T.C.
FIRAT ÜNİVERSİTESİ
FEN BİLİMLERİ ENSTİTÜSÜ

VERİ GÜVENLİĞİ İÇİN GİZLİLİK PAYLAŞIMI TEMELLİ BİR UYGULAMA

YÜKSEK LİSANS TEZİ

Ersan YAZAN

Anabilim Dalı: Bilgisayar Mühendisliği
Programı: Bilgisayar Donanımı
Tez Danışmanı: Prof.Dr. Yetkin TATAR (F.Ü.)

OCAK-2016

T.C.
FIRAT ÜNİVERSİTESİ
FEN BİLİMLERİ ENSTİTÜSÜ

VERİ GÜVENLİĞİ İÇİN GİZLİLİK PAYLAŞIMI TEMELLİ BİR UYGULAMA

YÜKSEK LİSANS TEZİ

Ersan YAZAN
122129104

Tezin Enstitüye Verildiği Tarih:
Tezin Savunulduğu Tarih:

Tez Danışmanı: Prof. Dr. Yetkin TATAR (F.Ü.)
Diğer Jüri Üyeleri : Yrd. Doç. Dr. Taner TUNCER (F.Ü.)
: Yrd. Doç. Dr. Metin ERTÜRKLER (İ. Ü.)

OCAK-2016

ÖNSÖZ

Bu tez çalışması kapsamında veri güvenliği alanında önemli bir yere sahip olan Gizlilik Paylaşımı fikri konusunda literatür taraması yapılarak, bu fikri ilk olarak ortaya atan Shamir'in yöntemi detaylı bir şekilde ele alınmıştır. Shamir'in yönteminin ses dosyalarına uyarlanması ile ilgili yazılımsal ve donanımsal olmak üzere iki farklı gerçekleştirme yapılmıştır.

Bu çalışma esnasında bana her türlü hoşgörü, destek ve bilgisiyle katkıda bulunan saygıdeğer danışmanım Prof. Dr. Yetkin TATAR' a, çalışmalarım sırasında yardımını esirgemeyen Yrd. Doç. Dr. Taner TUNCER'e, bu günlere gelmemde emeklerini inkâr edemeyeceğim değerli aileme, her zaman yanımda olan ve desteklerini esirgemeyen çok kıymetli eşime ve arkadaşlarıma teşekkürü bir borç bilirim.

Ersan YAZAN

ELAZIĞ - 2016

İÇİNDEKİLER

ÖZET

Bilgisayar ve Sayısal İletişim teknolojilerinin kullanılması günlük hayatımızda vazgeçilmez bir unsur haline gelmiştir. Bununla birlikte sayısal ortamlarda saklanan veya iletilen verilerin güvenlikleriyle ilgili sorunlar da giderek artmaktadır. Bu sorunlardan birisi de gerek arşivlenmiş haldeki gerekse iletişim halindeki sayısal ses verilerinin istenmeyen kişiler tarafından ele geçirilmesidir. Bu sorunun çözümü için kullanılan yöntemlerden birisi de *Gizlilik Paylaşımı Yöntemi* olabilir. Gizlilik Paylaşımı yöntemi, gizlenecek verinin paylara ayrılması ve gizlenmiş veriyi tekrar oluşturabilmek için belirli sayıda payın bir araya getirilmesini gerektiren bir yöntemdir.

Bu tez çalışmasında gizlilik paylaşımı yöntemine dayanan iki uygulama yapılmıştır. Bunlardan ilki, ses dosyalarının gerçek zamanlı iletimi sürecindeki güvenliğin sağlanmasına yönelik FPGA (Sahada Programlanabilir Kapı Dizeleri) tabanlı donanımsal bir gerçekleştirme uygulamasıdır. İkincisi ise sayısal ses arşivlerindeki ses dosyalarını yetkisiz kişilerin veya tek bir kişinin dinlemesini önlemek amacıyla yapılmış bir yazılım aracıdır.

Yapılan uygulamaların sonuçları analiz edilerek, FPGA donanımsal uygulama sonuçlarının, gerçek zamanlı ses uygulamaları için yeterince güvenilir olduğu ve arşivleme yazılımının da arşivlenmiş ses dosyalarının sadece yetkilendirilmiş kullanıcı gurupları tarafından dinlenebildiği gözlemlenmiştir. Sonuç olarak her iki uygulamanın da pratikte kullanılabilir olduğu gösterilmiştir.

Anahtar Kelimeler: Gizlilik paylaşımı, FPGA, ses arşivleme, güvenli ses iletimi

SUMMARY

A SECRET SHARING BASED APPLICATION FOR DATA SECURITY

The use of computers and digital communication technology has become indispensable element in our daily lives. However, problems with the security of stored or transmitted data in a digital environment are increasing. One of the problems is seizing of archived or transmitted digital voice data by unwanted person. Secret Sharing Method could be one of the methods used for the solution of the problem. The Secret Sharing method requires divided data to shares and coming together of certain number of shares to reconstruct the secret data.

In this thesis, two applications were implemented related to Secret sharing method. The first is an FPGA (Field Programmable Gate Array) based hardware realization practices to ensure security in real-time transmission of audio files. The other application is a software tool aiming to prevent listening audio files on digital audio archive by only one person or unauthorized people.

By analizing the results of the implemented application, it has been observed FPGA hardware implementation results are sufficiently reliable for real-time voice applications and in the archiving software, archived audio files can be listened by authorized user groups only. As a result, it has been shown that both applications can be usable in practise.

Keywords: Secret Sharing, FPGA, archiving audio, secure voice transmission

ŞEKİLLER LİSTESİ

Sayfa No

KISALTMALAR LİSTESİ

OGGP **:** Olasılıklı Görsel Gizlilik Paylaşımı

FPGA **:** Field Programmable Gate Array

PLD **:** Programmable Logic Device

ASIC **:** Application Specific Integrated Circuit

SDGAY **:** Ses Dosyası Gizli Arşivleme Yazılımı

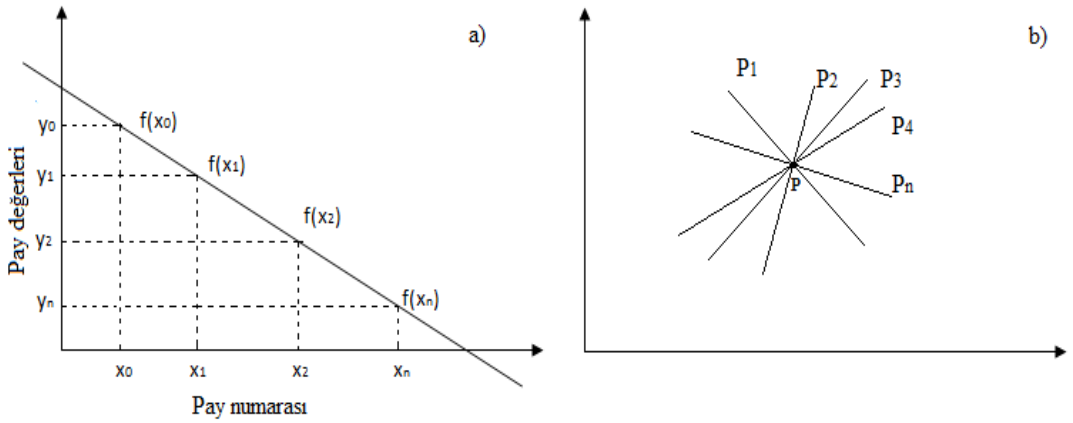
1. GİRİŞ

Günümüz dünyasında bilgisayar, bilgisayar ağları ve internet gündelik hayatın vazgeçilmezi haline gelmiştir. Teknolojinin gelişmesiyle beraber hayatın her alanına hitap eden sayısal teknolojiler, eksikliği hemen hissedilen öğeler olmuşlardır. Büyük kolaylıklar sağlayan bu sistemler çok önemli bir sorunu da beraberinde getirmektedir. Bu sorun, gerek bilgisayar ortamındaki gerekse ağ ortamındaki sayısal olarak kodlanmış metin, resim, video ve ses vb. verilerin güvenliği sorunudur. Özellikle internet gibi herkese açık bir ağ ortamında bulunan veriler için bu risk çok daha büyüktür. Bu sorunun çözülmesi için gösterilen çabalar neticesinde bilgi güvenliği kavramı ortaya çıkmıştır.

Bilgi güvenliği gerek bilgisayar ortamında statik haldeki, gerekse iletim halindeki dinamik verilerin gizlilik ve bütünlüğünün korunmasının yanı sıra yetkisiz kişilerce erişiminin önlenebilmesinin sağlanması şeklinde tarif edilebilir. Bilgi güvenliği kapsamında şifreleme, elektronik imza, erişim kontrol mekanizmaları ve kimlik doğrulama sistemleri gibi birçok yöntem geliştirilmiştir ve bu alandaki çalışmalar devam etmektedir.

Veri güvenliğini sağlamak amacıyla gerçekleştirilen yöntemlerden birisi de "Gizlilik Paylaşımı" fikridir. Şifrelemede kullanılan anahtarın alıcıya güvenli bir şekilde iletilmesini sağlamak amacıyla önerilen bu fikir ilk olarak 1979 yılında Shamir [1] ve Blakley [2] tarafından birbirinden bağımsız olarak ortaya atılmıştır. Fakat yapılan çalışmalar gösteriyor ki özellikle görüntü ve ses dosyalarında bu yöntem verinin kendisini şifrelemek amacıyla da kullanılmıştır. Gizlilik Paylaşımının ana fikri orijinal verinin belirli sayıda paylara ayrılması ve ancak bu payların birkaçının bir araya getirilmesi ile orijinal verinin yeniden elde edilmesine dayanır. Orijinal veriden oluşturulan bu payların her biri tek başına orijinal veriyi oluşturamazlar ve onunla ilgili bir bütünlük sağlayamazlar. Orijinal verinin belirli sayıda paya ayrılmasıyla güvenlik tek bir yerde toplanmayıp dağıtılarak daha etkin bir şekilde sağlanmakta ve payların tamamı yerine bir kısmı ile orijinal verinin elde edilebilmesi ile de orijinal verinin yeniden elde edilme işlemi garanti altına alınmaya çalışılmaktadır. Dolayısıyla gizlenmek istenen veriden n adet payın oluşturulup ilgili alıcılara dağıtılması ve orijinal verinin tekrardan elde edilmesi için, $k \leq n$ olmak üzere en az k tane payın bir araya getirilmesi gerekir. k-1 ya da daha az sayıda pay ile orijinal veri elde edilememektedir. Orijinal veriden oluşturulan n adet paydan k tanesi ile orijinal verinin tekrardan elde edilebildiği bu yöntem, (k, n) eşik şeması yöntemi olarak da adlandırılmaktadır [4]. Shamir'in önerdiği (k, n) eşik şeması yöntemi, polinom tabanlı

bir yöntemdir. Shamir'in yöntemine göre, paylar oluşturulurken (k-1). dereceden bir polinom oluşturulur. Bu polinomun sabit terimi gizlenecek veridir, polinomun diğer katsayıları ise rastgele olarak belirlenir. Paylar oluşturulduktan sonra bu polinomun bir gerekliliği kalmamaktadır. Gizli verinin yeniden elde edilmesinde de kullanılmayacaktır. Şekil1.1- a' da görüldüğü üzere x – y düzleminde x değerleri pay numaralarını, x değerlerine karşılık gelen y değerleri ise oluşturulan pay değerlerini ifade eder ve gizlenmiş olan verinin paylar aracılığı ile yeniden elde edilme aşamasında, herhangi k tane pay (x, y çiftleri) ile Lagrange interpolasyon tekniği kullanılır [5].



Şekil 0.1 a) Shamir'in yöntemine göre x pay numaralarına karşılık, y pay değerleri b) Blakley'in Gizlilik Paylaşım şeması

Blakley'in yöntemi ise geometrik tabanlı bir yöntemdir. Blakley, önerdiği yöntemde Şekil 1.1b'de görüldüğü gibi gizli veriyi k boyutlu uzayda bir nokta gibi düşünmüştür. Buna göre bu noktadan geçen n farklı hiper düzlem katılımcılara gönderilen pay bilgileridir. Bunlardan paralel olmayan herhangi k tanesinin kesişimi ise gizlenmiş olan veridir [2, 5].

Gizlilik Paylaşımı ile alakalı birçok araştırma yapılmış olup bu fikri gerçekleştirmek amacıyla farklı yaklaşımlar sunulmuştur. Gerçekleştirilen bazı çalışmalarda gizli bilginin paylaştırılmasında sayı teorisinin özelliklerini kullanan yöntemler önerilmiştir. 1981 yılında McElice ve Sarwate tarafından Reed Solomon kodlarını kullanarak gerçekleştirilen çalışma [6] bunlardan bir tanesidir. Asmuth-Bloom [7] ve Mignotte [8] ise Çin Kalan Teoremine dayalı yöntemler önermişlerdir. Bazı

çalışmalarda ise payların oluşturulmasında lineer bir yaklaşım kullanılması durumunda sistemin çok güvenli olmayacağı, daha fazla güvenli bir çözüm için lineer olmayan yaklaşımların kullanılması gerektiği belirtilmiş ve bu şekilde çözüm önerilerinde bulunulmuştur [9]. Bu yaklaşımlar da non-lineer Gizlilik Paylaşımı olarak adlandırılmışlardır.

Gizlilik Paylaşımında önemli noktalardan bir tanesi belirlenen k eşik değerinden daha az sayıda pay ile orijinal verinin elde edilememesidir. Bununla birlikte k-1 ya da daha az sayıda pay ile orijinal veri hakkında hiçbir bilgiye erişilemiyorsa bu özelliği sağlayan yöntemler mükemmel olarak nitelendirilirler [10]. Bir diğer önemli nokta ise her bir payın büyüklüğüdür. Gerçekleştirilen bazı çalışmalarda pay boyutları orijinal verinin boyutundan çok daha büyük olabilmektedir [11, 12]. Fakat Gizlilik Paylaşımı yönteminde genel olarak istenen, payların büyüklüğünün orijinal verinin büyüklüğünden daha fazla olmamasıdır. Yani her bir payın büyüklüğü orijinal verinin büyüklüğüne eşit ya da küçük olmalıdır. Bunu sağlayan yöntemler "*İdeal Gizlilik Paylaşım Yöntemi"* olarak adlandırılırlar [13]. Fakat her bir payın büyüklüğü orijinal verinin büyüklüğüne eşit olsa da, bu payları saklamak için ihtiyaç duyulan alan orijinal veri için gerekli olan alandan daha fazla olacaktır. Bu nedenle pay boyutlarının orijinal veriden küçük olması daha uygun bir çözüm olmaktadır. Pay boyutlarının küçültülmesi de Gizlilik Paylaşımı konusunda bir diğer çalışma konusu olmuştur [14].

Gizlilik Paylaşımı yönteminin metin, resim ve ses verileri üzerinde uygulamalarıyla ilgili farklı çalışmalar yapılmıştır. 2015 yılında Belenli ve arkadaşlarının yapmış oldukları çalışmada [15] web tabanlı uygulamalarda kimlik doğrulama amacıyla kullanılmak üzere bir sistem önerilmiştir. Önerilen sistemde kullanıcı şifresi önce görselleştirilmekte ve sonrasında bu görselden iki pay oluşturulmaktadır (pay sayısı opsiyonel olabilmekte). Paylardan biri veritabanında saklanmakta, diğeri ise kullanıcıya verilmektedir. Kullanıcıya verilecek olan pay (görsel) kullanıcının isteği doğrultusunda direk olarak kullanıcıya verilir ya da kullanıcının bilgisayarında belirttiği bir resmin içerisine saklanabilir. Sisteme giriş aşamasında kullanıcının kendi parola resmi ile veritabanındaki görsel kullanılarak orijinal parola elde edildiği takdirde giriş sağlanmaktadır. Bir başka çalışmada [16] Nabiyev ve Zadeh, DataMatrix barkotların veri güvenliğini artırmak için bir yöntem önermişlerdir. Bu yöntemde, gizli veri paylara ayrılarak her pay, bir DataMatrix taşıyıcı içine gömülmekte ve daha sonra bu paylar katılımcılara dağıtılmaktadır. Her hangi bir katılımcıya ait payı içeren barkoddan gizli veri kesinlikle elde edilememektedir. Çünkü her bir barkoddaki bilgi tek

başına anlamsız verileri ifade etmektedir. Gizli verinin elde edilmesi, önceden belirlenen eşik değere eşit veya daha büyük sayıda payın bir araya gelmesiyle gerçekleşmektedir.

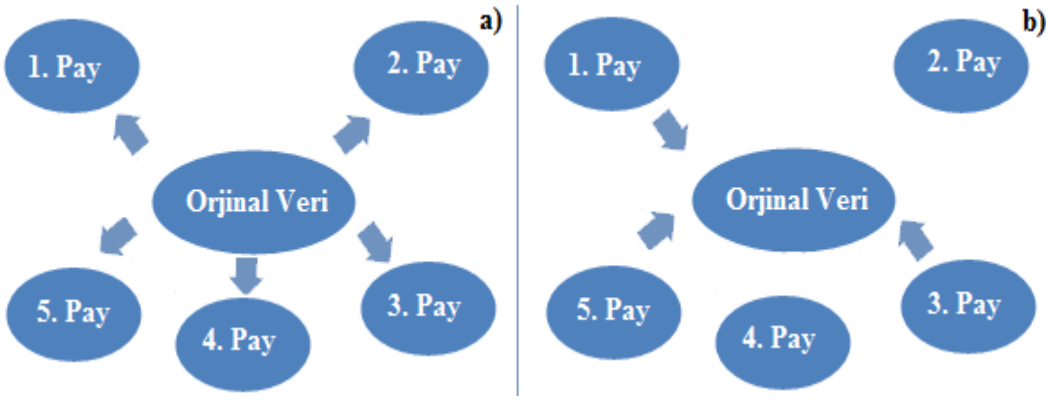
1.1. Tez Çalışmasının Amacı

Tez çalışmasında, "Gizlilik paylaşımı" algoritması kullanılarak, sayısal verilerin ve özellikle ses dosyalarının off-line / on-line olarak güvenilir bir şekilde saklanması veya iletilmesi için uygulamaların geliştirilmesi amaçlanmaktadır. Böylece;

- Gizlilik paylaşım algoritmasının off-line ve on-line analizleri yapılarak gerçek zamanlı uygulamalar için uygun olup olmadığı tespit edilebilir. Gerçek zamanlı uygulamalar için algoritmada iyileştirmeler yapılabilir.
- Gizlilik paylaşımı yöntemiyle güvenlik altına alınmış ve arşivlenmiş veri dosyalarının deşifrelenmesi sürecinde, tekbir şifreye bağımlı olmak yerine, yetkilendirilmiş belirli sayıda pay sahibinin oluşturduğu bir ortamda deşifrelemenin gerçekleştirilmesi mümkün olur. Böylece arşivdeki herhangi bir dosyaya, sadece aynı anda ulaşması gereken kişilerin beraberce ulaşması garantilenmiş olur.
- Sayısal telefon görüşmelerinin bir yetkisiz dinleyici tarafından çözülmesi yerine yetkili bir guruptan birkaç kişinin beraberce deşifreleme yapabilmesi sağlanabilir.
- Ses dosyalarının gerçek zamanda, gizlilik paylaşımı yöntemiyle paylara ayrılması ile telefon görüşmelerinin yetkisiz kişilerce dinlenmesi önlenebilir.
- Belirlenen amaca ulaşmak için, tezin ikinci bölümde Shamir'in Gizlilik Paylaşımı yöntemi detaylı bir şekilde incelenmiş ve bu konuda yapılan çalışmalar kısaca özetlenmiştir. Ayrıca resim ve metin dosyaları üzerinde gizlilik paylaşımı yöntemi için örnek uygulamalar gerçekleştirilmiştir. Üçüncü bölümde ise ses dosyalarından payların elde edilmesi sürecinde, elde edilen paylar ile orijinal ses dosyasının benzerliğinin azaltılması için önerilmiş olan teknik açıklanarak MATLAB ortamında uygulaması yapılmıştır. Dördüncü bölümde, gizlilik paylaşımının ses dosyaları üzerinde gerçek zamanlı bir uygulaması için, FPGA platformu kullanılarak yapılan donanımsal gerçekleştirme ve testler sunulmuştur. Tezin beşinci bölümünde ise ses dosyalarının gizlilik paylaşımı yöntemiyle paylara ayrılarak arşivlenmesini sağlayan bir yazılım aracının gerçekleştirilmesi aşamalarından bahsedilmiştir. Çalışmanın altıncı bölümünde ise sonuç ve öneriler ele alınmıştır.

