerildiği çalışmalar gerçekleştirilmiştir [10 - 12]. GPY'nin Naor ve Shamir tarafından 1994 yılında siyah beyaz görüntü dosyalarına uygulanması [13] ile "Görsel Gizlilik Paylaşımı" kavramı ortaya çıkmıştır.

Gizlilik Paylaşımı yönteminin uygulandığı bir diğer ortam ise ses dosyaları olmuştur. "Ses Gizlilik Paylaşımı" (Audio Secret Sharing – ASS) olarak adlandırılan bu çalışmalarda payların elde edilmesinde farklı yöntemler geliştirilmekle birlikte orijinal sesin paylar aracılığı ile elde edilmesi süreci, genel olarak hiçbir hesaplamaya ihtiyaç duyulmadan, yeterli sayıda payın birlikte eşzamanlı olarak çalınması ile gerçekleştirilir. Bu alandaki ilk çalışma 1998 yılında Desmedt ve arkadaşları tarafından gerçekleştirilmiştir [14]. Ses Gizlilik Paylaşımı ile ilgili sonraki yıllarda yapılan çalışmalarda farklı teknikler sunulmuştur [15 - 19]. Ayrıca gerçek zamanlı ses iletiminde de Gizlilik Paylaşımı yöntemi kullanılmıştır. Yapılan bazı çalışmalarda internet üzerinden VoIP protokolü ile aktarılan seslerin, gizlilik paylaşım yöntemine göre paylar oluşturularak, farklı rotalardan alıcıya gönderilmesi ve alıcı tarafta bu payların birleştirilerek konuşma sesinin elde edilmesi amaçlanmıştır. Böylelikle iletim hattının yetkisiz kişilerce dinlenmesi ihtimaline karşı bir güvenlik önlemi oluşturulmuştur [20, 21].

Gizlilik Paylaşım yönteminde önemli noktalardan bir tanesi orijinal dosyadan elde edilen payların, orijinal dosyaya benzerlik oranıdır. Shamir'in sunmuş olduğu metotla resim ve ses dosyalarından elde edilen payların, orijinal dosyaya benzerlik oranı yüksektir. Bu istenmeyen bir durumdur. Thien ve Lin, orijinal resim dosyasını ilk olarak bir anahtar değeri ile permüte ederek bu sorun için bir çözüm sunmuşlardır [10, 22]. Bir başka çalışmada ses dosyalarından pay elde ederken Shamir'in yöntemi

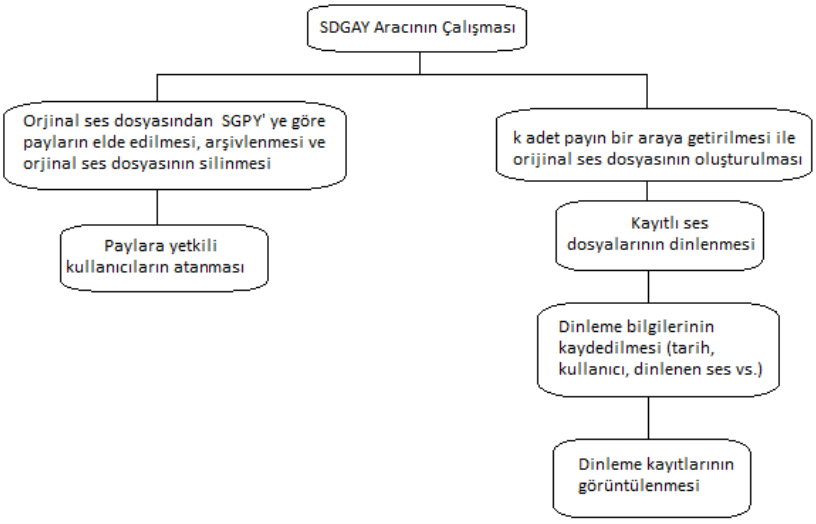
uygulanmadan önce bir karıştırma işlemi yapılarak payların orijinal ses dosyasına benzeşim sorununa çözüm önerilmiştir [23].