2. GİZLİLİK PAYLAŞIMI

Gizlilik Paylaşımı'nın genel tanımı, gizlenmek istenen orijinal veriden belirli sayıda ve birbirine benzemeyen payların oluşturulması ve bu payların birkaç tanesinin biraraya getirilmesiyle gizlenmiş orijinal verinin yeniden elde edilmesi şeklindedir. Bu tanımdan da anlaşılacağı gibi Gizlilik Paylaşımı temelde iki aşamadan oluşmaktadır. Bu aşamalardan ilki, orijinal veriden n adet payın oluşturulmasıdır. Öyle ki, bu payların sadece bir tanesinin kullanılmasıyla orijinal verinin oluşturması söz konusu olamaz. İkinci aşama ise en az k ($k \leq n$) adet payın bir araya getirilerek orijinal verinin yeniden elde edilmesi sürecidir. Bu aşamalar Şekil 2.1'de temsili olarak gösterilmiştir.



Şekil 0.1 a) Orijinal veriden payların oluşturulması (n = 5) b) Orijinal verinin elde edilmesi (k=3)

Gizlilik paylaşımı üzerine yapılan çalışmalarda önerilen tüm yöntemler, bu iki aşamanın gerçekleştirilme şekilleri açısından birbirlerinden farklılık göstermektedir. Shamir 'in önerdiği yaklaşım ise en sık kullanılan ve polinom tabanlı bir yöntem olup aşağıda izah edildiği şekilde gerçekleştirilmektedir [1].

Gizlenmek istenen veriden n adet payın oluşturulmasında şu adımlar izlenmektedir:

1-Paylaştırıcı tarafından orijinal veriyi paylara ayırmak için, eşik değeri (k) belirlenir ve eşitlik 2.1'deki gibi k-1. dereceden bir polinom oluşturulur. Bu polinomdaki a_0 katsayısı gizlenmek istenen **S** verisidir [1]. Diğer katsayılar ise (a_1, a_2, … a_{k-1}) gelişigüzel belirlenen değerlerdir.

$$P = f(x) = a_0 + a_1 x + a_2 x^2 + \cdots + a_{k-1} x^{k-1} \qquad (\mathbf{2.1})$$

2-Shamir modüler aritmetik kullanarak kendi deyimiyle bu yöntemi daha kusursuz hale getirmiştir. Bunun için a_0 sabitinden ve n'den daha büyük bir m asal sayısı seçilerek eşitlik 2.2 elde edilmiş olur. Paylaştırıcı, gizlenmek istenen veriden eşitlik 2.2'deki polinoma göre n tane pay (P) oluşturur. Bu payların her biri, bir pay sahibine gönderilir.

$$P_i = a_0 + a_1 x_i + a_2 x_i^2 + \cdots + a_{k-1} x_i^{k-1} \, mod \, m, i = 1,2, \ldots n, m > a_0, \quad m > n \qquad (\mathbf{2.2})$$

Elde edilen paylardan k tanesinin bir araya getirilerek orijinal verinin elde edilmesi işlemi ise "Lagrange İnterpolasyon" yöntemi ile gerçekleştirilir. Lagrange interpolasyonu, değerleri bilinen k tane nokta ile k-1. dereceden bir polinom tanımlayan bir yöntemdir. Paylar oluşturulurken gerçekleştirilen mod işlemi aynı değer ile gizlenen verinin elde edilmesinde de uygulanır. Buna göre f(x) polinomu aşağıdaki formül ile elde edilir.

$$f(x) = \sum_{i=1}^{k} f(i) * \prod_{\substack{j=1 \\ j \neq i}}^{k} \frac{x - x_j}{x_i - x_j} mod(m) \qquad (\mathbf{2.3})$$

Burada x_i ve x_j gizli verinin elde edilmesinde kullanılacak payların indeks numaralarını, f(i) ise bu paylardan i. Payın verisini temsil etmektedir. İşlem sonucunda elde edilen f(x) değeri ise orijinal veridir. Shamir' in k tane pay ile orijinal veriyi tekrar elde etmede kullanmış olduğu Lagrange interpolasyon yöntemi matematiksel olarak şu şekilde izah edilmiştir [17]:

$x_0, x_1, x_2, \ldots\ldots x_n$ noktalarındaki fonksiyon değerleri $f(x_0), f(x_1), f(x_2), \ldots\ldots f(x_n)$ olsun. $(x_0, f(x_0)), (x_1, f(x_1)), (x_2, f(x_2)), \ldots\ldots (x_n, f(x_n))$ noktalarından geçen n. dereceden benzersiz bir P(x) polinomu $P(x) = a_0 + a_1x + a_2x^2 + a_3x^3 + \ldots\ldots + a_nx^n$ şeklinde tanımlanabilir. Bu polinom $f(x_0) = (x_0, y_0)$, $f(x_1) = (x_1, y_1)$, $f(x_2) = (x_2, y_2)$, $\ldots\ldots f(x_n) = (x_n, y_n)$ noktalarından geçtiğine göre $P(x_0) = f(x_0)$, $P(x_1) = f(x_1)$, $P(x_2) = f(x_2)$, … , $P(x_n) = f(x_n)$ eşitlikleri yazılabilir ve $P(x_i) = f(x_i)$ şeklinde genellenebilir. n. dereceden bir P(x) polinomu x_i noktasından geçiyorsa, bu noktadaki $f(x_i)$ değeri n. dereceden bir L(x) polinomu ile çarpılarak P(x) polinomu elde edilmiş olur.

$$P(X) = \sum_{i=0}^{n} f(Xi) * L_i(X) \qquad (\mathbf{2.4})$$

Yukarıdaki eşitlikte x yerine x_j yazdığımızda aşağıdaki eşitlik elde edilir.

$$P(Xj) = \sum_{i=0}^{n} f(Xi) * L_i\,(Xj) \qquad (\mathbf{2.5})$$

$P(x_i) = f(x_i)$ olduğundan dolayı, i = j iken $L_i(x_j) = 1$, i≠j iken $L_i(x_j) = 0$'dır.

$$\mathbf{Li(xj)} = \begin{cases} \mathbf{1} & , \quad \boldsymbol{i = j} \\ \mathbf{0} & , \quad \boldsymbol{i \neq j} \end{cases} \qquad (\mathbf{2.6})$$

n. dereceden kökleri bilinen bir eşitlik kendi kökleri ile; $L_i(x) = \lambda_i . (x-x_0)\ldots.(x-x_{i-1}).(x-x_{i+1})\ldots (x-x_n)$ şeklinde elde edilir. $L_i(x_j)=1$ olduğundan dolayı bu eşitlikte λ_i çekilerek aşağıdaki eşitlik elde edilir.

$$\lambda i \; = \; \frac{1}{(xi - x0). \ldots (xi - xi - 1).(xi - xi + 1) \ldots \; (xi - xn)} \qquad (\mathbf{2.7})$$

Buna göre n. dereceden $L_i(x)$ polinomu şu şekilde yazılır.

$$Li(x) = \frac{(x - x0). \ldots (x - xi - 1).(x - xi + 1) \ldots \; (x - xn)}{(xi - x0). \ldots (xi - xi - 1).(xi - xi + 1) \ldots \; (xi - xn)} \qquad (\mathbf{2.8})$$

Bu durumda eşitlik 2.4'de, $L_i(x)$ polinomu yerine eşitlik.2.8 değeri yazılırsa eşitlik.2.9 elde edilmiş olur.

$$P(x) = \sum_{i=0}^{n} f(xi) * L_i\,(x) = \sum_{i=0}^{n} \left(\prod_{\substack{j=1 \\ j \neq i}}^{n} \frac{(x - xj)}{(xi - xj)} \right) * f(xi) \;\; mod\, m \qquad (\mathbf{2.9})$$

Yöntemin nasıl çalıştığını göstermek amacıyla 7 rakamının gizlenecek veri olarak seçildiği bir uygulamayı göz önüne alalım. Gizlenecek verinin 5 pay sahibine paylaştırılıp

her hangi 3 payın bir araya getirilmesi ile 7 rakamının tekrardan elde edilmesinin istendiği durumda k = 3, n = 5 olacaktır.

k = 3 olduğu için 2. dereceden (k- 1). $P(x) = a_0 + a_1x + a_2x^2$polinomu oluşturulur. a_0 katsayısı gizlenmek istenen verinin kendisi yani 7'dir. a_1 ve a_2 rastgele değerler olarak sırasıyla 19 ve 21 seçilsin. Buna göre polinom $P(x) = 7 + 19x + 21x^2$ haline gelir. Bundan sonraki aşama ise a_0 ve n değerlerinden daha büyük bir asal sayının seçilmesi ve her bir pay sahibinin payının oluşturulması işlemidir. Seçilen asal sayı 31 olsun. Mod 31' e göre P(x) polinomunu hesaplayarak payları elde edelim.

$P(x) = 7 + 19x + 21x^2 \text{mod } (31)$ polinomundan x = 1, 2, 3, 4, 5 için aşağıdaki değerler elde edilir.

$P(1) = 7 + 19 + 21 \text{ mod } (31) = 16$

$P(2) = 7 + 19.2 + 21.2^2 \text{mod } (31) = 5$

$P(3) = 7 + 19.3 + 21.3^2 \text{mod } (31) = 5$

$P(4) = 7 + 19.4 + 21.4^2 \text{mod } (31) = 16$

$P(5) = 7 + 19.5 + 21.5^2 \text{mod } (31) = 7$

Buna göre gizlenmek istenen veriden (7 rakamı), $Pay_1 = (1, 16)$, $Pay_2 = (2, 5)$, $Pay_3 = (3, 5)$, $Pay_4 = (4, 16)$, $Pay_5 = (5, 7)$ şeklinde 5 tane pay oluşturulmuş olur. Payların hiçbiri gizlenmek istenen veriye benzememektedir.

Şimdide herhangi 3 payı kullanarak orijinalin verinin elde edilmesi aşamalarını gerçekleştirelim. $Pay_1 = (1, 16)$, $Pay_2 = (2, 5)$ ve $Pay_3 = (3, 5)$ değerlerinin seçelim. Bunun için Lagrange interpolasyon eşitliğinde (Eşitlik.2.9) değerler yerine yazılıp aşağıda belirtilen gerekli düzenlemeler yapılarak;

$$P(x) = \frac{(x-2).(x-3)}{(1-2).(1-3)}.16 + \frac{(x-1).(x-3)}{(2-1).(2-3)}.5 + \frac{(x-1).(x-2)}{(3-1).(3-2)}.5 \ (mod\ 31)$$

$$P(x) = (x^2 - 5x + 6).8 + (-x^2 + 4x - 3).5 + (x^2 - 3x + 2).\frac{5}{2} \ (\text{mod } 31)$$

$$P(x) = 8x^2 - 40x + 48 - 5x^2 + 20x - 15 + \frac{5x^2 - 15x + 10}{2} \ (\text{mod } 31)$$

$$P(x) = \frac{6x^2 - 40x + 66 + 5x^2 - 15x + 10}{2} \ (\text{mod } 31)$$

$$P(x) = \frac{11x^2 - 55x + 76}{2} \ (\text{mod } 31)$$

$$P(x) = \frac{11x^2}{2} + \frac{55x}{2} + 38 \ (\text{mod} 31)$$

P(x) polinomunda x yerine 0 yazıldığında a_0 sabit sayısı yani gizlenen veri elde edilmiş olur. Buna göre P(0) = 38 mod 31 ≡ 7'dir.

Görüldüğü gibi gizlenen 7 rakamı tekrar elde edilmiştir. Farklı paylar ile denendiğinde yine aynı şekilde orijinal verinin elde edildiği görülecektir. Burada bulunan P(x) polinomunun başlangıçta oluşturulan polinomla aynı çıkmamasının sebebi mod işlemidir. Eğer paylar oluşturulurken mod alınmasaydı başlangıçta oluşturulan polinom elde edilecekti. Bu işlemde önemli olan gizli veri olduğundan dolayı direkt olarak gizli veriyi elde etmek için yani P(0) değerini bulmak için aşağıdaki eşitlik kullanabilir.

$$\boldsymbol{P}(0) = \sum_{i=0}^{n} \left(\prod_{\substack{j=1 \\ j \neq i}}^{n} \frac{(xj)}{(xi - xj)} \right) * f(xi)(mod\ m) \qquad (\mathbf{2.10})$$

Bu eşitliğe göre çözümü tekrardan yapacak olursak,

$$P(0) = \frac{(2).(3)}{(1-2).(1-3)}.16 + \frac{(1).(3)}{(2-1).(2-3)}.5 + \frac{(1).(2)}{(3-1).(3-2)}.5\ (mod\ 31)$$

$$P(0) = 48 - 15 + 5\ (mod\ 31)$$

$$P(0) = 38\ mod\ 31 \equiv 7$$

Yukarıdaki örnek, tek bir karakter veya sembolün gizlenmesi için paylara ayrılması ve bu paylardan, tek karakterin yeniden oluşturma sürecini kapsamaktadır. Buradan yola çıkılarak, birçok karakterden oluşmuş bir dokümanın bütün karakterleri için veya MxN piksellik bir resim dosyasının bütün pikselleri için veya z tane örneklenmiş değerden oluşmuş bir ses dosyasının bütün örneklenmiş değerleri için yukarıdaki işlemlerin tekrar edilmesiyle doküman, resim veya ses dosyalarının paylara ayrılması veya tersi işlemlerin yapılması mümkündür. Yöntemin basit hesaplamalarla gerçekleştirildiği göz önüne alındığında bu işlemlerin gerçek zamanlı uygulamalarda rahatlıkla yapılabileceği söylenebilmektedir.

Yöntemin en büyük avantajlarından bir tanesi de yukarıdaki örneklerde de görüldüğü üzere çok karmaşık matematiksel hesaplamalar içeren işlemlerin

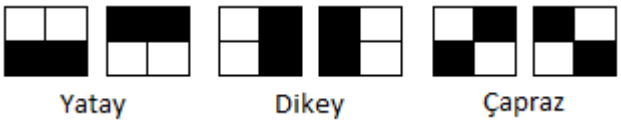
kullanılmamasıdır. Bu nedenle uygulanması kolay ve gerçek zamanlı işleyebilen bir yöntem özelliği taşımaktadır.

Gizlilik Paylaşımı ile ilgili olarak yapılan bazı çalışmalarda pay oluşturma aşaması için yeni yaklaşımlar önerilmekte iken bazı çalışmalarda ise yöntem farklı açılardan ele alınarak geliştirilmesine yönelik metotlar önerilmiştir. Paylarda bir bozulma ya da hile olup olmadığının tespiti, bir seferde paylaşılacak olan gizli bilgi sayısının arttırılması, payların yetkilendirilerek sadece yetkili paylar ile gizlenmiş verinin elde edilmesi gibi çalışmalar bunlardan bazılarıdır [18 - 31].

Paylarda bir bozulma ya da hile ile elde edilmiş bir pay olduğu zaman gizlenmiş veriyi yeniden elde etmek her zaman mümkün olmayacaktır. Bu nedenle hatalı payın tespit edilmesi gizli veriyi yeniden elde edebilmek açısından önemlidir. Tompa ve Woll, Shamir'in yöntemini biraz değiştirerek hileli katılımcıları tespit edebilecek bir yaklaşım önermişlerdir [18]. Brickell ve Stinson ise Blackley'in yöntemini uyarlamışlardır [19]. Bunların haricinde farklı yaklaşımların önerildiği çalışmalar da gerçekleştirilmiştir [20, 21]. Bir seferde paylaşılacak olan gizli bilgi sayısının arttırılması ile ilgili çalışmalar "Çoklu Gizlilik Paylaşımı" (Multi Secret Sharing) olarak adlandırılmaktadır [22]. Çoklu Gizlilik Paylaşımında her bir pay birden fazla bilgiden elde edilir. Bu alanda gerçekleştirilen ilk çalışmalarda gizli verilerin elde edilmesi bir seferde değil ayrı ayrı gerçekleştirilir [23, 24]. Yani bir seferde tek bir gizlenmiş verinin orijinali elde edilir. 2000 yılında Chien ve arkadaşları, yeni bir yöntem önermişlerdir [25]. Bu yönteme göre bir seferde paylar aracılığı ile birden fazla gizlenmiş veri elde edilebilir. Bu açıdan daha önceki yöntemlere göre daha kullanışlı olan yöntemin dezavantajı ise çok fazla karmaşık bir yapısının olmasıdır [26]. Yang ve arkadaşlarının 2004 yılında Shamir'in yöntemine dayanarak önerdiği yöntem [27] ise Chien'in yöntemine göre çok daha kolay ve sadedir. Sadece yetkili payların gizlenmiş veriyi yeniden elde etmesi üzerine gerçekleştirilen çalışmalar, "Çok Parçalı Gizlilik Paylaşım Şemaları" (Multipartite Secret Sharing Schemes) olarak adlandırılmaktadır [28]. Bu yönteme göre payların dağıtılacağı kişiler gruplara bölünür ve aynı grup içerisindeki kişiler aynı yetkiye sahiptir. Bu gruplardan yetkili olanları ile gizlenmiş veri yeniden elde edilir. Çok Parçalı Gizlilik Paylaşım Şemaları ile ilgili farklı çalışmalar [28 – 31] gerçekleştirilmiş olup bu çalışmalarda önerilen yöntemler pay sahiplerinin yetkilendirilme şekline göre farklılık göstermektedirler.

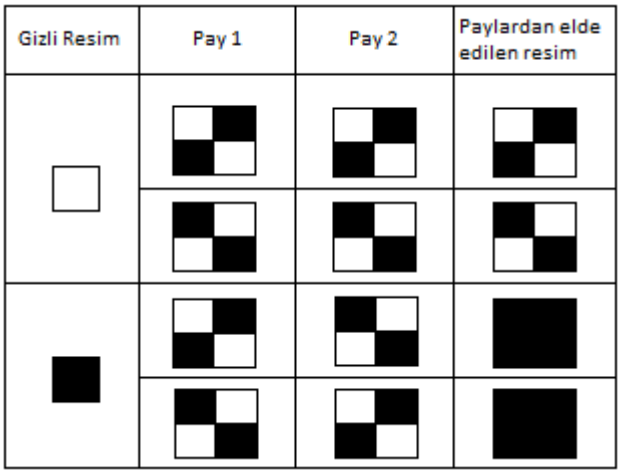
2.1. Görsel Gizlilik Paylaşımı

Naor ve Shamir'in, 1994 yılında yaptıkları çalışmada [32] Gizlilik Paylaşımı yöntemini siyah beyaz görüntü dosyalarına uyarlamasıyla "Görsel Gizlilik Paylaşımı" kavramı ortaya çıkmış oldu. Bu çalışmada (2,2) eşik şeması yöntemi temel olarak alınmıştır. Buna göre her pikselin paylarda iki alt pikselle temsil edilmesi gerekirken bu şekilde bir çözüm resmin en boy oranını bozacağı için gizlenecek resmin her bir pikseli 4 piksele (2X2) genişletilmiş ve Şekil 2.2'deki modellerden biri ile temsil edilmiştir.