Bu bildiride, Shamir'in Gizlilik Paylaşımı yöntemi kullanılarak, değişik ses dosyalarının güvenilir bir şekilde arşivlenmesi ve dinlenmesini sağlayacak bir "Ses Dosyası Gizli Arşivleme Yazılımı - SDGAY" aracının gerçekleştirme süreci açıklanmıştır. Yazılımda her bir ses dosyası, gizlilik paylaşım yöntemi kullanılarak farklı paylara bölünür ve sunucularda arşivlenir. Bir kullanıcı her bir orijinal ses dosyasının tek bir payına erişim için yetkilendirilir. Her hangi bir ses dosyasının dinlenebilmesi için arşivlenmiş en az k payın bir araya getirilmesi yani k sayıda kişinin bir araya gelmesi gerekir. Dolayısıyla ilgili ses dosyalarının yetkisiz kişiler tarafından dinlenmesi veya tek bir pay dosyasına sahip kişilerin bu ses dosyasını tek başına dinleyememesi sağlanmış olur. Yazılımın iki temel biriminden birincisi; arşivlenecek ses dosyaları için gizlilik paylaşım yöntemine göre payların elde edilmesi, paylara yetkili kullanıcıların atanması ve arşivlenmesidir. İkinci birimde ise orijinal ses dosyalarının paylardan oluşturulması, ne zaman kimler tarafından dinlendiğinin ve dinlemeye teşebbüs edenlerin kayıtlarının tutulması sağlanır. Bildirinin ilerleyen kısımlarında, gizlilik paylaşım yöntemi ve uygulamaları ile geliştirilen ses arşivleme programının gerçekleştirme süreci açıklanacaktır.

II. GELİŞİTİRİLEN UYGULAMA

Visual Studio ortamında C# dili ile veritabanı olarak da MSSQL kullanılarak geliştirilen Ses Dosyası Gizli Arşivleme Yazılım (SDGAY) aracı; ses dosyalarının paylara ayrılıp arşivlenmesi suretiyle, en az k tane erişim izni olan kişinin bir araya gelmesiyle ses kayıtlarının dinlenebilmesini sağlamak için tasarlanmıştır. Arşivdeki bir ses kaydının dinlenebilmesi için k = 3 adet yetkilinin parolası gerekmektedir. Geliştirilen SDGAY aracında; saklanacak orijinal ses dosyalarının her birinden, Ses gizlilik paylaşımı yöntemine göre n adet pay oluşturulup veri tabanına kaydedildikten sonra orijinal ses dosyaları silinir. İstenildiği takdirde her bir pay farklı bir veritabanı sunucusuna kaydedilebilir. Böylelikle bir sunucu çalışmaz durumda olsa bile sistem bu olumsuzluktan etkilenmeden işlevine devam edecektir. Bununla birlikte, oluşturulan paylar tek başlarına orijinal sese ait bir bilgi vermediğinden, her hangi bir sunucudaki veriler istenmeyen kişilerin eline geçse dahi orijinal ses hakkında bilgi sahibi olunamaması sağlanır. Bu da uygulamanın güvenliğini önemli bir ölçüde arttırmaktadır.

Şekil1'de görüldüğü gibi temelde iki kısımdan oluşan yazılım aracının birinci aşaması; orijinal ses dosyalarından Ses Gizlilik Paylaşım Yöntemine (SGPY) göre payların elde edilmesi ve paylara yetkili kullanıcıların atanması sürecidir.



Şekil 1. *Sistemin işleyiş şeması*

İkinci kısımda ise, ilgili şartların oluşturulup, payların birleştirilmesiyle elde edilen orijinal ses dosyalarının geri elde edilmesi, ne zaman hangi kullanıcılar tarafından dinlendiğinin kayıtları ve yetkisiz kişilerin dinleme teşebbüslerinin kayıtlarının tutulması gerçekleştirilir.

A. SES GİZLİLİK PAYLAŞIM YÖNTEMİ

Geliştirilen SDGAY aracının amacı, paylar şeklinde arşivlenmiş olan ses kayıtlarına, sadece k sayıda yetkili kişinin bir araya gelmesiyle erişimin sağlanmasıdır. Bunun için yazılımda her bir orijinal ses dosyası, Shamir'in Gizlilik Paylaşım yöntemi kullanılarak farklı paylara bölünüp, aynı veya farklı sunucularda arşivlenir. Her hangi bir ses dosyasının dinlenebilmesi için arşivlenmiş en az k tane payın bir araya getirilmesi gerekmektedir.

Uygulamada payların elde edilmesinde, Shamir'in Lagrange İnterpolasyon kuralına dayandırdığı eşik şeması yöntemi kullanılmıştır. Yöntem iki aşamadan oluşmaktadır.

1 – Belirlenen k eşik değerine göre k-1. dereceden bir polinom oluşturulur. Eş. 1'de verilen polinomda a_0 değeri gizlenmek istenen veridir. Diğer katsayılar (a_1, a_2, …, a_{k-1}) rastgele şekilde seçilen değerlerdir. P_i, i'nci pay değeridir.

$$P_i = a_0 + a_1 x_i + a_2 x_i^2 + \cdots + a_{k-1} x_i^{k-1} \mod m, \qquad i = 1,2,\ldots n, \qquad m > a_0, \; m > n \tag{1}$$

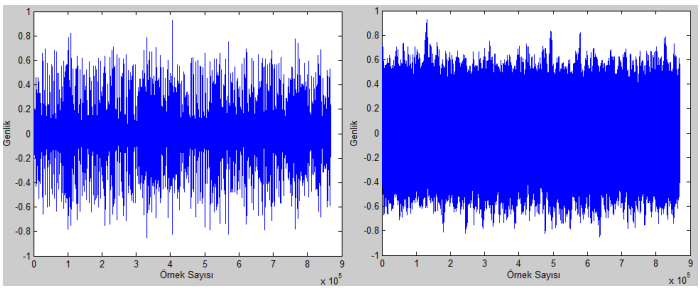
2 – Eş. 1 kullanılarak elde edilen n adet pay aracılığı ile orijinal veri elde edilmek istendiğinde, paylardan herhangi k tanesi kullanılarak Eş. 2' de verilen Lagrange interpolasyon yöntemi ile bu işlem gerçekleştirilir.

$$f(x) = \sum_{i=1}^{k} f(i) * \prod_{\substack{j=1 \\ j \neq i}}^{k} \frac{x - x_j}{x_i - x_j} \mod m \tag{2}$$

Gizlenmek istenen değer Eş. 1' de verilen polinomda, a_0 yerine yazılarak ilgili paydaki yeni değer elde edilir. Bu işlem bir resim dosyası ya da ses dosyası için gerçekleştiriliyorsa a_0 değeri resim dosyasındaki her bir pikselin renk değeri ya da ses dosyasındaki örneklenmiş ses genlik değerlerinden

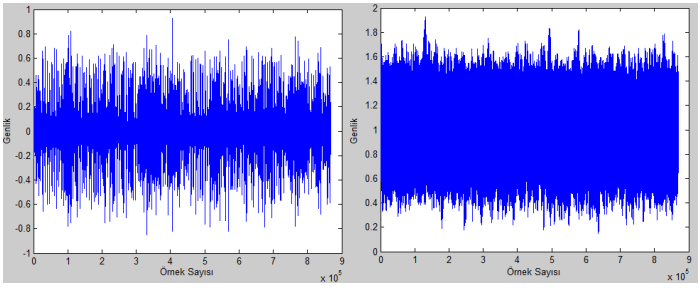
bir tanesi olabilir. Bu durumda her bir veri için Eş. 1'deki polinom ayrı ayrı kullanılacaktır. Eş. 1 dikkatle incelendiğinde yeni pay değerlerinin, orijinal verilere belirli sabit değerlerin eklenmesiyle elde edildiği görülebilir. Bundan dolayı elde edilen pay dosyaları orijinal resim dosyasına ya da ses dosyasına benzerlik gösterebilir. Çünkü bu şekilde gerçekleştirilen işlem sonucunda elde edilen paylar resim dosyasının renk tonunun veya ses dosyasının genliğinin değişmiş halidir. Bu benzerlik istenmeyen bir durum olup çözülmesi gerekir. Bu problemin çözümü için literatürde önerilen [23] bir karıştırma tekniği kullanılmıştır. Bu tekniğe göre paylar elde edilmeden önce ses verileri bir ön işlemden geçirilir. Bu ön işlem ses verilerinin karıştırılması işlemidir. Bunun için tek boyutlu bir dizi olan ses verilerinden, ilk N elemanı birinci satırı, sonraki N elemanı ikinci satırı oluşturacak şekilde MxN boyutlu bir matris elde edilir. Daha sonra her bir sütundaki elemanlar sırasıyla yan yana getirilerek tek boyutlu yeni bir dizi elde edilmiş olur. Bu yeni dizi orijinal ses dosyasından farklı olduğu için bu aşamadan sonra elde edilecek olan paylar orijinal dosyadan farklı olacaktır. Karıştırılmış olan ses dosyasından Eş. 1'de verilen polinoma göre paylar elde edilir. Orijinal ses dosyasından bu şekilde payların elde edilmesi sürecine "Ses Gizlilik Paylaşım Yöntemi – SGPY" denilmiştir. Orijinal ses dosyasının yeniden elde edilmesi aşamasında ise öncelikle k adet pay bir araya getirilerek Eş. 2'ye göre karıştırılmış ses dosyası elde edilir. Sonrasında ise ilk aşamada gerçekleştirilen karıştırma işlemi tersten uygulanarak orijinal ses dosyası elde edilmiş olur.