Şekil 0.2 Piksel genişletme için kullanılan modeller veya maskeler

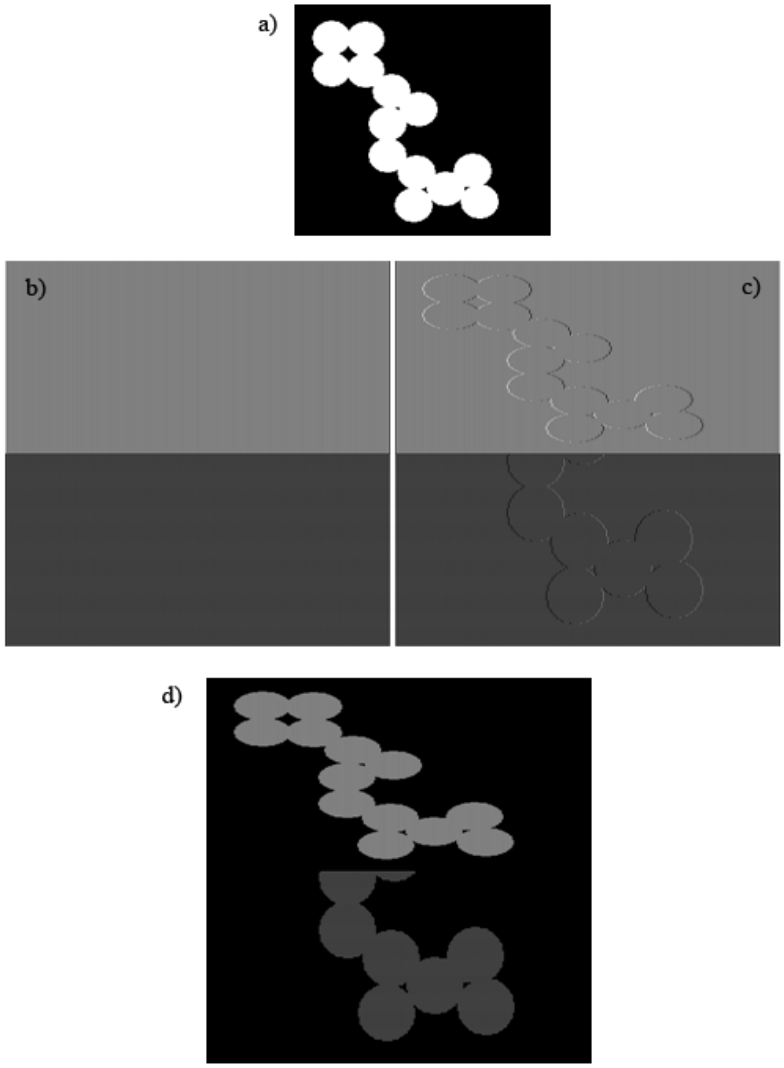
(2x2) eşik şeması yöntemi şu şekilde izah edilmiştir. Gizlenmek istenen resmin her bir pikseli iki pay için aynı model seçilerek Şekil 2.2'deki yatay, dikey ya da çapraz modellerden birine genişletilir. Bu piksel genişletme işlemi, orijinal pikselin siyah ya da beyaz olma durumuna göre şu şekilde gerçekleştirilir. Orijinal resmin pikseli beyaz ise, her iki pay da aynı şekilde genişletilir. Eğer orijinal resmin pikseli siyah ise paylardan birinde modelin bir şekli diğerinde ise aynı modelin diğer şekli ile genişleme işlemi gerçekleştirilir. Orijinal resmin elde edilmesi payların üst üste getirilmesi ile elde edilir. Bu işlem çapraz genişleme modeli için Şekil 2.3'te gösterilmiştir.



Şekil 0.3 Beyaz ve siyah piksellerin paylaşımı ve payların üst üste getirilmesi

Şekil 2.3'te de görüldüğü gibi pay bloklarının üst üste bindirilmesinde bir birine denk gelen piksellerin en az bir tanesi siyah ise sonuç siyah, her ikisi de beyaz ise sonuç beyaz piksel oluyor. Bundan dolayı orijinal resimdeki piksel siyah ise paylar aracılığı ile tekrardan oluşturulan resimde de siyah olarak elde edilmektedir. Orijinal resimdeki piksel beyaz ise paylar aracılığı ile elde edilen piksel yarı siyah yarı beyaz yani gri olarak elde edilmektedir.

Yukarıda izahı anlatılan işlemin MATLAB ortamında 2 farklı siyah beyaz resim için uygulanmış örneği aşağıda gösterilmiştir. Birinci örnekte, Şekil 2.4.a'daki 256x256 boyutlarındaki orijinal *circles* resminden 2 tane pay oluşturulmuş (Şekil 2.4.b ve c) ve sonrasında da bu iki pay ile orijinal resim elde edilmeye çalışılmıştır.



Şekil 0.4 256x256 boyutlarında siyah beyaz resimden çapraz modelle pay oluşturma işlemi a) Orijinal resim b) Pay 1 (512 x 512) c) Pay 2 (512 x 512) d) Paylardan elde edilen resim

Şekil 2.5'te, görüntü dosyasından payların elde edilmesi ve paylardan orijinal görüntünün yeniden oluşturulması aşamalarının MATLAB ortamında gerçeklendiği kodlar gösterilmiştir.

a)

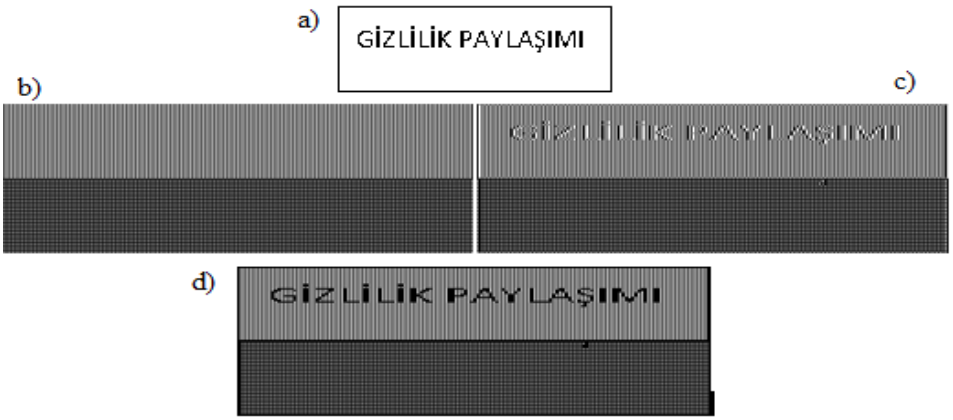
```
image = imread('circles.png');
[satir sutun] = size(image);
ip = 1;
jp = 0;
for i = 1:satir
for j=1:sutun
if image(i,j) == 0
share1(i,j + jp) = 1;
share1(i,j+jp+1) = 0;
share1(i + ip, j + jp) = 0;
share1(i + ip, j + jp + 1) = 1;
share2(i,j + jp) = 0;
share2(i,j+jp+1) = 1;
share2(i + ip, j + jp) = 1;
share2(i + ip, j + jp + 1) = 0;
end
if image(i,j) == 1
share1(i,j + jp) = 1;
share1(i,j+jp+1) = 0;
share1(i + ip, j + jp) = 0;
share1(i + ip, j + jp + 1) = 1;
share2(i,j + jp) = 1;
share2(i,j+jp+1) = 0;
share2(i + ip, j + jp) = 0;
share2(i + ip, j + jp + 1) = 1;
end
jp = jp + 1;
end
ip = ip + 1;
jp = 0;
end
 imwrite(share1, 'D:\yukseklisans\tez\circles_share1.bmp');
 imwrite(share2, 'D:\yukseklisans\tez\circles_share2.bmp');
```

b)

```
[satir sutun] = size(share1);
for i = 1:satir
for j = 1:sutun
if (share1(i,j) == 0)
reconstructedImage(i,j) = 0;
elseif(share2(i,j) == 0)
reconstructedImage(i,j) = 0;
else
reconstructedImage(i,j) = 1;
end
end
end
imwrite(reconstructedImage, 'D:\yukseklisans\tez\reconstructed_image.bmp');
```

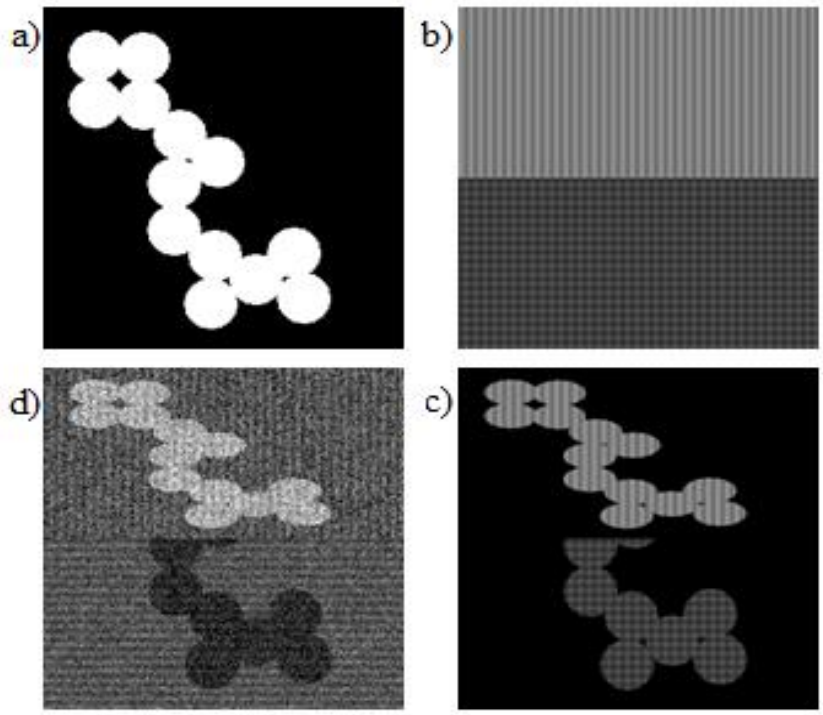
Şekil 0.5 Orijinal görüntüden payların oluşturulması ve kaydedilmesiişlemleri için MATLAB kodları.

Aynı işlemin 150 x 52 boyutlarındaki farklı bir resim için uygulama sonuçları Şekil 2.6 a, b, c, d ‘de verilmiştir.

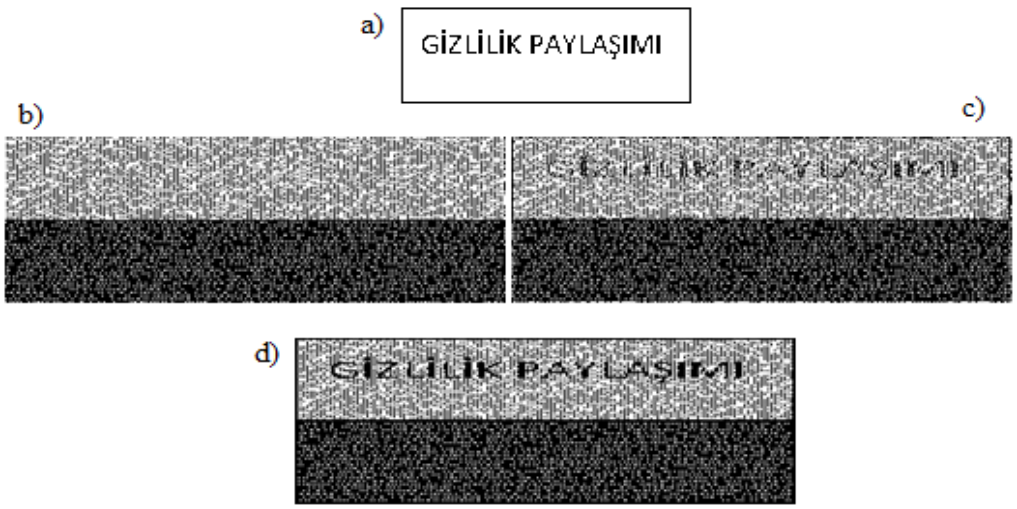


Şekil 0.6 150x52 boyutlarında siyah beyaz resimden çapraz modelle pay oluşturma işlemi a) Orijinal resim b) Pay 1 (300 x 104) c) Pay 2 (300 x 104) d) Paylardan elde edilen resim (300 x 104))

Gerçekleştirilen her iki uygulamada da orijinal görüntü dosyasının pikselleri paylarda çapraz modele göre genişletilmiştir. Şekil 2.7 ve 2.8 ‘de iki görüntü dosyası için rastgele (yatay, dikey, çapraz) modele göre piksel genişletme uygulaması sonuçları gösterilmiştir.



Şekil 0.7 256x256’lık resimden rastgele modelle pay oluşturma a) Orjinal resim b) Pay 1 (512 x 512) c) Pay 2 (512 x 512) d) Paylardan elde edilen görüntü (512 x 512)



Şekil 0.8 150x52’lik resimden rastgele modelle pay oluşturma a) Orijinal resim b) Pay 1 (300 x 104) c) Pay 2 (300 x 104) d) Paylardan elde edilen görüntü (300 x 104)

Yukarıdaki uygulamalarda da görüldüğü üzere paylar aracılığı ile elde edilen görüntü orijinal görüntünün bire bir aynısı değildir. Elde edilen görüntünün boyutları orijinal görüntüden daha büyük ve kontrast değeri %50 bozuk olmaktadır. Bu bozulmanın sebebi, paylarda 4 piksel ile temsil edilen her bir siyah piksel için payların birleştirilmesiyle elde edilen görüntüde 4 pikselin de siyah olarak görülmesine karşın beyaz piksellerin ikisi siyah ikisi beyaz olarak görünmesidir. Kontrast problemi bu yöntem üzerine yapılan araştırma konularından bir tanesidir. Naor ve Shamir daha sonra yapmış oldukları çalışmada [33] kontrast değerindeki bozulmayı azaltmak için yöntem üzerinde düzeltme yapmışlardır. Bir diğer çalışmada ise önerilen yöntem renkli resimler üzerinde kontrast problemi oluşmadan uygulanmıştır [34].

Görsel Gizlilik Paylaşımı yöntemi üzerine birçok araştırma yapılmış ve uygulamalar gerçekleştirilmiştir. Yöntem üzerine yapılan çalışmalardan bazılarında yöntemin sadece siyah beyaz resimler üzerinde değil, gri seviye [35, 36] veya renkli resimler [34, 37] üzerinde de uygulanabileceği gösterilmiştir. Görsel gizlilik paylaşımı yönteminde genel olarak gizlenecek görüntü dosyasının bir pikseli paylarda birden fazla alt pikselle temsil edilir. Bu durum görüntü dosyalarının belirli oranda büyümesine neden olur. Bu büyüme oranının küçültülmesi bir diğer çalışma konusu olmuştur. Bu konuda yapılan bazı çalışmalarda "Olasılıklı Görsel Gizlilik Paylaşımı" (OGGP) yöntemi önerilmiştir [38]. Bu yöntem ilk olarak Yang tarafından 2004 yılında önerilmiştir [39]. OGGP yöntemine göre gizlenecek olan görüntünün her bir pikseli paylarda da yine bir piksel ile temsil edilir. Bundan dolayı payların büyüklüğü gizlenecek olan görüntünün büyüklüğü ile aynı olmaktadır. Wang 2007 yılında önerdiği (2, n) OGGP şemasında AND ve XOR gibi mantıksal işlemleri kullanmıştır [40]. Siyah beyaz resimlerde uygulanan bu yöntem siyah pikselleri %100 beyaz pikselleri ise %50 oranında olasılıkla doğru olarak koruyabilmektedir. Wang'ın yönteminin geliştirilerek beyaz piksellerin doğruluk oranının yükseltildiği bir çalışma da 2008 yılında gerçekleştirilmiştir [38]. Gri seviye ve renkli resimler için önerilen Olasılıklı Görsel Gizlilik Paylaşım şeması çalışmasında [41] ise gri ve renkli görüntü dosyaları için ayrı şemalar önerilmiş ve paylardaki piksel genişlemesi kullanıcı tanımlı olarak ayarlanmıştır.

Thien ve Lin ise yapmış oldukları çalışmada önerdikleri yöntemin gri ve renkli resimlere direk olarak uygulanabilirliğini göstermekle birlikte pay boyutlarını da daha küçük boyutlara indirgemişlerdir [42]. Thien ve Lin tarafından öne sürülen yöntemde her bir payın boyutu orijinal görüntü dosyasının 1/k'sı büyüklüğündedir. Daha küçük

boyutlarda payların oluşturulması konusunda Thien ve Lin haricinde de çalışmalar yapılmıştır [43, 44].

2.2. Ses Gizlilik Paylaşımı

Gizlilik Paylaşımı şemalarının kullanıldığı bir diğer alan da ses dosyaları olmuştur ve bu alanda yapılan çalışmalar "Ses Gizlilik Paylaşımı" (Audio Secret Sharing, ASS) olarak adlandırılmıştır. (k, n) eşik şeması fikrinin temel alındığı bu çalışmalarda k değeri genel olarak 2 olmakla birlikte $k \geq 3$ olduğu çalışmalar da mevcuttur. Ses Gizlilik Paylaşımı şemalarında paylar ses, gizlenecek olan veri ise yine bir ses ya da bit dizesi olmaktadır. Gerçekleştirilen çalışmaların genel olarak ortak yönleri gizli verinin elde edilmesinde herhangi bir hesaplamaya ihtiyaç duyulmamasıdır. Gizlenen veri yeterli sayıda payın birlikte eşzamanlı olarak çalınması ile elde edilmektedir.

Bu alanda ilk çalışma 1998 yılında Desmedt ve arkadaşları tarafından gerçekleştirilmiştir [45]. Bu çalışmada ses dosyası paylara ayrılarak, elde edilen payların içerisine bilgi gizlenmektedir. Bu çalışmaya göre gizlenmek istenen veri bit dizesidir. Verinin gizlendiği ortam (Cover sound, örtü ses) olarak ise harmonik ses veya yüksek kaliteli müzik kullanılabilmektedir. Çalışmada sunulan yöntem şu şekilde izah edilmiştir.

S: Gizlenecek olan veri (bit dizesi)

L: Gizlenecek verinin bit uzunluğu

T: Gizlenecek olan verinin her bir biti için kullanılacak süre. Başka bir ifade ile 1 bitlik verinin gizlenmesi için belirlenen saniye değeri.

B: Verinin gizlenmesi için kullanılacak TxL saniye uzunluğundaki örtü ses.

Öncelikle s1 ve s2 olmak üzere iki pay oluşturulur ve bu paylar örtü ses olarak kullanılacak ses dosyası (B) ile aynıdır. Sonrasında s1 payı için her T saniyede, rastgele seçilen b (1 ya da 0) değerine göre faz değişimi gerçekleştirilir. Rastgele seçilen b'nin değeri 1 ise 180 (π) derece faz değiştirilir. 0 ise her hangi bir değişiklik yapılmaz. s2 ise $b' = \overline{b \oplus S}$ denkleminden b' değerine göre hesaplanır. Eğer b' 1 ise 180 derece faz değiştirilir. 0 ise bir değişiklik yapılmaz.

Gizlenen verinin elde edilmesi için iki metot önerilmiştir. İlk metoda göre, iki tane hoparlör çok yakın olarak birbirine bakacak şekilde yerleştirilir. s1 bir hoparlöre, s2 de diğer hoparlöre gönderilerek sesler çalınır. Bu şekilde hoparlörlerden gelen seslerin değişimine göre gizli bitler elde edilir. Yüksek ses 1 bitini, düşük ses ise 0 bitini temsil

eder. Böylelikle sesler tamamen dinlendiğinde gizlenen verinin tüm bitleri elde edilmiş olur.

İkinci metotta hoparlörün yerleştirilmesi farklıdır. Hoparlörün biri sağ tarafımıza diğeri ise sol tarafımıza gelecek şekilde yerleştirildikten sonra sesler çalınır. Hoparlörlerin kenarlardan ortaya, ortadan kenarlara doğru hareket ettirilmesiyle gelen sese göre gizli veri elde edilir. Bu yöntem iki kanaldan gelen seslerin faz farklılıklarına göre gizli verinin elde edilmesine dayanır. Eğer her iki kanaldaki sesin fazı aynı ise gizli verinin biti 1 demektir ve hoparlörler ortadayken tek bir ses duyulur. Seslerin fazları farklı ise, gizli verinin biti 0 demektir ve biri sağ taraftan diğeri sol taraftan olmak üzere her iki hoparlörden de sesler duyulur.

Yukarıda izahı edilen işlem (2, 2) eşik şeması yöntemine dayanmaktadır. Çalışmada bu yöntemin (k, n) eşik şeması yöntemine genelleştirilmesi de izah edilmiş olup, bunun için $\log_2$ n tane örtü ses dosyası gerektiği izah edilmiştir.