Yukarıda izah edilen SGPY'nin testi için, wav formatındaki tek kanallı, 8 bitlik ses örnekleme değerine sahip bir ses dosyası kullanılmış olup elde edilen sonuçlar, Şekil 2. de orijinal ses ve orijinal sesten elde edilen karıştırılmış ses dosyasının normalize genlik – örnek sayısı grafiği gösterilmiştir.



Şekil 2. (a) *Orijinal ses grafiği* ***(b)*** *Karıştırılmış ses grafiği*

Grafikten de anlaşılacağı üzere karıştırılmış ses ile orijinal ses bir birinden farklıdır. Dolayısıyla karıştırılmış sesten elde edilen paylar da orijinal sesten farklı olacaktır. Şekil 3. de ise orijinal ses ile karıştırılmış sesten elde edilen birinci pay dosyasının grafikleri örnek olması için verilmiştir. Görüldüğü gibi pay grafiği ile orijinal ses grafiği birbirinden oldukça farklıdır.



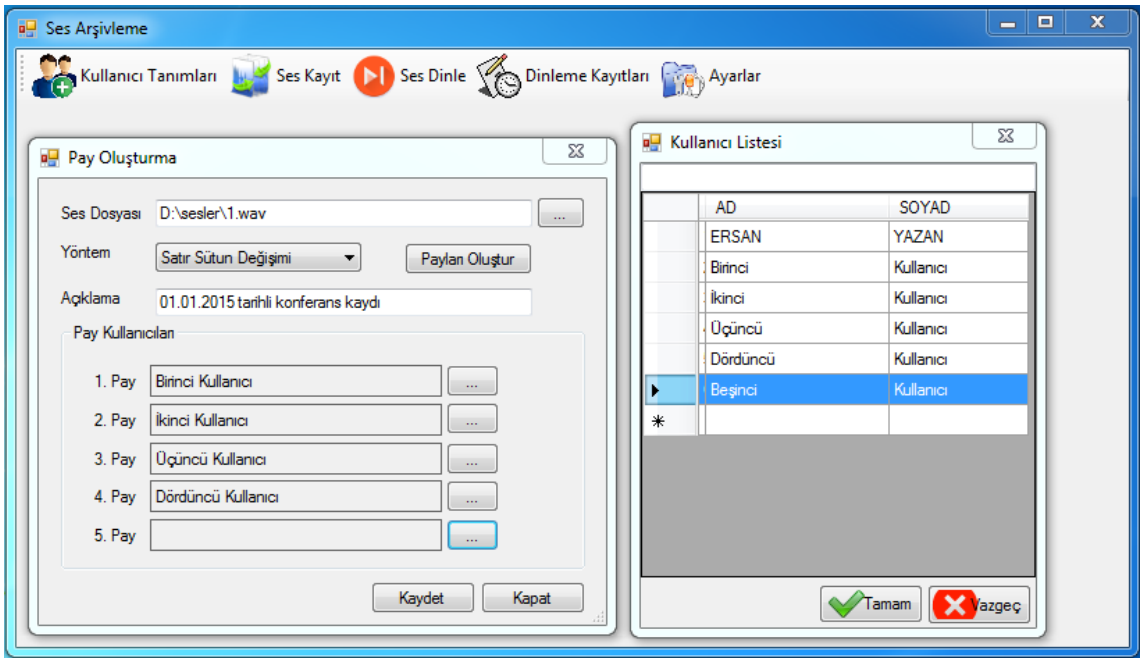
Şekil 3. (a) *Orijinal ses grafiği* ***(b)*** *Karıştırılmış sesin 1. Pay grafiği*

Bahsedilen karıştırma tekniği ile gerçekleştirilen uygulamalarda, orijinal ses dosyasından elde edilen payların orijinal ses dosyasına benzemediği ve tek bir pay dosyasından orijinal ses hakkında yorum yapılamadığı olumlu sonucuna ulaşılmıştır. Bu olumlu sonuç, karıştırma tekniğinin kullanılabilirliğini göstermiştir.