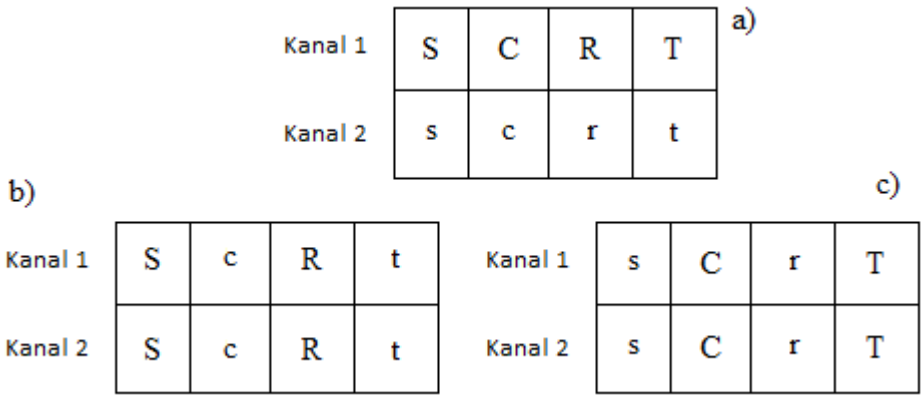
Sonraki yıllarda gerçekleştirilen bir çalışmada [46] ise Desmedt ve arkadaşlarının sunduğu bu yöntem [45], n değeri ne olursa olsun sadece bir tane örtü ses gerekli olacak şekilde geliştirilmiştir.

Socek ve Magliveras, Naor ve Shamir'in Görsel Şifreleme olarak sundukları çalışmadaki piksel genişletmesi mantığını seslerin şifrelenmesinde kullanmışlardır [47]. Çalışmada şifrelemek için mors koduna benzer sesler kullanılmıştır. Bu sesler kısa ve uzun olmak üzere iki farklı bip sesinden oluşmaktadır. Görsel Şifrelemeyle kıyas yapılarak kısa bip sesi beyaz piksellere, uzun bip sesi ise siyah piksellere karşılık geldiği belirtilmiştir. Çalışmada kısa ve uzun bip sesleri görsel olarak nitelenmiş ve uzun bip sesi için "_", kısa bip sesi için "." kullanılmıştır. Yöntem şu şekilde izah edilmiştir. Gizlenecek olan S sesi için S1 ve S2 olmak üzere iki tane pay oluşturulur. S' teki her bir bip paylarda iki tane bip sesi olacak şekilde genişletilir. S' in i. bip sesi b_i olmak üzere eğer b_i uzun bip sesi ise S1(i) = ._ ve S2(i) = _. veya S1(i) = _. ve S2(i) = ._ şeklinde rastgele belirlenir. Eğer b_i kısa bip sesi ise S1(i) = S2(i) = ._veya S1(i) = S2(i) = _. olacak şekilde genişletilir. Gizli veriyi elde etmek için S1 ve S2 birlikte eş zamanlı olarak çalınır. S1 ve S2'nin karşılık gelen bip sesleri her ikisinde de kısa ise duyulacak ses kısa bip sesidir. Eğer ikisinden bir tanesi bile uzun bip sesi ise duyulacak ses uzun bip sesi olur.

Yönteme göre m tane bip sesinden oluşan S için üretilen S1 ve S2 paylarının her biri 2m tane bip sesinden oluşur. Dolayısıyla bu payların birlikte çalınmasıyla duyulacak olan toplam bip sesi yine 2m tanedir. Bundan dolayı aslında payların çalışmasıyla elde

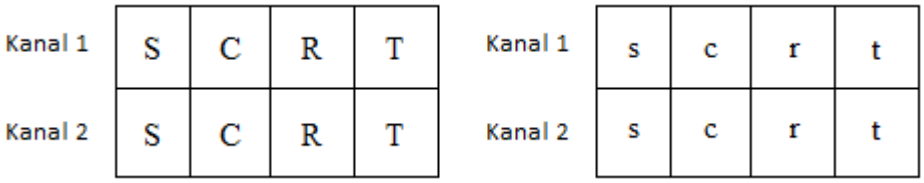
dilen ses orijinal sesin birebir aynısı olmamaktadır. Çalışmada bu kontrast probleminin göz ardı edildiği ifade edilmiş.

Bu alanda yapılan çalışmaların bazıları ise ses dosyalarının yapıları temel alınarak gerçekleştirilmiştir. Örneğin wave dosyaları üzerinde yapılan bir çalışmada [48] iki kanallı (stereo) sesin şifrelenmesi üzerine bir yöntem tavsiye edilmiş. (2,2) gizlilik paylaşımı şeması olarak sunulan yönteme göre iki tane stereo ses dosyası oluşturularak her iki paya orijinal ses dosyasının başlık bilgileri kopyalanır. Sonrasında orijinal ses dosyası, uzunluğuna göre n tane parçaya bölünür. İlk kanalın ilk parçası birinci payın her iki kanalına, ikinci kanalın ilk parçası ikinci payın her iki kanalına kopyalanır. Sonraki adımda ilk kanalın ikinci parçası ikinci payın her iki kanalına, ikinci kanalın ikinci parçası birinci payın her iki kanalına kopyalanır. Bu işlem tüm parçalar kopyalanana kadar her aşamada kopyalanacak olan hedef paylar değiştirilerek devam ettirilir. Gizlenecek olan ses dosyasından iki tane pay elde etme işlemi Şekil 2.9' da gösterilmiştir.



Şekil 0.9 İki kanallı ses dosyasından payların elde edilmesi: a) Orijinal iki kanallı ses dosyası b) Birinci pay c) İkinci pay

Wave formatındaki ses dosyaları ile gerçekleştirilen bir diğer çalışmada [49] ise kopyalama işleminde ufak bir değişiklik yapılarak orijinal sesin birinci kanalındaki veriler birinci payın her iki kanalına, orijinal sesin ikinci kanalındaki veriler ikinci payın her iki kanalına kopyalanmıştır. Bu işlem yukarıdaki orijinal ses için Şekil 2.10'da gösterilmiştir.



Şekil 0.10 İki kanallı ses dosyasından payların elde edilmesi a) Birinci pay b) İkinci pay

Bu çalışmalarda da tek bir sesin çalınması ile orijinal ses elde edilemezken her iki sesin birlikte eşzamanlı olarak çalınması ile orijinal ses duyulur. Tek bir sesin çalınmasıyla orijinal sesin elde edilememesinden kasıt orijinal sesin tamamının elde edilememesidir. Zira seslerden bir tanesinin çalınmasıyla orijinal ses hakkında bilgi sahibi olunabilir. Bundan dolayı her iki yöntem de güvenli değildir.

Bazı çalışmalarda ise gizlenecek olan ses, sinyal olarak ele alınmış ve frekans, genlik gibi özellikleri üzerinde işlem yapılarak sesin parçalara ayrılması gerçekleştirilmiştir. M. Ehdaie ve arkadaşları gerçekleştirmiş oldukları çalışmada [50] ses dosyasının genliğini kullanarak parçalara ayırma işlemi gerçekleştirmişlerdir. Genlik vektörleri A ve B olmak üzere aynı uzunluktaki iki ses dosyasının birlikte çalınmasıyla genlik vektörü A+B olan bir ses duyulur. M. Ehdaie ve arkadaşlarının yaptıkları çalışma bu özelliğe dayanmaktadır. Çalışmada gizlenmek istenen ses dosyasının genlik vektörü A olmak üzere, bu ses dosyası için ilk payın genlik vektörü s_1, rastgele oluşturulur. Daha sonra oluşturulacak her pay için $2 \leq i \leq n$ olmak üzere $s_1 + s_i = a_i A$ olacak şekilde diğer paylar oluşturulur. Burada a_i değeri sabit bir katsayıdır. Böylelikle oluşturulan n tane paydan her hangi iki tanesi birlikte çalındığında orijinal ses biraz güçlendirilmiş olarak dinlenebilmektedir.

Bu alanda yapılan çalışmalar sadece bilgisayarda depolanan, statik haldeki ses dosyaları üzerinde olmayıp iletim halindeki sesler üzerinde gerçekleştirilen pay oluşturma uygulamaları da mevcuttur. VoIP görüşmelerinde güvenliği sağlamak amacıyla Gizlilik Paylaşımı yönteminin kullanıldığı çalışmalar da gerçekleştirilmiştir. Maheswari ve Punithavalli tarafından birlikte gerçekleştirilen farklı iki çalışmada [51, 52] Shamir'in eşik şeması yöntemi değiştirilerek uygulanmıştır. Bu çalışmaların farkı ise [51] numaralı çalışmada pay ses verilerinin iletimi tekil rota üzerinden gerçekleştirilirken, diğer çalışmada ise çoklu rotalama tekniğinin kullanılmasıdır. 2010 yılında gerçekleştirilen bir diğer çalışmada [53] ise ses verilerinin sıkıştırma işleminden hemen sonra Shamir'in eşik şeması yöntemi bire bir uygulanarak paylar elde edilip her bir pay çoklu rotalama tekniği

ile farklı rotalardan alıcılara iletilmiştir. Ayrıca ses verilerinin iletiminde IPSec protokolü kullanılarak iletişim güvenliği daha da güçlendirilmiştir. Sarma'nın gerçekleştirmiş olduğu çalışmada [54] ise Görsel Gizlilik Paylaşımı tekniği kullanılmıştır. Bu çalışmaya göre, sıkıştırılmış olan ses verisi alıcıya gönderilmeden önce 256 bitlik parçalara ayrılıp resme dönüştürüldükten sonra Naor ve Shamir'in Görsel Gizlilik Paylaşımı tekniği ile paylar elde edilir. Sonrasında her bir pay çoklu rotalama yapılarak farklı portlardan alıcıya gönderilir. Alıcı tarafta, iki pay resimden orijinal resim elde edildikten sonra tekrardan sese dönüştürülüp alıcının sesi dinlemesi sağlanmaktadır. Bir diğer çalışmada [55] ise VoIP güvenliğini sağlamak için steganografi tekniği kullanılmıştır. Bu teknik Lagrange interpolasyonu ve LACK [56] steganografi tekniğinin birlikte kullanılmasına dayandırılmıştır. Çalışmada hata toleransını azaltmak için Shamir'in (k, n) eşik şeması yönteminin biraz değiştirilerek kullanıldığı belirtilmiştir. Ayrıca çalışmada, Lagrange interpolasyon tekniğinin VoIP steganografisinde kullanılan diğer bazı tekniklere göre (Hamming Code, CRC vb.) güvenliği sağlama konusunda daha etkili olduğu ifade edilmiştir.

3. SHAMİR'İN GİZLİLİK PAYLAŞIMI YÖNTEMİNİN MATLAB ORTAMINDA SES DOSYALARINA UYARLANMASI

Gizlilik Paylaşımı yönteminin en önemli özelliklerinden bir tanesi yeterli sayıda pay bir araya getirilmeden orijinal veri hakkında bilgi sahibi olunamamasıdır. Bunun için elde edilecek herbir pay dosyasının orijinal dosyaya benzerlik oranının minimum olması veya hiç benzememesinin sağlanabilmesi çok önemlidir. Eğer bir sayıyı gizlemeye çalışıyorsak ya da gizlenecek dosya ASCII, EBDIC gibi kodlanmış karakterlerden oluşan bir metin dosyası ise bu dosyalardan Shamir'in Gizlilik paylaşımı yöntemiyle elde edilecek pay dosyalarının orijinal dosyaya benzeme ihtimali azdır. Fakat bir ses veya resim dosyasında ise paylar orijinal dosyaya benzerlik gösterebilmektedir. Bunun nedeni Shamir'in yönteminde gizlenecek olan verilere sabit değerlerin eklenmesinden kaynaklanmaktadır. Ses veya resim dosyalarında her bir örneklenmiş ses genliği veya resmin piksel değerlerine sabit değerlerin eklenmesi neticesinde elde edilen pay dosyaları orijinal ses dosyasının biraz gürültülü hali veya orijinal resim dosyasının renk tonlarının değişmiş hali olacaktır. Bu durum Shamir'in Gizlilik Paylaşımı yönteminin ses ve resim dosyalarında direk olarak uygulanamayacağını göstermektedir. Bu nedenle, Thien ve Lin, ilk olarak resim dosyasının herhangi bir anahtar değeri ile permüte edilmesini tavsiye etmişlerdir [3, 42]. Bu şekilde hem güvenliğin artırılması hem de söz konusu benzerliğin azaltılması sağlanmıştır.

Bu tez çalışmasında ise pay dosyalarının orijinal dosyaya benzerlik probleminin çözümü için, orijinal ses dosyası paylar elde edilmeden önce bir önişleme tabi tutulmuştur [57]. Bu önişlem ses genliklerinin karıştırılması işlemidir. Bunun için orijinal ses dosyasındaki örneklenmiş genlik değer dizilimleri değiştirilerek, karıştırılmış yeni bir ses dosyası elde edilmiştir. Daha sonra genlik dizilimleri karıştırılmış olan bu dosyadan Shamir'in Gizlilik Paylaşımı yöntemi ile paylar elde edilmiştir. Orijinal dosyanın elde edilme aşamasında, paylar aracılığı ile elde edilecek olan ses karıştırılmış ses olacaktır. Bu nedenle paylar aracılığı ile karıştırılmış olan ses elde edildikten sonra, bu karıştırılmış sesin dizilimleri ilk aşamanın tersi şeklinde değiştirilerek orijinal ses dosyası elde edilebilmektedir. Sunulan bu teknikle tek kanallı bir ses dosyasından payların elde edilmesi ve paylar aracılığı ile orijinal ses dosyasının tekrardan oluşturulması süreci üç aşamada izah edilebilir [57].

a. Ses verilerinin dizilimlerinin karıştırılması işlemi: Tek kanallı bir ses dosyası tek boyutlu bir dizi/vektör formundadır. Bu aşamada ilk olarak vektör formundaki orijinal ses verileri MxN'lik bir matris formatına dönüştürülür. Bu işlem, oluşturulan MxN'lik matristen tekrar bir dizi vektör elde edildiğinde, bu dizi orijinal ses vektöründen farklı olacak şekilde gerçekleştirilir. Ses vektörünün matris formatına dönüştürülmesi şu aşamalardan oluşur:

1 – Çarpımları ses vektörünün uzunluğuna eşit olacak şekilde, birbirine yakın M ve N sayıları seçilir. Çünkü M ve N değeri bir birine ne kadar yakın değerler olursa ses verileri de o kadar fazla karışmış olacaktır. Bu nedenle uygulamada ses vektörünün uzunluğunun bir tam kare olup olmadığına bakılır. Eğer bir tam kare ise M ve N bu sayının kareköküne eşit olur. Eğer uzunluk değeri tam kare bir sayı değilse bu durumda M ve N değeri bu sayının kareköküne yakın iki tam sayı seçilerek elde edilir. Bu durumda da ses dosyasının boyutunda biraz büyüme olacaktır.

2 – Ses dizisinin ilk N elemanı birinci satırda, ikinci N tanesi ikinci satırda olacak şekilde MxN boyutunda bir matris oluşturulur. Eğer M ile N değerlerinin çarpımı ses dosyasının uzunluğundan büyükse kalan kısımları doldurmak için herhangi bir değer kullanılabilir. Uygulamada bu değer 0 olarak alınmıştır.

3 – MxN uzunluğundaki matrisin elemanları ilk sütundan başlayarak yan yana yazılır. Matrisin bütün sütunları (N adet) birleştirilerek karıştırılmış yeni bir S elemanlı (S=MxN) ses vektörü elde edilmiş olur.

b. Payların elde edilmesi veya birleştirilmesi işlemi: k ve n değerleri belirlenerek birinci aşamada elde edilen karıştırılmış ses dosyasından Eşitlik.2.1'e göre n adet pay elde edilir. Karıştırılmış sesten elde edilmiş olan pay dosyaları orijinal ses dosyasından farklı olmaktadır. Paylardan karıştırılmış ses dosyasının elde edilmesi ise paylardan herhangi k tanesinin Eşitlik.2.2' ye göre hesaplanmasıyla gerçekleştirilir.

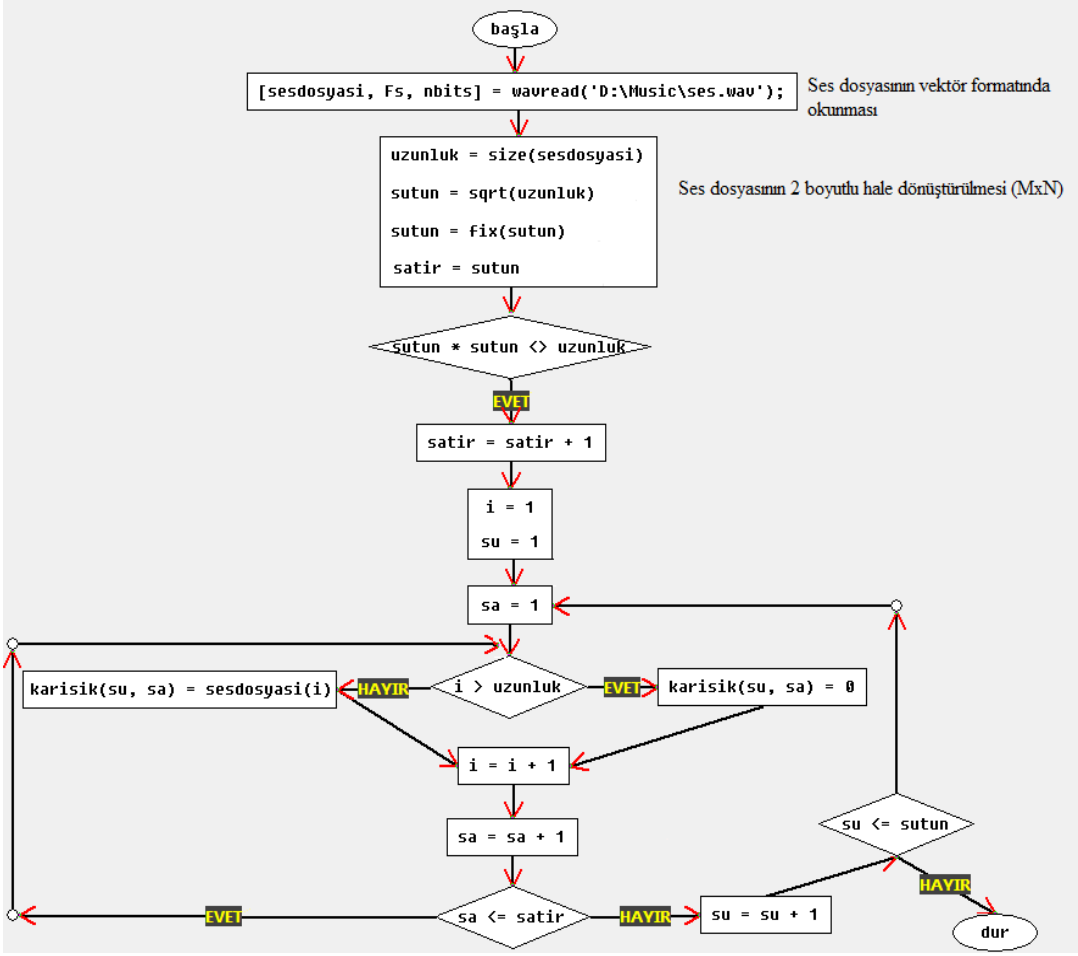
c. Orijinal ses dosyasını elde etme işlemi: Paylar aracılığı ile karıştırılmış ses dosyası elde edildikten sonra orijinal ses dosyasını elde etmek için ilk aşamada gerçekleştirilen karıştırma işleminin tersi uygulanarak ses verilerinin dizilimlerinin normal sıralaması elde edilir. Bu süreç üç aşamada izah edilebilir.

1 – Ses genlik verileri ile MxN boyutundaki bir matris oluşturulur. Bu matrisin her bir sütununda ses verilerinin sırayla M tanesi yer alır. İlk M ses verisi birinci sütunda, ikinci M tanesi ikinci sütunda olacak şekilde N sütunlu matris oluşturulur.

2 – MxN boyutundaki bu matrisin elemanlarının, ilk satırdan başlayarak sırayla yan yana gelecek şekilde tüm satırların birleştirilmesiyle tek boyutlu ses dosyası elde edilmiş olur.

3 – Eğer M ile N'in çarpımı ses dosyasının uzunluğundan büyükse, ilk aşamada MxN boyutundaki matrisi oluşturabilmek için eklenen değerler silinir. Böylelikle orijinal ses dosyası elde edilmiş olur.

Burada izah edilen teknik MATLAB ortamında wav formatındaki tek kanallı bir ses dosyasında uygulanmış olup işlemin akış diyagramı Şekil 3.1'de gösterilmiştir.

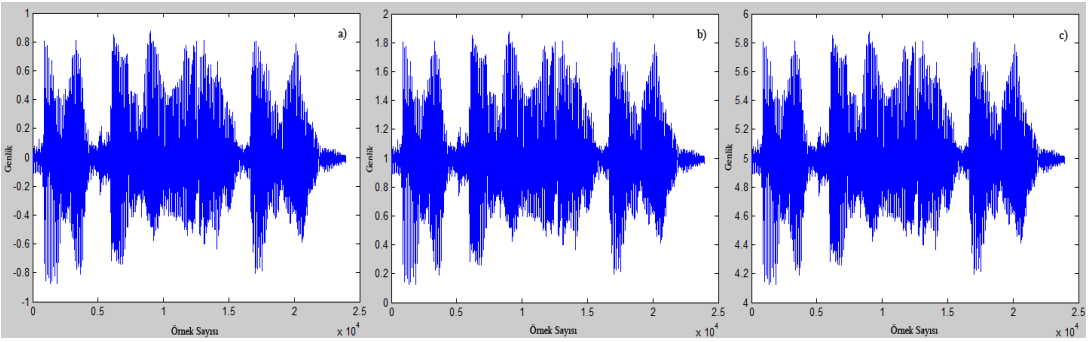


Şekil 0.1 Ses dizilimlerinin karıştırılması işleminin akış diyagramı

Uygulama için 24086 byte büyüklüğündeki konuşma içeren bir ses dosyası kullanılmıştır. Bu ses dosyasına ait bazı başlık bilgileri, Sample Rate: 11025, Byte Rate: 11025, Block Align:1, Bit Per Sample:8 şeklindedir.

İlk olarak ses dosyasından, k=3 ve n=5 olacak şekilde herhangi bir ön işlem yapmadan 5 adet pay oluşturulmuştur. Bu şekilde elde edilen paylar incelendiğinde, pay

dosyalarının orijinal ses dosyasına benzediği ve pay dosyalarından elde edilen seslerin de orijinal sese benzediği ve biraz gürültülü olarak dinlenebildiği tespit edilmiştir. Bu sonucu göstermek için orijinal ses dosyasının ve orijinal ses dosyasından elde edilen birinci ve ikinci pay dosyasının örnek – genlik grafikleri Şekil 3.2'de gösterilmiştir.



Şekil 0.2 Tek kanallı konuşma sesinden Shamir'in yöntemine göre payların elde edilmesi a) Orijinal ses b) 1.pay c) 2 pay genlik-örnek sayısı grafiği

Her üç grafik de incelendiğinde, normalize genlik değerlerinin örneklenmiş zamana göre birbirlerine benzediği görülmektedir. Bu benzerlik istenmeyen bir durum olup bu durumun önüne geçmek için, payların elde edilmesinden önce yukarıda izahı yapılan ses dizilimlerinin karıştırılması işlemi uygulanarak payların oluşturulması işlemi yeniden gerçekleştirilmiştir. Bu işleme örnek olması amacıyla 16 elemanlı bir dizi üzerinde yapılan işlem Şekil 3.3'te gösterilmiştir.

S = [23 76 54 49 88 35 71 121 96 48 17 61 28 37 58 94]

$$L = \begin{bmatrix} 23 & 76 & 54 & 49 \\ 88 & 35 & 71 & 121 \\ 96 & 48 & 17 & 61 \\ 28 & 37 & 58 & 94 \end{bmatrix}$$

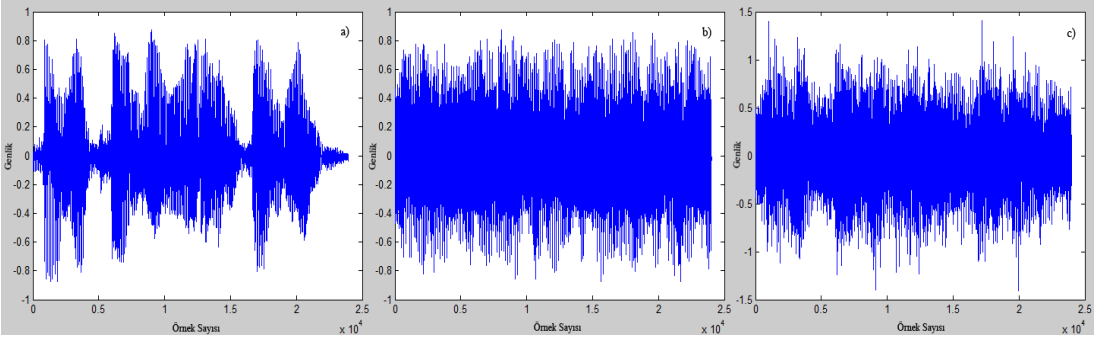
K = [23 88 96 28 76 35 48 37 54 71 17 58 49 121 61 94]

Şekil 0.3 16 elemanlı bir dizinin elemanlarının karıştırılması.

Şekil 3.3'te görüldüğü gibi 16 elemanlı bir S dizisinden 4x4 boyutunda bir L matrisi elde ediliyor. Bunun için dizinin ilk dört elemanı birinci satıra sonraki dört elemanı ikinci satıra gelecek şekilde matris oluşturulmaktadır. Sonrasında L matrisinin ilk sütunu

dizinin ilk elemanlarını oluşturacak şekilde sütunlar sırayla birleştirilerek K dizisi elde ediliyor. Kısaca S vektörünün elemanları satır bazlı yazılıp sütun bazlı birleştirilmektedir. Böylelikle karıştırma işlemi tamamlanmış olur.

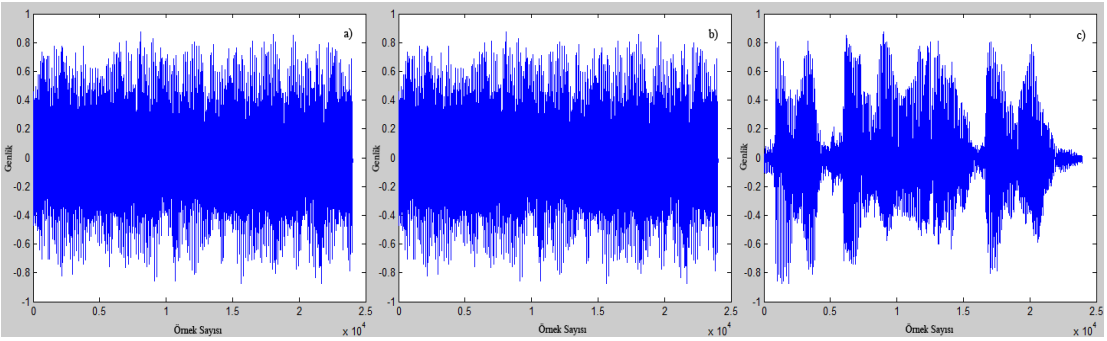
Bu şekilde orijinal ses dosyasının örnekleme verilerinin dizilimlerinin değiştirilmesiyle elde edilen karıştırılmış ses ve orijinal ses dosyası ve her iki dosya arasındaki farkın normalize genlik – örnekleme sayısı grafikleri Şekil 3.4'te görüldüğü gibidir ve orijinal ses ve karıştırılmış ses birbirine benzememektedir.



Şekil 0.4 Orijinal ses dosyasının karıştırılması a) Orijinal ses b) Karıştırılmış ses c) Fark ses genlik-örnek sayısı grafiği

Karıştırılmış diziden orijinal diziye dönüşüm işleminde karıştırma işleminin tersi uygulanmaktadır. Matris oluşturma aşamasında ses verilerinin her bir N tanesi bir satıra gelecek şekilde M satırlı matris oluşturulurken, bu aşamada karıştırılmış ses verilerinin her bir M tanesi bir sütuna gelecek şekilde N sütunlu matris oluşturulur. Sonrasında ise her bir satır sırayla yan yana getirilerek orijinal ses dosyası elde edilmiş olur.

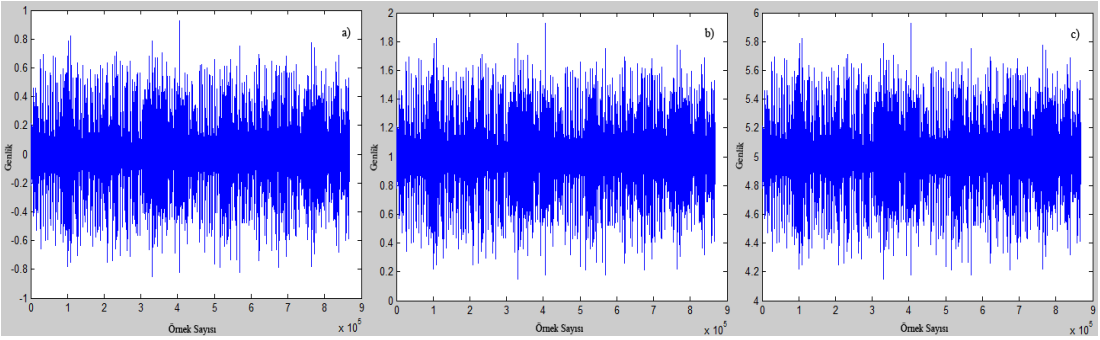
Yukarıdaki şekilde gösterilen karıştırılmış ses ile bu sesten oluşturulan 1, 4 ve 5. paylar ile tekrardan elde edilen karıştırılmış sesin ve orijinal sesin grafikleri Şekil 3.5'te gösterilmiştir.



Şekil 0.5 Paylardan karıştırılmış sesin ve orijinal sesin elde edilmesi a) Karıştırılmış ses b) 1, 4, 5. paylarla elde edilen ses c) Orijinal ses genlik-örnek sayısı grafiği

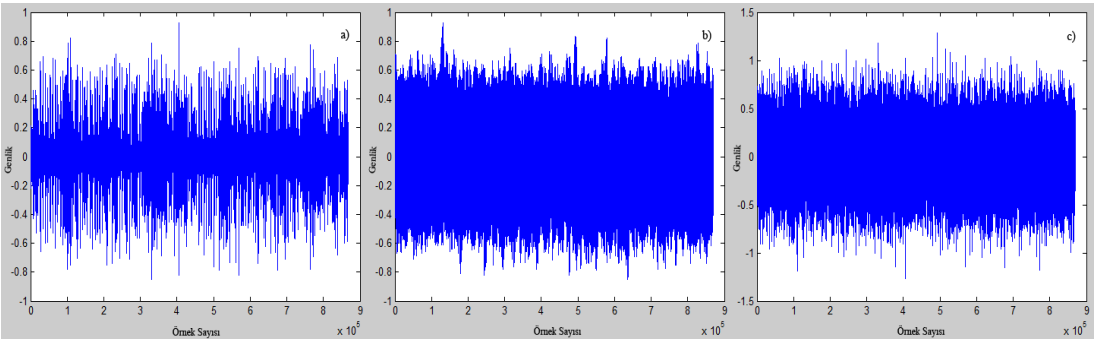
Yukarıda tek kanallı konuşma sesinin karıştırılması sonucunda elde edilen yeni ses ve bu sesten elde edilen pay boyutları 24135 byte boyutunda olup orijinal ses dosyasına göre biraz büyüme olmuştur.

Tek kanallı konuşma sesi içeren ses dosyası için gerçekleştirilen işlemler yine tek kanallı bir müzik dosyası için uygulanmış olup bu işlemlerin sonuçları Şekil 3.6'da gösterilmiştir. 869028 byte büyüklüğündeki bu ses dosyasına ait bazı başlık bilgileri ise Sample Rate: 2000, Byte Rate: 2000, Block Align:1, Bit Per Sample:8 şeklindedir.



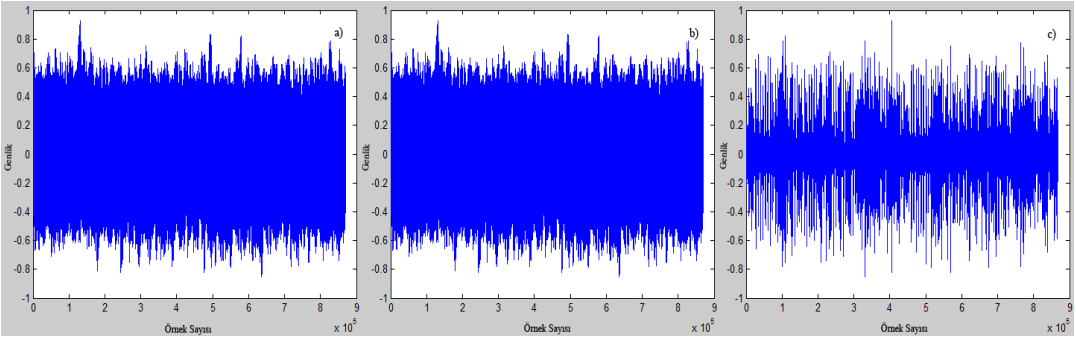
Şekil 0.6 Tek kanallı müzik sesinden Shamir'in yöntemine göre payların elde edilmesi a) Orijinal ses b) 1.pay c) 2 pay genlik-örnek sayısı grafiği

Bu ses dosyası ile gerçekleştirilen uygulama sonucunda da orijinal dosyadan elde edilen payların orijinal dosyaya benzediği Şekil 3.6'da yer alan grafiklerden anlaşılmaktadır. Orijinal sesin karıştırılmış hali ve fark ses grafiği Şekil 3.7'de gösterilmiştir.



Şekil 0.7 Orijinal ses dosyasının karıştırılması a) Orijinal ses b) Karıştırılmış ses c) Fark ses genlik-örnek sayısı grafiği

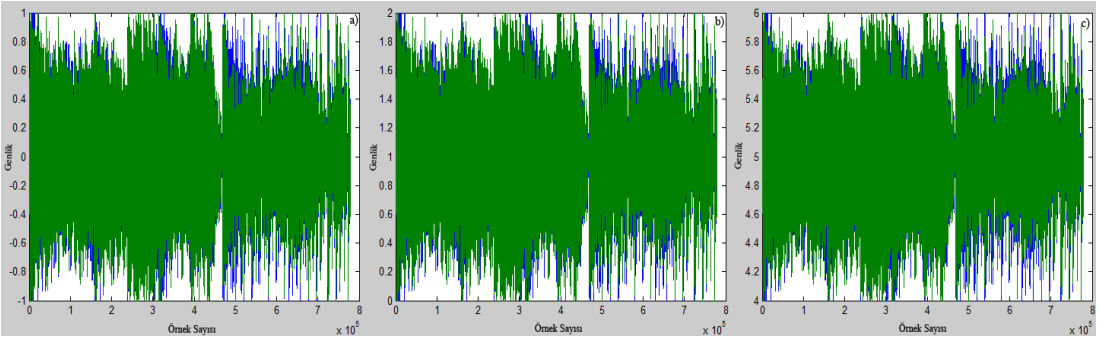
Karıştırma işleminden sonra ses dosyasının orijinal dosyadan farklı olduğu yukarıdaki grafiklerde görülmektedir. Bu nedenle karıştırılmış sesten elde edilen paylar da orijinal dosyaya benzememektedir. Şekil 3.8'de karıştırılmış sesten oluşturulan paylar aracılığı ile yeniden elde edilen karıştırılmış ses dosyası ve sonrasında ses dizilimlerinin tersi şekilde karıştırılarak elde edilen orijinal ses dosyalarının grafikleri gösterilmektedir.



Şekil 0.8 Paylardan karıştırılmış sesin ve orijinal sesin elde edilmesi a) Karıştırılmış ses b) 1, 4, 5. paylarla elde edilen ses c) Orijinal ses genlik-örnek sayısı grafiği

Bu uygulamada ise, karıştırılmış ses ve bu sesten elde dilen payların boyutları 869592 byte büyüklüğündedir. Yine orijinal dosyaya göre paylarda bir miktar büyüme olmuştur.

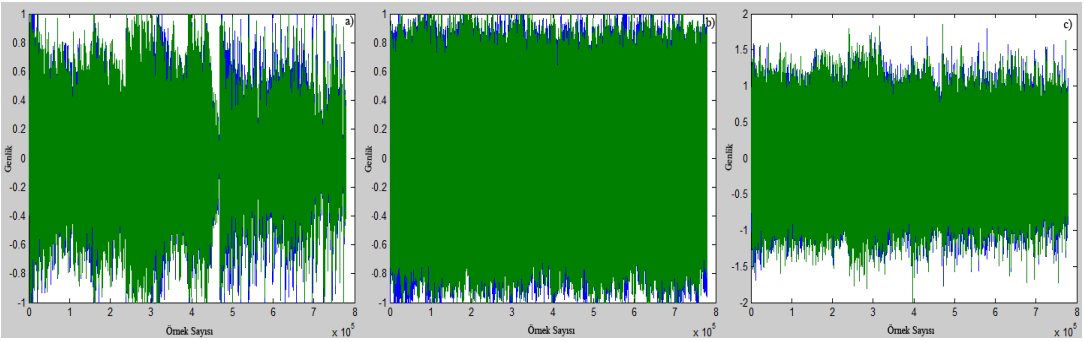
Son olarak yukarıdaki işlemler çift kanallı 3115242 byte büyüklüğündeki bir ses dosyası için de uygulanmış olup bu uygulamanın sonuçları da Şekil 3.9'da gösterilmiştir.



Şekil 0.9 Çift kanallı müzik sesinden Shamir'in yöntemine göre payların elde edilmesi a) Orijinal ses b) 1.pay c) 2 pay genlik-örnek sayısı grafiği

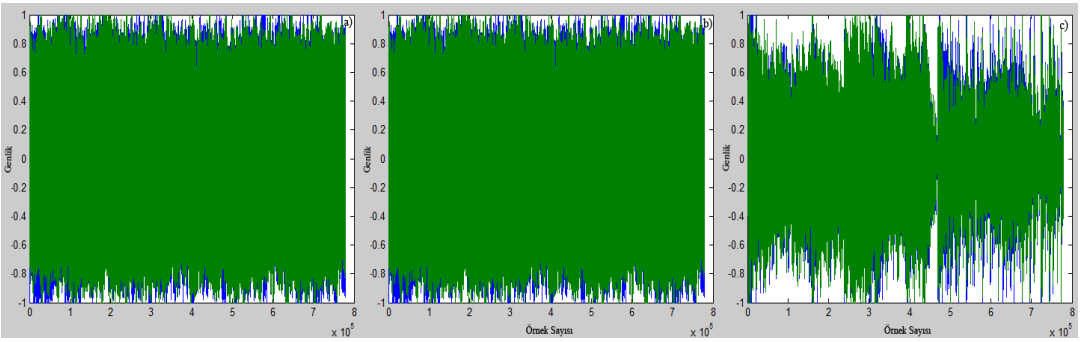
Çift kanallı bu ses dosyasından her hangi bir önişlem uygulanmadan elde edilen payların yine orijinal ses dosyasına benzediği yukarıdaki grafiklerden açıkça görülmektedir. Bu ses dosyasının örnekleme değerlerinin karıştırılması işlemi her iki kanal

içinde gerçekleştirilmiş olup elde edilen yeni ses dosyasının ve fark sesin grafikleri de Şekil 3.10'da gösterilmiştir.



Şekil 0.10 Orijinal ses dosyasının karıştırılması a) Orijinal ses b) Karıştırılmış ses c) Fark ses genlik-örnek sayısı grafiği

Şekil 3.10 – c' deki fark grafiğinden de görüldüğü üzere karıştırılmış ses dosyası orijinal dosyaya benzememektedir.



Şekil 0.11 Paylardan karıştırılmış sesin ve orijinal sesin elde edilmesi a) Karıştırılmış ses b) 1, 4, 5. paylarla elde edilen ses c) Orijinal ses genlik-örnek sayısı grafiği

Bu uygulama neticesinde karıştırılmış ses ve bu sesten elde edilen pay boyutları 3115268 byte büyüklüğünde olup orijinal dosyaya göre bir miktar büyüme olmuştur.