B. SDGAY YAZILIMSAL ARACI

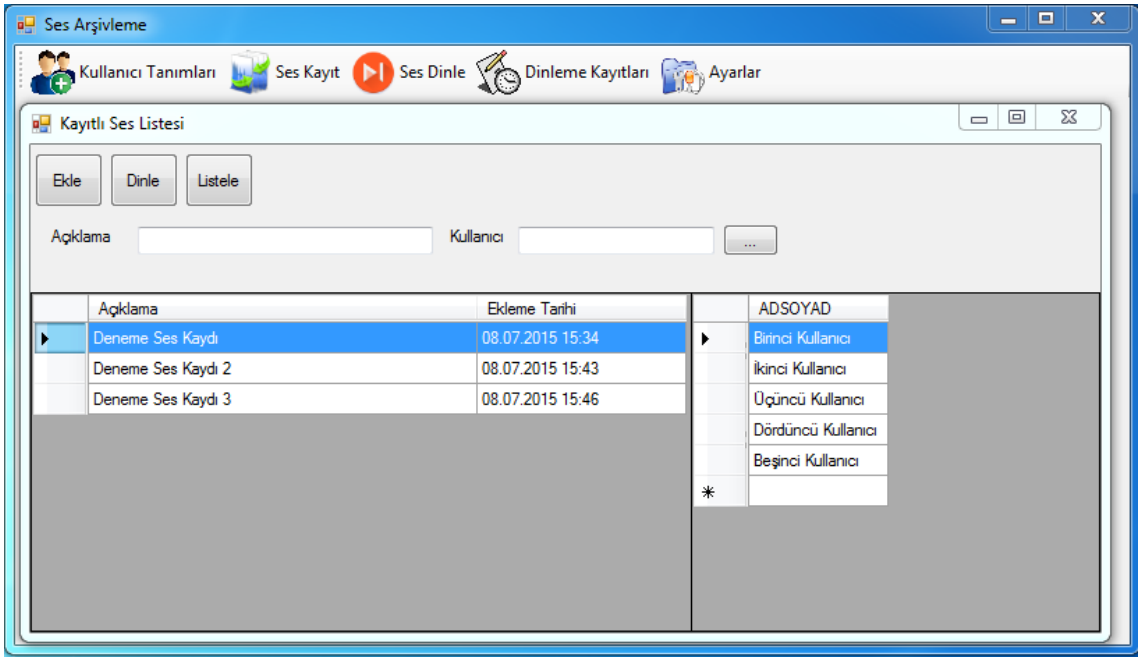
Geliştirilen SDGAY yazılımsal aracında, arşivlenmesi istenen orijinal ses dosyasının karıştırılması, paylarının oluşturulması ve k adet pay ile orijinal sesin yeniden oluşturulması sürecinde yukarıda açıklanan karıştırma ve SGPY yöntemleri kullanılmıştır. SDGAY yazılımsal araçta, sistem yöneticisi ve normal kullanıcı olmak üzere iki türlü kullanıcı mevcuttur. Sistem yöneticisi tarafından gerçekleştirilen işlemler, kullanıcı tanımları, ses pay dosyalarının oluşturulması, karıştırılması ve arşivlenmesi, dinleme kayıtlarının izlenmesi ve sistem ayarlarının yapılmasıdır. Normal kullanıcılar ise; diğer yetkili kullanıcılar ile bir araya gelerek ses kayıtlarını dinleyebilmekte ve kendi şifreleri ile dinlenen ses kayıtları geçmişini izleyebilmektedirler.

Şekil 4. de ekran görüntüsü verilen geliştirilmiş yazılım uygulamasındaki kullanıcı tanımlama ekranında, sistem yöneticisi yeni kullanıcı oluşturma, kullanıcı bilgilerini güncelleme ve mevcut kullanıcıyı silme gibi işlemleri gerçekleştirir.



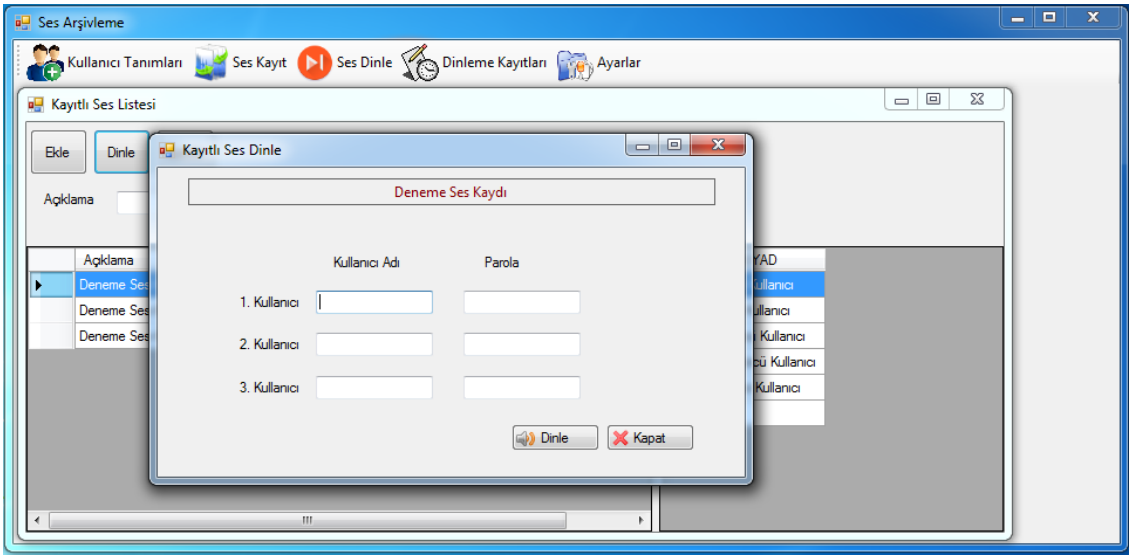
Şekil 4. *Yeni ses dosyası kayıt ekranı*

Bir ses dosyasının arşivlenmesi sürecinde; ses kayıt ekranında ilgili ses dosyası seçilerek yukarıda açıklanan ses karıştırma ve SGPY işlemi yani pay dosyalarının oluşturulması işlemi ilgili menüler aracılığı ile gerçekleştirilir. Bu şekilde elde edilmiş her bir pay için, kullanıcı listesinden seçilen kişiler atanır. Bu işlemleri sistem yöneticisi yapabilir. Seçilen kullanıcılar o ses dosyasının dinlenmesi için yetkilendirilmiş kullanıcılardır. Arşivde yer alan bir ses dosyası dinlenmek istendiğinde bu ekranda seçilen kullanıcılardan her hangi üçünün parolası ile işlem yapılması gerekir.



Şekil 5. *Kayıtlı ses dosyalarının listesi*

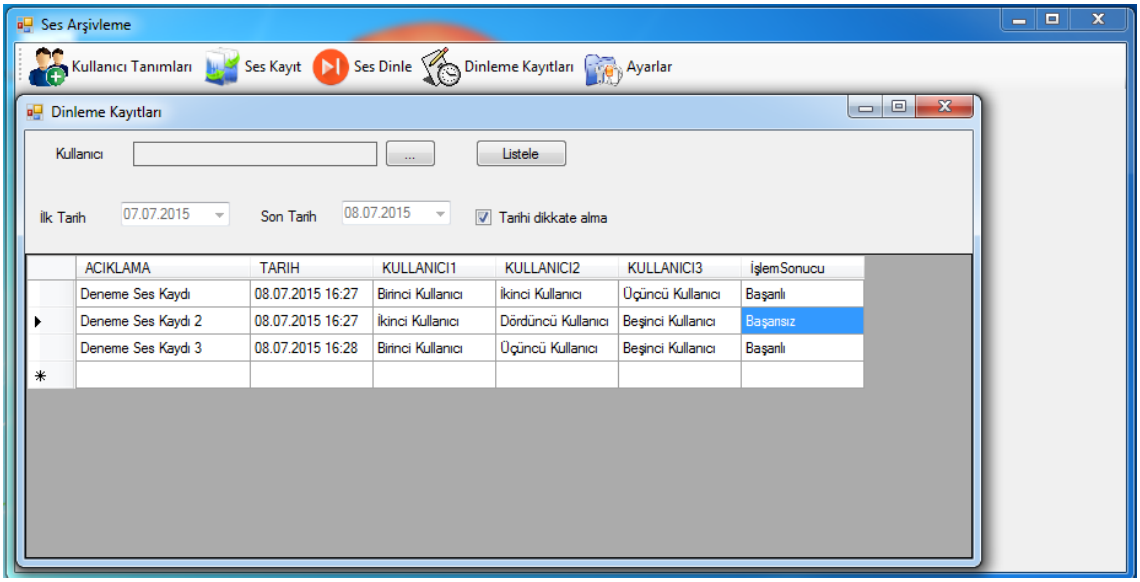
Kayıtlı seslerin dinlenebilmesi için, listede dinlenmek istenen ses dosyası seçilir. Bu ekranda her hangi bir kullanıcının yetkili olduğu kayıtlar listelenebilir. Dinlenmek istenen ses kaydı seçildikten sonra Dinle butonuna basıldığında bu ses kaydından oluşturulan payların yetkili kullanıcılarından herhangi 3 tanesinin parolası istenecektir. Bu durum Şekil 5. de görülmektedir.