MATLAB ortamında gerçekleştirilen ve sonuç grafikleri yukarıda gösterilen uygulamalardan, karıştırma tekniği uygulanarak orijinal ses dosyasından elde edilen pay dosyalarının orijinale benzemediği ve tek bir pay dosyasından orijinal ses hakkında fazla bir yorum yapılamayacağı sonuçları elde edilmiştir. Bununla birlikte her üç uygulama neticesinde de ses dizilimlerinin karıştırılması sonucu elde edilen yeni ses ve bu karıştırılmış sesten elde edilen payların boyutlarının orijinal dosyaya göre bir miktar arttığı görülmektedir. Bu artışın sebebi, vektör formatındaki ses dosyasını MxN'lik matrise

dönüştürürken matris elemanlarını tamamlamak için 0 değerlerinin eklenmesidir. Büyüme miktarları ilk uygulamada 49 byte, ikinci uygulamada 564 byte, üçüncü uygulamada ise 26 byte kadardır. Ayrıca orijinal dosyadan birden fazla pay elde edildiği ve bu payların her biri orijinal dosya büyüklüğünde olduğu için (bu çalışmada bahsedilen karıştırma tekniği ile elde edilen ses dosyasının payları, orijinal ses dosyasından daha büyük olabilmektedir) depolama alanı ihtiyacı pay sayısı oranınca artmaktadır. Bu ise Gizlilik Paylaşımı yönteminin doğası gereğidir. Günümüz depolama alanları açısından bu büyüme çok fazla bir önem taşımasa da yine de yöntemin bir dezavantajı olarak söylenebilir.

Hem Shamir'in yöntemi hem de ses dizilimlerinin karıştırılması tekniği çok karmaşık matematiksel hesaplamalar içermediğinden dolayı yazılımsal ve donanımsal olarak, gerek bilgisayar sistemlerinde depolanan sabit haldeki, gerekse iletim halindeki ses verilerinin güvenliğini korumak amacıyla gerçeklenebilir bir yöntem özelliği taşımaktadır. Kayıt altına alınan ses dosyalarının yetkisiz kişilerce dinlenmesinin engellenmesi veya dinleme işleminin tek bir kişi yerine belirli sayıda kişinin bir araya gelerek yapabilmesini gerektirecek durumlarda alternatif bir çözüm olarak kullanılabilir. Örneğin müzik albümlerinin ya da albümlerdeki parçaların internet ortamında herkes tarafından dinlenmesi yerine telif hakları doğrultusunda sadece lisans sahibi (ücretini ödemiş / yasal olarak dinleme hakkına sahip) kişilerin dinleyebileceği bir on-line platform gerçekleştirilebilir. VoIP görüşmeleri gibi internet üzerinden sesli iletişim uygulamalarında da iletişimin güvenliğini sağlamak amacıyla ses verilerinden payların oluşturulup her bir payın aynı veya farklı bir rota üzerinden alıcıya gönderilmesi sağlanabilir. Böylelikle iletim hattını dinleyen bir kişi o hat üzerinden geçen pay sesini ele geçirmiş olsa bile orijinal ses hakkında her hangi bir bilgiye sahip olamayacaktır.

4. SHAMİR'İN GİZLİLİK PAYLAŞIMI YÖNTEMİNİN FPGA ORTAMINDA GERÇEKLENMESİ

Gerçekleştirilen FPGA uygulamasında ses dosyalarından Shamir'in Gizlilik Paylaşımı yöntemiyle pay oluşturma süreci donanımsal olarak tasarlanmıştır. Uygulamadaki amaç, ses verilerinin iletiminde güvenlik sağlayıcı bir önlem için öneri sunmaktır. Bu bölümde FPGA hakkında kısaca bilgi verilmiş olup devamında, gerçekleştirilen uygulamanın detayları izah edilmiştir.

4.1. FPGA

FPGA'ler, programlanabilir mantık blokları ile bu bloklar arasındaki değiştirilebilir ara bağlantılardan oluşan sayısal tümleşik devrelerdir [59]. "Field Programmable Gate Array" ifadesinin kısaltılması olan FPGA, "Sahada Programlanabilir Kapı Dizileri" anlamına gelmektedir. Sahada programlanabilir isminin verilmesinin sebebi, üretimden sonraki aşamada tasarımcının kendi ihtiyacı doğrultusunda programlayabilmesidir. Yani kullanıcı her bir mantık bloğunun işlevini gerçekleştireceği fonksiyona göre kendisi düzenleyebilmektedir.

FPGA içerisindeki transistörler birbirinden bağımsız olarak üretilmişlerdir. Kullanıcının belirlediği fonksiyona göre FPGA içerisindeki transistörler birbirlerine bağlanır ve kullanıcının istediği fonksiyon gerçekleştirilir.

FPGA temelde üç ana bölümden oluşmaktadır. Bunlar; mantık hücreleri, bu hücreleri çevreleyen giriş-çıkış blokları ve ara bağlantılardır [60]. Mantık hücreleri ara bağlantılar içerisinde bulunur ve basit fonksiyonların gerçekleştirildiği yapılardır. Giriş – çıkış blokları ise FPGA ile dış çevre arasında bir arayüz görevi görürler.

80'li yıllarda FPGA teknolojisinden önce sayısal tümleşik devre teknolojisi olarak "Programlanabilir Mantık Cihazları (PLD)" ve "ASIC" tasarım bulunmaktaydı. PLD'ler hızlı tasarım ve değişiklik sürecine sahip olsalar da karmaşık tasarımlara destek verememekteydi. ASIC'lerin pahalı olmasıyla birlikte zaman isteyen bir sürece sahip olması ve tasarımda geri dönüşlerinin olmaması ise bu teknolojinin dezavantajıydı. Her iki tümleşik devre teknolojisine rağmen bu alanda hissedilen boşluk Xilinx firmasının FPGA teknolojisini piyasa duyurmasıyla kapanmış oldu. Kullanıma ilk başlandığında genellikle ara yapıştırıcı mantık ve kısıtlı veri işleme işlemlerinde kullanılmışlardır. 1990'ların ilk

yıllarında kapasitelerinin artmasıyla haberleşme gibi geniş veri işlemleri gerektiren alanlarda kullanımı artmıştır [61].

FPGA'ler PLD ile ASIC arasında bir yer işgal ederler [59]. Çünkü FPGA'lerin işlevselliği PLD gibi alana özgü olabilir ve milyonlarca lojik kapı içerebilir. Ayrıca o dönemlerde, sadece ASIC'ler ile gerçekleştirilebilen çok büyük ve karmaşık fonksiyonlar FPGA'ler ile de gerçekleştirilebilmektedir. FPGA ile tasarım maliyetinin ASIC'e göre daha düşük olması ve tasarım değişikliklerinin daha kolay olması FPGA kullanımını arttıran etkenlerden olmuştur.

FPGA'lerin en önemli özelliklerinden birisi de aynı anda birden fazla işlemi yapabilmesi, yani paralel işlem yapabilme kabiliyetidir. Bu özelliği FPGA'in diğer entegrelere göre daha hızlı çalışmasını sağlar. FPGA'lerin 4 temel özelliği şu şekilde belirtilebilir [62]:

1. Sahada Programlanabilme: FPGA'lerin üretimden sonra çalıştığı ortamda programlanabilmesini ifade eder. Her hangi bir sınır olmaksızın programlanabilmesi tasarımcılara büyük kolaylık sağlar.

2. Tasarımın test edilip doğrulanması: Tasarlanan programın FPGA'e yüklenmeden önce bilgisayar ortamında simülasyonunun yapılabilmesidir. Bu özellik hataların önceden fark edilip düzeltilebilmesini sağlamaktadır.

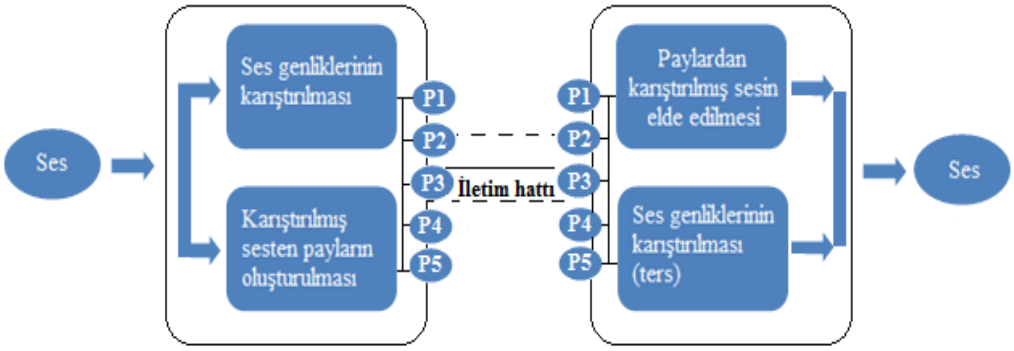
3. Paralel işlem yapabilme: Aynı anda birden fazla işlemi yapabilmesidir. Bu da FPGA'lerin daha hızlı çalışmasını sağlayan bir özellik olmakla birlikte daha karmaşık işlemleri yapılabilmesini sağlar.

4. FPGA'e işlemci gömülmesi: İşlemci gerektiren tasarımlarda FPGA içerisine soft işlemci gömülerek C/C++ gibi dillerle programlanabilmektedir. Bazı FPGA türlerinde birden fazla işlemci dahi tanımlanabilmektedir. Ayrıca fiziksel olarak gömülü işlemcilerin olduğu FPGA'ler de bulunmaktadır.

4.2. FPGA Uygulaması

Bu çalışmada, gerçek zamanlı ses iletimi sürecindeki izinsiz dinlemelere ve seslerin ele geçirilmelerine karşı önemli bir alternatif güvenlik uygulaması olan gizlilik paylaşımı temelli bir donanımsal uygulama açıklanmıştır. Gerçekleştirilen uygulama, ses verilerinin gönderici tarafta gerçek zamanda karıştırılıp paylara ayrılması sonrasında her bir payın farklı veya aynı iletişim hattından alıcıya gönderilmesi ve alıcı tarafta payların

birleştirilerek, ilk olarak karıştırılmış sesin sonrasında da orijinal sesin yine gerçek zamanda elde edilmesini kapsamaktadır. Bu işlemlerin gerçekleştirilme süreci Şekil 4.1'de gösterilmiştir.

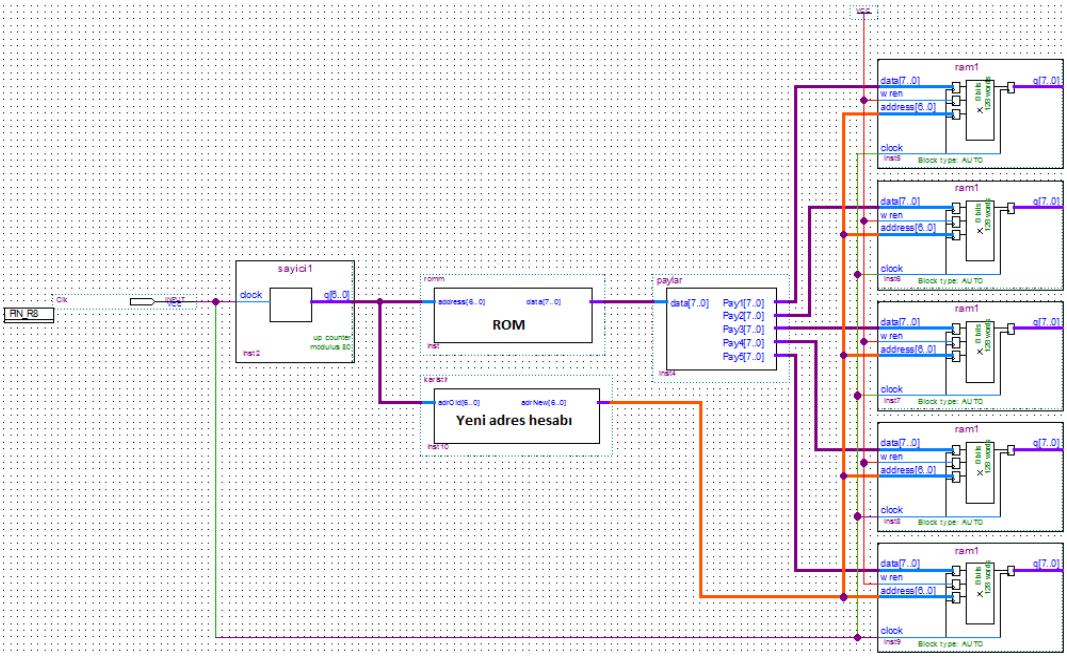


Şekil 0.1 VoIP telefon görüşmesi süreci

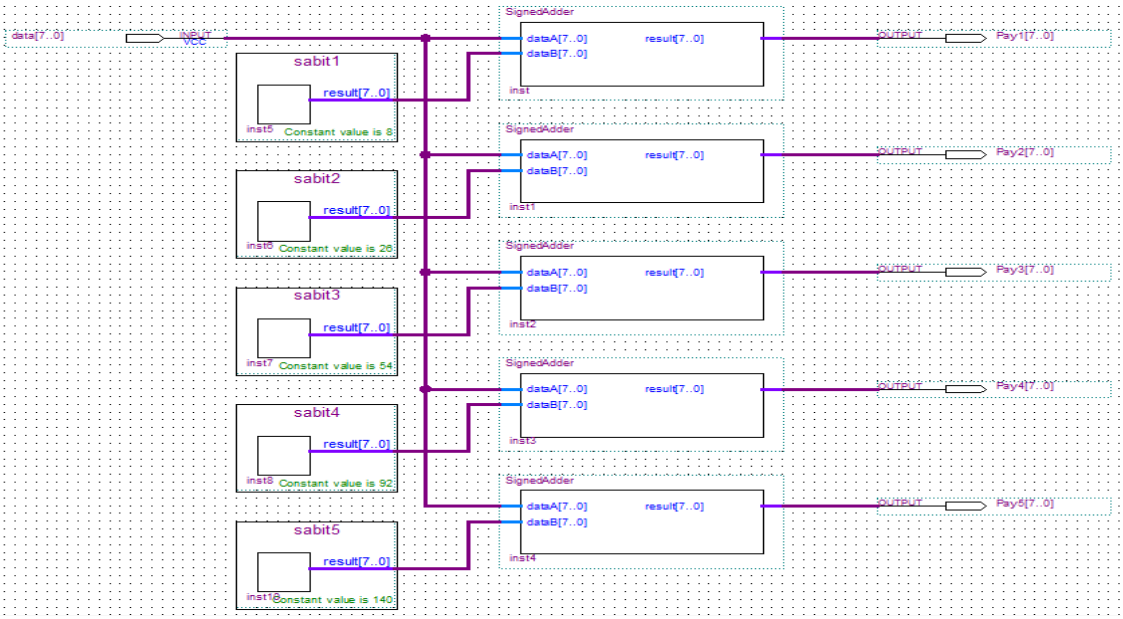
Gerçekleştirilen uygulamanın birinci kısmında örneklenmiş ses genlik verilerinin dizilimlerinin karıştırılarak, orijinal sese benzerliği azaltılmış 5 adet payın elde edilmesi işlemini gerçekleştirecek donanımsal devre VHDL dili ile programlanıp FPGA içerisine gömülmüştür. FPGA ortamında oluşturulmuş donanımsal devrenin blok şeması Şekil 4.2 ve 4.3'te verilmiştir.

Uygulamanın birinci aşamasında ilk olarak vektör formatındaki orijinal ses dosyasının genlik verileri, FPGA ortamında oluşturulan ROM hafıza modülüne ilk adresten başlanarak kaydedilmiştir. Bu çalışmada kullanılan ses genlik vektörü 80 adet örneklenmiş genlik değeri içermektedir. Şekil 4.2'deki devre şemasında görüldüğü gibi, ROM'daki her bir orijinal genlik verisinin, *paylar* ünitesine sırayla uygulanması için 7 bitlik bir ROM adres sayıcı kullanılmıştır. ROM'un her bir adresinden okunan örneklenmiş ses değeri, Şekil 4.2'de görülen paylar ünitesinin girişine uygulanmaktadır. Paylar ünitesinde birbirinin aynısı 5 adet pay birimi vardır. Bu birimler Denklem.1'e göre pay verisi üretmektedir. Bunlar eşzamanlı ve paralel çalışarak, girişten okunan her bir orijinal ses verisinden bir birim zamanda 5 adet pay verisini oluştururlar. Buna göre 80 adet örneklenmiş ses verisinin 5 paya ayrılması sadece 80 birimlik zamanda gerçekleşmiş olur. Elde edilen her bir payın orijinal sese benzerliğinin önüne geçmek için, paylara ayrılmış veriler Bölüm.3'te önerilen karıştırma tekniğini sağlayacak şekilde RAM'deki ayrı hafıza yerlerine kaydedilmelidirler. Bu işlemi yapmak için FPGA'da *karistir* isimli bir ünite

oluşturulmuştur. Böylelikle paylara ayrılan her bir orijinal veri karıştırma tekniğine uygun olarak ilgili adreslere yazılabilmektedir.



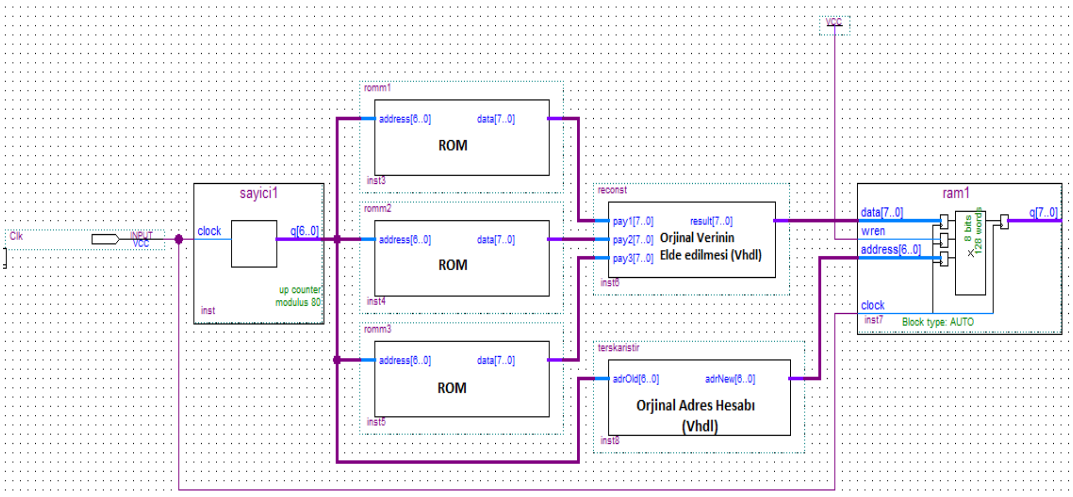
Şekil 4.2 Payların oluşturulup kaydedilme süreci devresi



Şekil 4.3 Pay oluşturma devresi (paylar modülü)

Gerçekleştirilen uygulamada, 5 adet payın oluşturulması için $P(x) = a_0 + 3x + 5x^2$ polinomu uygulanmıştır. Burada a_0 gizlenmek istenen ses genlik verisi, x ise oluşturulacak payın indeks numarasıdır. Buna göre x değeri, birinci pay için 1, ikinci pay için 2, beşinci pay için 5 alınarak hesaplanır. Uygulamada işlem kolaylığı ve daha hızlı işlem yapabilmek için bu polinomda gizlenmek istenen a_0 genlik verisine eklenen $3x + 5x^2$ ifadesi sabit değerler olarak eklenmiştir. Bu sabit değer birinci pay için $3*1 + 5*1^2 = 8$ şeklinde olup diğer paylar için de benzer şekilde hesaplanarak Şekil 4.3'te görülen pay oluşturma devresinde, sabit1…sabit5 birimlerinde gösterildiği gibi eklenmiştir. Bu şekilde gerçekleştirilen uygulamada payların elde edilmesi aşamasında her bir örnekleme değerinden 5 adet payın oluşturulup RAM'lere kaydedilme sürecinde, payların oluşturulması aşamasında 5 adet toplama, pay verilerinin karıştırılması işleminde 1 adet çarpma ve 1 adet mod alma işlemi gerçekleştirilmiştir. 80 adet örnekleme değeri içeren ilk ses için gerçekleştirilen uygulamada 400 adet toplama, 80 adet çarpma ve 80 adet mod alma işlemi gerçekleştirilmiş olmaktadır.