Şekil 6. *Ses dosyası dinleme ekranı*

Kullanıcılar, Şekil 6. da gösterilmiş ekrandan parolalarını girdikten sonra, pay verileri bulundukları sunuculardan çekilerek birleştirilir. Eğer kullanıcı bilgilerinden en az birisi yanlışsa veya yetkisiz kullanıcı bilgileri girilmişse dinleme işlemi başarısız olacak ve aynı zamanda veritabanına başarısız dinleme teşebbüsü olarak kaydedilecektir. Sistem yöneticisi ve bu ekranda parolalarını giren

kullanıcılar bu başarısız dinleme teşebbüsünü kendi ekranlarında görebileceklerdir. Dinleme ekranında girilen kullanıcı bilgileri doğru ise orijinal ses dosyası paylar aracılığı ile elde edilecek, ilgili ses dinlenecek, işlem başarılı dinleme olarak veritabanına kaydedildikten sonra sistem yöneticisi ve parolalarını giren kullanıcılar tarafından başarılı dinleme olarak görülebilecektir. Şekil 7.'de bu işlemlerle ilgili bir ekran görüntüsü verilmektedir.



Şekil 7. *Başarılı ve başarısız dinleme kayıtları listesi*

Ana hatlarının yukarıda açıklandığı SDGAY aracı birçok ses dosyasının arşivlenmesi işlemiyle test edilmiş olup istenilen sonuçların alındığı görülmüştür.

III. BULGULAR ve TARTIŞMA

Bu çalışmada Gizlilik Paylaşımı fikrini ilk olarak ortaya atan Shamir'in bu fikir için önerdiği polinom tabanlı yöntemin ses dosyalarına uyarlanarak ses dosyalarının arşivlenmesi üzerine bir uygulama gerçekleştirilmiştir. Çalışmalar neticesinde bu yöntemin ses dosyalarında başarılı sonuçlar vermediği, orijinal dosyadan elde edilen payların orijinal dosyaya benzediği gözlemlenmiştir. Ses dosyalarından payların oluşturulmasından hemen önce orijinal dosyanın verileri karıştırılarak payların orijinal dosyaya olan benzerlikleri azaltılmıştır. Bu şekilde elde edilen payların orijinal dosya hakkında bir bilgi vermediği gözlenmiştir.

Her bir pay orijinal dosya büyüklüğünde olduğundan dolayı, orijinal dosyanın ihtiyaç duyduğundan daha fazla bir alan gerekmektedir. Bu da sistemin bir dezavantajı olarak söylenebilir.

IV. SONUÇ

Günümüz dünyasında görüntülü ve sesli iletişim sistemleri artık sayısal teknoloji platformları üzerinden gerçekleşmekte olup, gerek kayıt gerekse iletişim sürecinde analog iletişim sistemlerine göre oldukça avantajlı duruma gelmişlerdir. Ancak statik haldeki sayısal veriler veya ağ üzerinde seyahat eden veriler korumasız bir durumdadır ve tedbir alınmadığı takdirde yetkisiz kişiler tarafından gerçekleştirilecek dinlenme, değiştirilme v.b saldırılara karşı savunmasızıdır. Ayrıca arşivlenmesi gereken ses dosyalarının izinsiz kişiler tarafından ele geçirilse bile dinlenememesi veya işe özel olarak sadece k sayıda kişinin bir araya gelerek birlikte dinlemesi gereken ses dosyaları olabilmektedir.