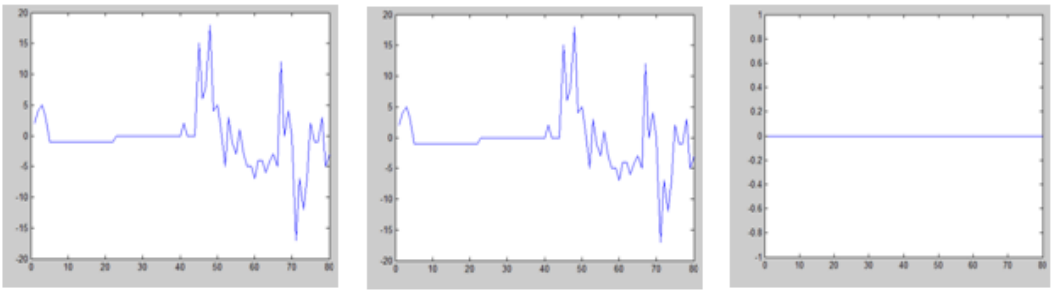
Uygulamanın ikinci kısmında ise paylardan orijinal verinin elde edilmesi işlemi gerçekleştirilir. Gelen 5 paydan her hangi 3'ünün kullanılarak orijinal sesin elde edilmesini sağlamak için FPGA ortamında oluşturulmuş donanımsal devre Şekil 4.4'te verilmiştir.



Şekil 0.2 Paylardan orijinal verinin elde edilme devresi

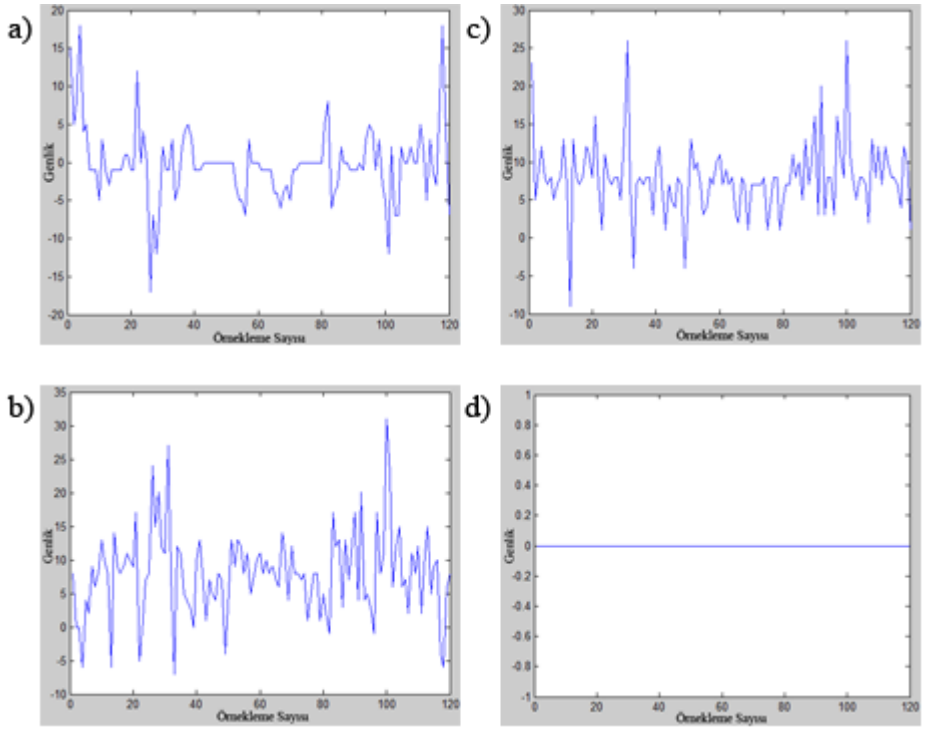
Uygulamada, herhangi 3 pay dosyası kullanılarak orijinal ses dosyasının elde edilmesi gerçekleştirilmiştir. Şekil 4.4'te görüldüğü gibi ROM hafızadaki pay verileri *reconst* modülüne giriş olarak verilmiştir. Reconst modülü, Denklem.2.3'e göre ses genliğinin orijinalini hesaplamak için oluşturulmuş donanımdır. Hangi sıradaki ses

genliğinin orijinalinin elde edileceğini belirlemek için sayıcı, genlik değerlerinin orijinal sıralamasını belirlemek için de *ters karıştır* modülü tasarlanmıştır. Böylelikle paylardan orijinal ses genlik değerleri elde edilirken aynı zamanda bu genliklerin orijinal sıralaması da bulunarak Şekil 4.4'te gösterilen RAM'e kaydedilir. Elde edilen sesin orijinal sese birebir benzediği Şekil 4.5'te gösterilmiştir. Şekil 4.5'te görüleceği üzere orijinal ses ve paylardan elde edilen ses benzer olup iki ses arasındaki fark sıfırdır. Paylardan orijinal sesin elde edilmesi ve RAM'e kaydedilmesi sürecinde, paylardan orijinal ses genliğinin elde edilmesi aşamasında 2 adet çarpma 1 adet toplama 1 adet çıkarma ve 1 adet mod alma işlemi gerçekleştirilmiştir. Elde edilen ses genliğinin orijinal sırasını hesaplamak için ise, 1 adet çarpma ve 1 adet mod alma işlemi gerçekleştirilmiştir. Bu aşamada da 80 adet örnekleme değeri içeren sesin elde edilmesinde toplamda 240 adet çarpma, 80 adet toplama, 80 adet çıkarma ve 160 adet mod alma işlemi gerçekleştirilmiştir.



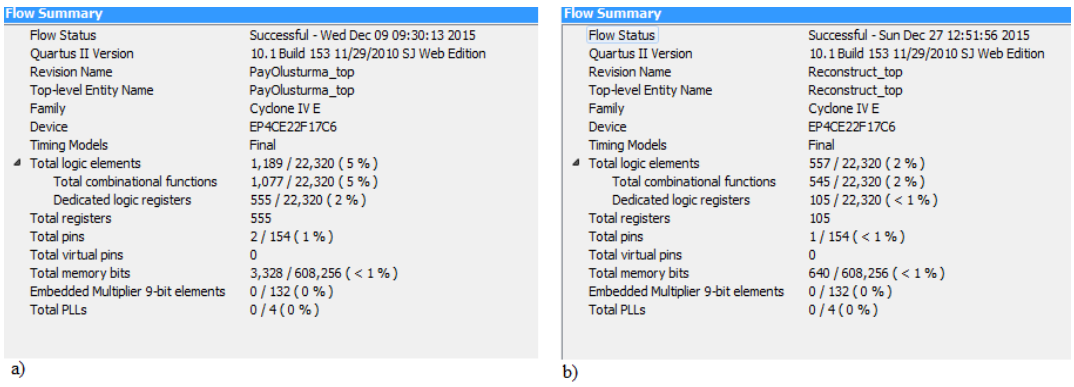
Şekil 4.5 Orijinal ses ile FPGA ortamında paylardan elde edilen sesin karşılaştırılması a) Orijinal ses b) Paylardan elde edilen ses c) Fark ses grafiği

Uygulamanın her iki aşaması 120 adet örnekleme değeri içeren başka bir ses dosyası için tekrar test edilerek, 5 adet pay oluşturulmuş ve bu paylardan 3 tanesi ile orijinal sesin elde edilmesi işlemleri gerçekleştirilmiştir. 5 adet payın elde edilmesi aşamasında toplamda 600 adet toplama, 120 adet çarpma ve 120 adet mod alma işlemi gerçekleştirilmiştir. Herhangi 3 adet pay ile orijinal sesin elde edilmesi aşamasında ise, 360 adet çarpma, 120 adet toplama, 120 adet çıkarma ve 240 adet mod alma işlemi gerçekleştirilmiştir. Bu sesten elde edilen payların da orijinal sese benzemediği ve paylardan orijinal sesin başarılı bir şekilde elde edildiği sonucuna ulaşılmıştır. Sonuç olarak hata değeri 0 elde edilmiştir. Bu sonuçları gösteren grafikler şekil 4.6'da verilmiştir.



Şekil 4.6 Uygulama sonuçlarının grafiksel gösterimi **a)** Orijinal ses **b)** Birinci pay **c)** Birinci pay ile orijinal ses farkı **d)** Paylardan elde edilen ses ile orijinal ses farkı grafiği

Sesten payların oluşturulması ve paylardan orijinal sesin oluşturulması basit toplama ve çarpma işlemlerini içermektedir. Sesten payların oluşturulması ve paylardan orijinal sesin elde edilmesi için gerçekleştirilen FPGA uygulamasında harcanan sistem kaynakları Şekil 4.7'de verilmiştir. Şekil 4.7'den görüleceği üzere sistemde harcanan toplam lojik eleman sayısı toplam lojik eleman sayısının %5 ve %2' si kadardır.



Flow Summary

Flow Status	Successful - Wed Dec 09 09:30:13 2015
Quartus II Version	10.1 Build 153 11/29/2010 SJ Web Edition
Revision Name	PayOlusturma_top
Top-level Entity Name	PayOlusturma_top
Family	Cyclone IV E
Device	EP4CE22F17C6
Timing Models	Final
Total logic elements	1,189 / 22,320 (5 %)
Total combinational functions	1,077 / 22,320 (5 %)
Dedicated logic registers	555 / 22,320 (2 %)
Total registers	555
Total pins	2 / 154 (1 %)
Total virtual pins	0
Total memory bits	3,328 / 608,256 (< 1 %)
Embedded Multiplier 9-bit elements	0 / 132 (0 %)
Total PLLs	0 / 4 (0 %)

a)

Flow Summary

Flow Status	Successful - Sun Dec 27 12:51:56 2015
Quartus II Version	10.1 Build 153 11/29/2010 SJ Web Edition
Revision Name	Reconstruct_top
Top-level Entity Name	Reconstruct_top
Family	Cyclone IV E
Device	EP4CE22F17C6
Timing Models	Final
Total logic elements	557 / 22,320 (2 %)
Total combinational functions	545 / 22,320 (2 %)
Dedicated logic registers	105 / 22,320 (< 1 %)
Total registers	105
Total pins	1 / 154 (< 1 %)
Total virtual pins	0
Total memory bits	640 / 608,256 (< 1 %)
Embedded Multiplier 9-bit elements	0 / 132 (0 %)
Total PLLs	0 / 4 (0 %)

b)

Şekil 4.7 FPGA uygulama aşamalarının işlem özeti **a)** Pay oluşturma uygulaması **b)** Paylardan orijianal sesin elde edilmesi uygulaması

Uygulama sonuçları analiz edilerek, gerçekleştirilen FPGA donanımı ile oluşturulan payların orijinal sese benzemediği, paylardan elde edilen sesin orijianl sesin bire bir aynı olduğu ve gerçekleştirilen uygulamanın gerçek zamanlı uygulamalar için kullanılabilir bir alternatif olabileceği sonuçlarına ulaşılmıştır.

5. GİZLİLİK PAYLAŞIMI YÖNTEMİYLE SES DOSYASI ARŞİVLEME UYGULAMASI

İletim halindeki veriler gibi bilgisayar sistemlerinde depolanan statik haldeki veriler de korumasız bir durumdadır ve tedbir alınmadığı takdirde yetkisiz kişiler tarafından içeriğin ele geçirilmesi, değiştirilmesi gibi saldırılara maruz kalabilirler. Bu bölümde, ses dosyalarını bu tarz saldırılardan koruyarak yetkisiz kişilerce ele geçirilse dahi dinlenmesini önlemek veya işe özel olarak sadece belirli sayıda kişinin bir araya gelerek birlikte dinlemesi gereken durumlar için bir "Ses Dosyası Gizli Arşivleme Yazılımı - SDGAY" aracının geliştirilme süreci izah edilmiştir [58]. Ses dosyalarının güvenli bir şekilde arşivlenmesini sağlayan bu yazılım aracıyla ses dosyaları öncelikle özel pay dosyalarına dönüştürülmekte ve pay dosyalarının orijinal ses dosyasına bezerliği minimuma indirilerek arşivlenmektedir. Böylelikle pay dosyaları tek başına ele geçirilse dahi orijinal ses hakkında bilgi edilmemesi sağlanmıştır.

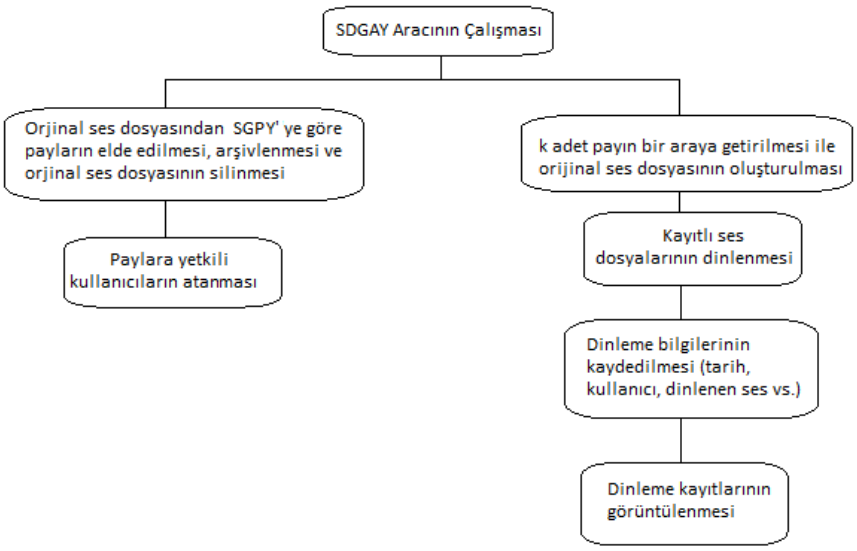
Geliştirilen yazılımda, öncelikle ses dosyalarından paylar elde edilir ve her bir pay sunucularda arşivlenir. Payların elde edilmesi Gizlilik Paylaşımı yöntemiyle gerçekleştirilir. Kullanıcılara ses dosyalarına erişim yetkisi sadece tek bir pay için verilir. Yani her bir kullanıcının orijinal ses dosyasının tek bir payına erişim izni vardır. Bu nedenle bir kullanıcı tek başına bir ses dosyasını dinleyememektedir. Her hangi bir ses dosyasının dinlenebilmesi için en az k adet payın bir araya getirilmesi gerekmektedir. Bunun için k sayıda kişi bir araya gelerek, her biri yetkili oldukları payların sisteme yüklenmesini sağlar ve orijinal sesin dinlenmesi gerçekleştirilir. Böylelikle ses dosyalarının yetkisiz kişiler tarafından dinlenmesi de önlenmiş olur.

Visual Studio ortamında C# dili ile MSSQL kullanılarak geliştirilen SDGAY aracı; ses dosyalarının paylara ayrılıp veri tabanında saklanması ve seslerin dinlenmesi için en az k tane erişim izni olan kişinin bir araya gelmesini gerektirecek şekilde tasarlanmıştır.

Geliştirilen SDGAY aracında; arşivlenmek istenen ses dosyalarından, ses gizlilik paylaşımı yöntemine göre n adet pay oluşturulur ve her bir pay veri tabanına kaydedildikten sonra orijinal ses dosyası silinir. Payların kaydedildiği sunucular istenildiği takdirde farklı olarak ayarlanarak her bir payın farklı bir sunucuda saklanması sağlanabilir. Böylelikle bir sunucunun çalışmadığı durumlarda sistem bu olumsuzluktan etkilenmeyecek ve çalışmasına devam edecektir. Ayrıca, orijinal sesten elde edilen paylar tek başlarına orijinal sese ait bir bilgi vermediğinden dolayı, her hangi bir sunucudaki verilerin kötü

niyetli kişilerin eline geçmesi durumunda orijinal ses hakkında bilgi sahibi olamayacaklardır. Bu da uygulamanın güvenliğini önemli bir ölçüde arttırmaktadır.

Temelde iki kısımdan oluşan yazılımın birinci aşamasında orijinal ses dosyalarından payların elde edilmesi ve bu paylara yetkili kullanıcıların atanması işlemleri gerçekleştirilir. Bu aşamanın işleyişi aşağıdaki şekilde gösterildiği gibidir.



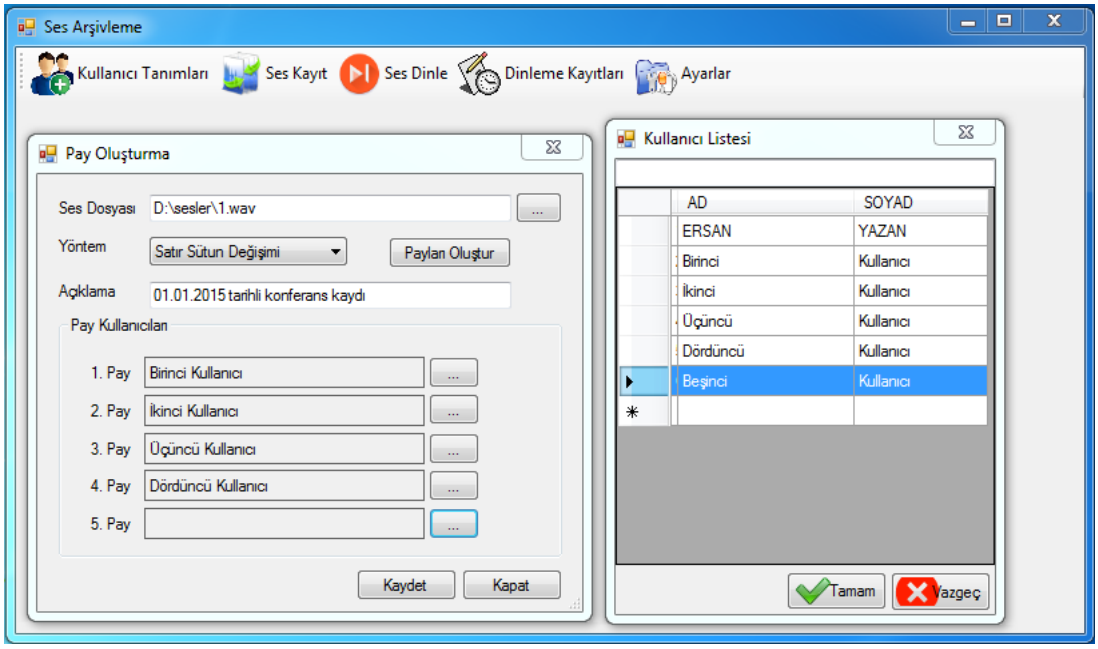
Şekil 0.1 SDGAY aracının işleyiş şeması[58]

İkinci aşamada ise, payların birleştirilerek orijinal ses dosyasının geri elde edilmesi, bir sesin ne zaman hangi kullanıcılar tarafından dinlendiğinin ve yetkisiz kişilerin dinleme teşebbüslerinin kayıt altına alınması işlemleri gerçekleştirilir.

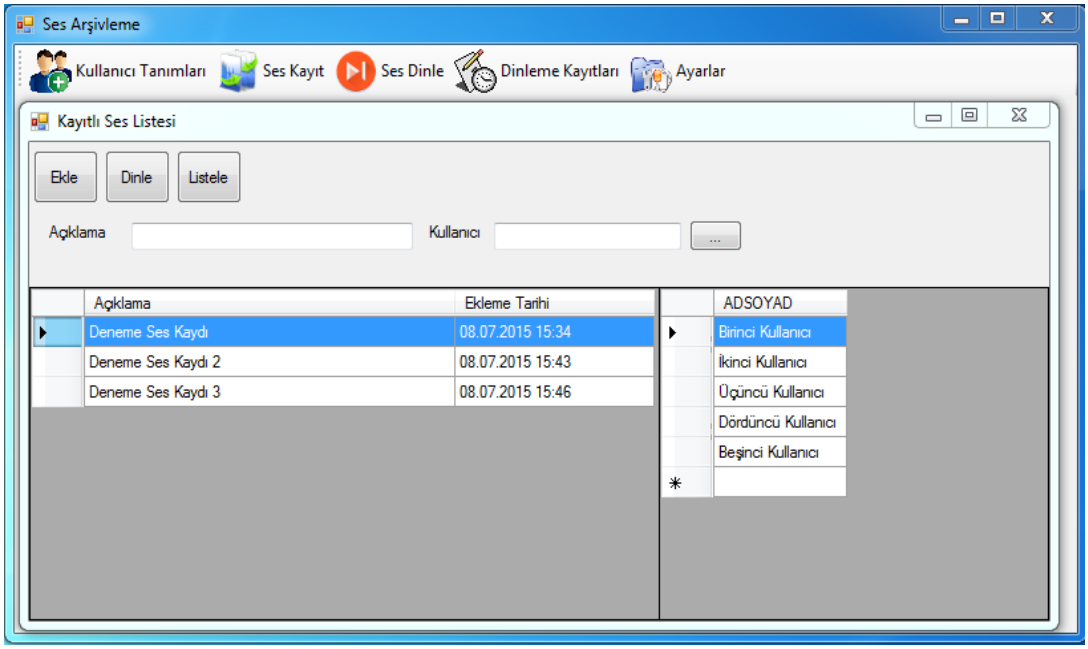
Geliştirilen SDGAY aracının amacı, ses dosyalarının paylar şeklinde arşivlenerek, ses dosyalarına erişebilmek için k sayıda yetkili kişinin bir araya gelmesini sağlamaktır. Bunun için yazılımda her bir ses dosyasından paylar oluşturulup, bu paylar aynı veya farklı sunucularda saklanır. Ses dosyasından payların oluşturulmasında ikinci bölümde izahı yapılan Shamir'in Gizlilik Paylaşım yöntemi kullanılmıştır. Payların orijinal dosyaya benzerliğinin azaltılması ise üçüncü bölümde izah edilen karıştırma tekniği ile gerçekleştirilmiştir. Her hangi bir ses dosyasının dinlenebilmesi için arşivlenmiş en az k tane payın biraraya getirilmesi gerekmektedir. Öncelikle bu paylar ile karıştırılmış ses elde edilir sonrasında da ters karıştırma işlemi gerçekleştirilerek orijinal ses dosyası elde edilir.