Bu bildiride önerilen yazılımsal çözüm, arşivlenecek orijinal ses dosyalarını özel pay dosyalarına dönüştürüp arşivleme işlemini yapmaktadır. Pay dosyalarının oluşturulması Shamir'in gizlilik paylaşım yöntemine dayandırılmış olup, pay dosyalarının orijinal ses dosyasına benzerliği minimuma indirilerek, pay dosyalarının tek başına ele geçirilse bile orijinal ses hakkında bilgi edinilememesi sağlanmıştır. Orijinal sesin dinlenebilmesi için k tane payın bir araya getirilmesi şartının sağlanmasını gerektiren bu yazılımsal araçta, şifre veya parola dağıtılmış üye kişilerin hangi dosyayı hangi payları bir araya getirerek dinlendiği veya yetkisiz dinleme teşebbüslerinin yapıldığının kayıtları da tutulmaktadır.

Bu şekilde elde edilmiş olan SDGAY aracı değişik kurumlarda kullanılabilecek seviyede tasarlanmış, test edilmiş ve başarılı olduğu görülmüştür. Yazılımsal aracın geliştirilmesi gerekli kısımlarının ise; pay dosyalarının boyutlarının toplamının orijinal dosyadan daha fazla yer kaplaması problemi ve pay yetkilendirme şifrelerinin daha dayanıklı bir şekilde elde edilip dağıtılması olduğu söylenebilir.

V. KAYNAKLAR

[1] A. Shamir *Communications of the ACM.* **22(11)** (1979) 612.

[2] G.R. Blakley, *Safeguardingcryptographickeys,* **National Computer Conference,** New York – Amerika (1979) 313.

[3] D. Arda, E. Buluş, *MDS kod tabanlı gizlilik paylaşım şemasında hileli katılımcıları tespit etmek ve kimliklendirmek*, **IV. Ağ ve Bilgi Güvenliği Ulusal Sempozyumu,** Ankara – Türkiye, (2011) 10.

[4] C.C. Yang, T.Y. Chang, M.S. Hwang (2004) **DOI:10.1016/S0096-3003(03)00355-2**.

[5] L. J. Pang, Y.M. Wang (2005) **DOI:10.1016/j.amc.2004.06.120**.

[6] M. Tompa, H. Woll (1989) **DOI: 10.1007/BF02252871**.

[7] M. Carpentieri (1995) **DOI: 10.1007/BF01388382**.

[8] E.D. Karnin, J.W. Greene, M.E. Hellman *IEEE Transactions on Information Theory.* **29(1) (**1983) 36.

[9] Y.C. Chen, D.S. Tsai, G. Horng (2012) **DOI: 10.1016/j.jvcir.2012.08.006**.

[10] C.C. Thien, J.C. Lin (2002) **DOI: 10.1016/S0097-8493(02)00131-0**.

[11] A. Renvall, C. Ding (1996) **DOI: 10.1007/BFb0023287**.

[12] A. Behimel, B. Chor (1995) **DOI: 10.1007/3-540-44750-4_28**.

[13] M. Naor, A. Shamir (1995) **DOI: 10.1007/BFb0053419**.

[14] Y. Desmedt, S. Hou, J.J. Quisquater (1998) **DOI: 10.1007/3-540-49649-1_31**.

[15] C.N. Yang *Journal of InforamtionScienceand Engineering.* **18(3)** *(*2002) 381.

[16] D. Socek, S. S. Magliveras (2005) **DOI: 10.1109/EIT.2005.1627018**.

[17] A. Nikam, P. Kapade, S. Patil *International Journal ofApplied Information Systems* **1(8)** (2010) 1.

[18] P.V. Khobragade, N. Uke *International Journal ofApplied Information Systems.***1(8)(**2012) 1.

[19] M. Ehdaie, T. Eghlidos, M.R. Aref (2008) **DOI: 10.1109/ISTEL.2008.4651264**.

[20] R. Nishimura, S.I. Abe, N. Fujita, Y. Suzuki *Journal of Information Hidingand Multimedia SignalProcessing.* **1(3)** (2010) 204.

[21] M. Hamdaqa, L. Tahvildari (2011) **DOI:10.1109/SSIRI.2011.24**.

[22] M.A. Şahin,D. Arda, *Renkli görüntü dosyalarında gizlilik paylaşımı uygulaması,* **IV İletişim Teknolojileri Sempozyumu,** Ankara – Türkiye (2009).

[23] E. Yazan, Y. Tatar, *Ses dosyaları için Shamir'in gizlilik paylaşımı yöntemine dayalı bir uygulama,* **3rd International Symposium On Digital Forensics and Security,** Ankara – Türkiye, (2015) 219.