Yazılımsal araçta iki türlü kullanıcı mevcuttur. Bunlar, sistem yöneticisi ve normal kullanıcı. Sistem yöneticisi tarafından gerçekleştirilen işlemler, kullanıcı tanımları, ses pay dosyalarının oluşturulması 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.

Aşağıdaki şekilde ekran görüntüsü verilen uygulamada kullanıcı tanımlama ekranında sistem yöneticisi kullanıcılarla ilgili işlemleri (kullanıcı oluşturma, kullanıcı bilgilerini güncelleme ve silme) gerçekleştirir. Ses kayıt ekranında ise arşivlenmek istenen ses dosyasından payların oluşturulup kaydedilmesi sağlanır. Burada pay oluşturulacak ses dosyası seçildikten sonra her bir pay için yetkili kullanıcı seçilir. Burada seçilen kullanıcılar, o ses dosyasının dinlenmesi için yetkilendirilmiş kullanıcılardır. Arşivde saklanan bir ses dosyasının dinlenmesi bu ekranda seçilen kullanıcılardan her hangi üçünün parolası ile gerçekleştirilir.

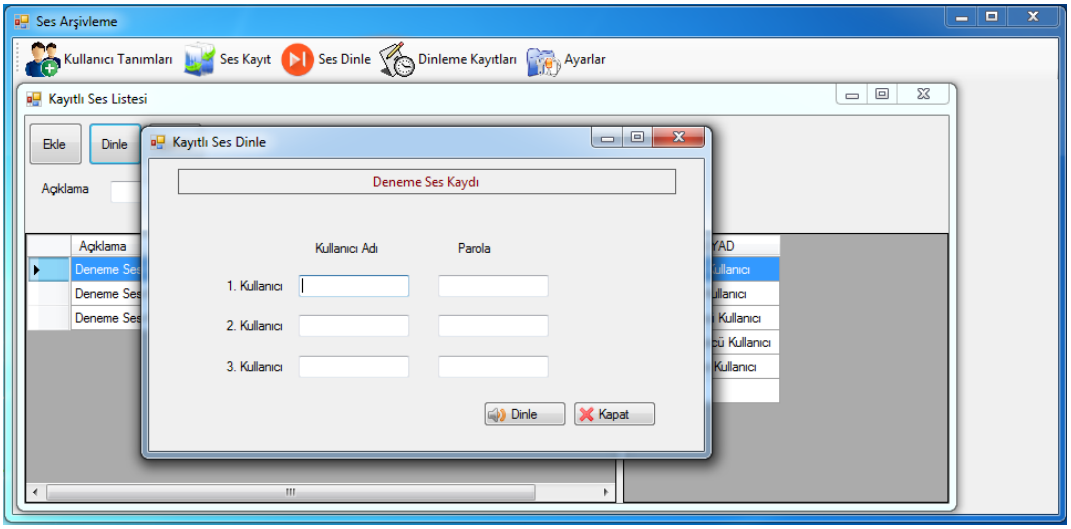


Şekil 0.2 Yeni ses dosyası kayıt ekranı[58]



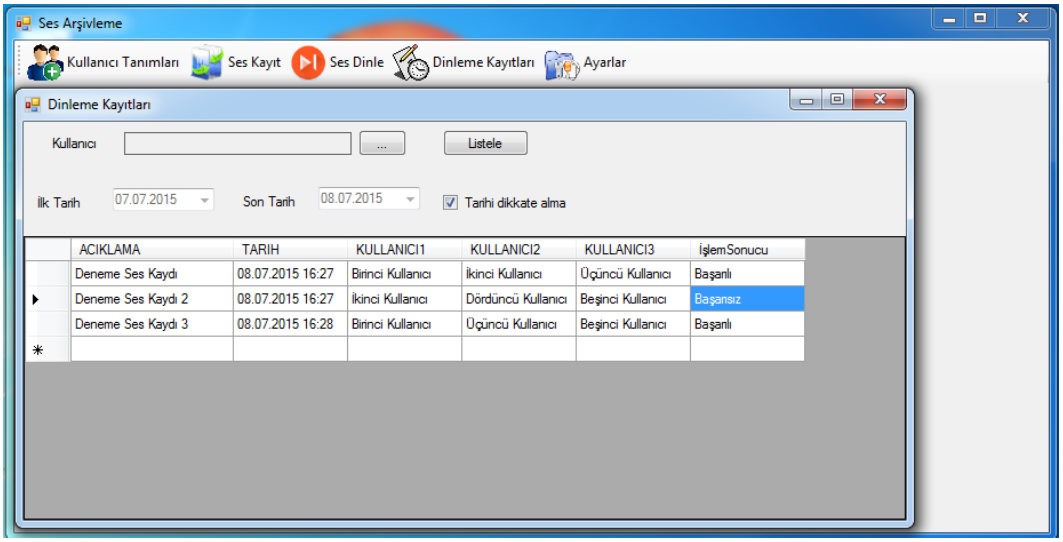
Şekil 0.3 Kayıtlı ses dosyalarının listesi ekranı[58]

Kayıtlı seslerin listelendiği ekranda kayıt sırasında yazılan açıklama veya kullanıcı bazlı filtrelemeler yapılabilmektedir. Listede bulunan bir ses kaydını dinlemek için ses kaydı seçildikten sonra Dinle butonuna basıldığında bu ses kaydından oluşturulan payların yetkili kullanıcılarından herhangi 3 tanesinin parolası istenecektir. Bu durum Şekil5.4'de görülmektedir.



Şekil 0.4 Ses dosyası dinleme ekranı[58]

Kullanıcılar, Şekil5.4'te gösterilen ekrandan parolalarını girdikten sonra, girilen kullanıcı bilgilerine ait pay verileri bulundukları sunuculardan çekilerek birleştirilir. Eğer parolalardan en az birisi yanlışsa veya yetkisiz kullanıcı parolası girilmişse dinleme işlemi başarısız olacaktır. Veritabanına da başarısız dinleme teşebbüsü olarak kaydedilecektir. Sistem yöneticisi ve bu ekranda parolalarını giren kullanıcılar bu başarısız dinleme teşebbüsünü kendi ekranlarında görebileceklerdir. Dinleme ekranında girilen parolalar doğru ise orijinal ses dosyası paylar aracılığı ile elde edilecek, ilgili ses dinlenecek ve işlem başarılı dinleme olarak veritabanına kaydedilecektir. Sistem yöneticisi ve bu ekranda parolalarını giren kullanıcılar tarafından başarılı dinleme olarak görülebilecektir. Şekil 5.5' de bu işlemlerle ilgili bir ekran görüntüsü verilmektedir.



Şekil 0.5 Başarılı ve başarısız dinleme kayıtları listesi[58]

Yukarıda izah edilen SDGAY aracı, değişik kurumlarda kullanılabilecek şekilde tasarlanmış olup, birçok ses dosyası arşivlenerek test edilmiştir ve istenilen sonuçlar elde edilmiştir.

6. SONUÇ VE ÖNERİLER

Sayısal teknoloji ürünlerinin kullanımı günümüzde hızla yaygınlaşmaktadır. Bu durum sayısal ortamlarda saklanan ve iletilen verilerin güvenliği sorununu da beraberinde getirmiştir. Her türdeki verilerin olduğu gibi ses verileri de bu güvenlik tehdidi ile karşı karşıyadır. Önlem alınmadığı takdirde sayısal ses dosyaları değiştirilme, dinlenme veya silinme gibi tehditlere maruz kalabilmektedir. Bu tez çalışmasında, sayısal ortamlarda depolanan veya sayısal ortamlar arasında iletilen ses verilerinin bu tehditlere karşı güvenliğini sağlamak üzere Gizlilik Paylaşımı yönteminin kullanılabilirliği farklı uygulamalar ile gösterilmeye çalışılmıştır. Shamir'in (k, n) eşik şeması yönteminin kullanıldığı uygulamalarda payların gizlenmek istenen ses verisine benzerliğini azaltmak için bir teknik açıklanmıştır. Bu tekniğe göre, önce ses dosyalarının örnekleme değerlerinin dizilimleri değiştirilerek karıştırılmış yeni bir ses elde edilip sonrasında bu yeni sesten gizlilik paylaşımı yöntemine göre paylar oluşturulmuştur. Bu şekilde elde edilen pay dosyalarının orijinal ses dosyalarına benzemediği tespit edilmiştir.

Bu karıştırma tekniği, ses dosyalarının iletimi ve sayısal ortamlarda depolanma sürecinde güvenliği sağlamaya yönelik iki farklı uygulamada kullanılmıştır. İlki gerçek zamanlı iletim sürecindeki ses dosyalarının güvenliğini sağlamaya yönelik FPGA tabanlı donanımsal gerçekleştirme uygulamasıdır. İkincisi ise sayısal ses dosyalarının yetkisiz kişilerce dinlenmesinin önlenmesini ve seslerin dinlenebilmesi için tek bir kişi yerine belirli sayıda kişilerin yetkilendirilmesini sağlayan bir sayısal ses arşivleme uygulamasıdır. Her iki uygulama da test edilerek seslerden payların oluşturulması ve paylar aracılığı ile orijinal seslerin yeniden elde edilmesi işlemlerinin başarılı bir şekilde gerçekleştirildiği gözlemlenmiştir.

Çok karmaşık hesaplamaları içermeyen bu gizlilik paylaşımı tekniğinin gerçek zamanlı uygulamalarda kullanılabilir olduğu FPGA uygulaması ile gösterilmiştir. Dolayısıyla bu tekniğin, özellikle internet üzerinden telefon görüşmeleri için kullanılan VoIP uygulamalarının güvenli bir şekilde yapılabilmesi için bir alternatif olarak kullanılabileceği önerilebilir.

7. KAYNAKLAR

[1] **Shamir, A.,**1979. How to Share a Secret, *Communications of the ACM,***22 (11),** 612, 613.

[2] **Blakley, G.R.,** 1979. Safeguarding Cryptographic Keys, *IEEE Transaction on Information Theory*,**48,** 313 – 317

[3] **Şahin, M. A. ve Arda, D.,**2009. Renkli Görüntü Dosyaları Üzerinde Gizlilik Paylaşımı Uygulaması, *IV İletişim Teknolojileri Sempozyumu,* Adana-Türkiye, 2009

[4] **Brickell, E. F.,**1990. Some Ideal Secret Sharing Schemes, *Advances in Cryptology – EUROCRYPT '89,*468-475.

[5] **Demir, M., Ulutaş, M., Odabaş,E.,** 2011, ASMUTH BLOOM SIR PAYLAŞIM TEKNİĞİNİN HIZLANDIRILMASI İÇİNKOŞUT PROGRAMLAMA, *Elektrik-Elektronik ve Bilgisayar Sempozyumu,* Elazığ, 5 – 7 Ekim, 10-14.

[6] **McEliece, R.J. and Sarwate, D.V.,** 1981. On Sahring Secrets and Reed Solomon Codes, *Communications of the ACM,***24(9)** 583-584.

[7] **Asmuth, C. and Bloom, J.,**1983. A modular approach to key safeguarding, *IEEE Transactions on Information Theory*,**29(2),** 208-210.

[8] **Mignotte, M.,**1983. How to Share a Secret, Lecture Notes in Computer Science,**149(10)**, 371 – 375.

[9] **Renvall, A. and Ding, C.,** 1996. A nonlinear secret sharing scheme, *Information Security and Privacy*,**1172,**56-66.

[10] **Stinson, D. R. and Vanstone, S.A.,**1988. A Combinatorial Approach to Threshold Schemes, *Advances in Cryptology — CRYPTO '87*,**293(5)**, 330-339

[11] **Ito, M., Saito, A., ve Nishizeki,T.,** 1987. Multiple Assignment Scheme for Sharing Secret,*Journal of Cryptology*,**6(6),** 15-20.

[12] **Csirmaz, L.,**1997. The Size of a Share Must Be Large, *Journal of Cryptology*,**10(4)** 223-231.

[13] **Özbek, İ.,**2012, Sır PaylaşımSistemleri, *Yüksek Lisans Tezi,*Yıldız Teknik Üniversitesi Fen Bilimleri Enstitüsü, İstanbul.

[14] **Krawczyk, H.,**1994. Secret Sharing Made Short, *Proceedings onAdvances in Cryptology — CRYPTO' 93*,773, 136-146.

[15] **Belenli, İ. L., Tuncer, T., Demir, F. B., Avcı, E., Ulaş, M., (**2015), A Scure Web Application Based Visual Cryptography and Secret Sharing, *Journal of Multidisciplinary Engineering Science and Technology*, **2(3),** 443 – 446.

[16] **Nabiyev,V., Zadeh, K. S.,** (2011), Blakley'in GizliSır Paylaşımına dayalı DataMatrix ECC200 Kodlama, *IV. Ağ ve Bilgi Güvenliği Ulusal Sempozyumu,* Ankara, 25-26 Kasım, 117 – 120.

[17] Bayıroğlu, H., 2006, Sayısal Yöntemler

[18] **Tompa, M. and Woll, H.,**1989. How to Share a Secret with Cheaters, *Journal of Cryptology,* **1(3),**133 – 138.

[19] **Brickell, E.F. and Stinson, D.R.,**1991. The detection of cheaters in treshold schemes, *SIAM J. Disc. Math.,***4,** 502 – 510.

[20] **Carpentieri, M.,** 1995. A perfect threshold secret sharing scheme to identify cheaters, *Design, Codes and Cryptography*,**5(3),** 183 – 187.

[21] **Derya, A., and Buluş, E.,** 2011. MDS Kod Tabanlı Gizlilik Paylaşım Şemasında Hileli Katılımcıları Tespit Etmek ve Kimliklendirmek, *IV. Ağ ve Bilgi Güvenliği Ulusal Sempozyumu*, Ankara, 25-26 Kasım, 10 – 13.

[22] **Jackson, W. A., Martin, K.M. and O'Keefe, C.M.,**1994. On sharing many secrets, *Advances in Cryptology - Asiacrypt'94,* 42–54.

[23] **He, J., Dawson, E.,**1994. Multistage secret sharing based on one-way function, *Electronic Letters*,**30 (19),** 1591 – 1592.

[24] **Harn, L.,**1995. Efficient sharing (brodcasting) of multiple secrets, *Computer and Digital Techniques,* **142 (3),** 237 – 240.

[25] **Chien, H. Y., Jan, J.K., Tseng, Y. M.,**2000. A practical (t, n) multi-secret sharing scheme, *IEICE Transactions on Fundamentals of Electronic, communications and computer sciences*,**83 (12),** 2762 – 2765.

[26] **Pang, L. J.,Wang, Y.M**.,2005. A new (*t, n*) multi-secret sharing scheme based on Shamir's secret sharing, *Applied Mathematics and Computation*,167 (2), 840 – 848.

[27] **Yang, C. C.,Chang, T. Y. and Hwang, M. S.,** 2004. A (t, n) multi-secret sharing scheme, *Applied Mathematics and Computation*,**151 (2)**, 483 – 490.

[28] **Zadeh, K.S.**, 2012. Çok Parçalı Sır Paylaşım Şemaları ve Uygulamaları,*Yüksek Lisans Tezi,* Fen Bilimleri Enstitüsü, Trabzon

[29] **Farras, O., Farre, J. M. And Padro, C.,**2007. Ideal Multipartite Secret Sharing Schemes,*Advances in Cryptology - EUROCRYPT 2007,* LNCS, 448 – 465.

[30] **Tassa, T.,**2007. Hierarchical treshold secret sharing, *Journal of Cryptology,* **20 (2)**, 237 - 264.

[31] **Belenkiy, M.,** 2008. Disjunctive Multi-Level Secret Sharing,*IACR Cryptology ePrint Archive,***18**.

[32] **Naor, M.,Shamir, A.,** 1994. Visual Cryptography, *Advances in Cryptology Eurocrypt'94*, 1-12.

[33] **Naor, M., Shamir, A.,**1997. Visual cryptography II: Improving the contrast via the cover base, *Security Protokols,* Springer Berlin Heidelberg, 197-202.

[34] **Cimato, S., De Prisco, R., De Santis A.,**2007. Colored visual Cryptography without color darkening, *Theoretical Computer Science,***374,** 261-276.

[35] **Blundo, C.,De Santis, A. and Naor, M.,** 2000. Visual Cryptography for greay level images,*Information Processing,***75,**255-259.

[36] **Lin, C. C., Tsai, W. H.,** 2003. Visual Cryptography for gray-level images by dithering techniques, *Pattern Recognition*, **24,** 349-358.

[37] **Hou, Y. C.,**2003. Visual Cryptography for color images,*Pattern Recognition,***36,** 1619-1629.

[38] **Nabiyev, V. V.,Ulutaş, M.,Ulutaş, G.,**2008. Doğruluk Oranı İyileştirilmiş (2, n) Olasılıklı Görsel Sır Paylaşma Şeması, *3. Uluslararası Katılımlı Bilgi Güvenliği ve Kriptoloji Konferansı,* Ankara, Türkiye, 25-27 Aralık.

[39] **Yang, C. N.,** 2004.New Visual secret sharing schemes using probabilistic method, *Pattern Recognition,***25**, 481 – 494.

[40] **Wang, D., Zhang, L., Ma, N.and Li, X.,**2007. Two Secret Sharing Schemes Based on Boolean Operations, *Pattern Recognition,***40**, 2776 – 2785.

[41] **Wang, D., Yi, F. and Li, X.,**2011. Probabilistic Visual secret sharing schemes for grey-scale images and color images, *Information Sciences,***181**, 2189 – 2208.

[42] **Thien, C. C., Lin, J. C.,** 2002. Secret image sharing. *Computers & Graphies,* **26**, 765-770

[43] **Wang, R.Z., Su C.H.,**2006. Secret image Sharing with smaller shadow images,*Patern Recognition,* **27,** 551-555.

[44] **Yang, C. N., Chen, T. S.,**2006. Reduce shadow size in aspect ratio invariant visual secret sharing schemes using a square block-wise operation, *Pattern Recognition,***39**, 1300–1314.

[45] **Desmedt, Y., Hou, S. and Quisquater, J. J.,**1998. Audio and Optical Cryptography, *Proceedings of the Advances in Cryptology – Asiacrypt'98*,Beijing, October 1998,392-404 (in China).

[46] **YANG, C. N.,**2002. Improvements on Audio and Optical Cryptography, *Journal of Information Scienceand Engineering*,**18,** 381-391.

[47] **Socek,D.,Magliveras, S.S.,** 2005. General Access Structures in Audio Cryptography, *IEEE International Conference on Electro Information Technology*, Lincoln, ABD, 22-25 Mayıs, s. 6-12.

[48] **Nikam, A., Kapade, P. and Patil S.,**2010. Audio Cryptography: A (2,2) Secret Sharing for Wave File, *International Journal of Computer Science and Application Issue,* 96 – 99.

[49] **Khobragade, P.V. and Uke, N.,**2012. Cogent Sharing Of Covert File Using Audio Cryptographic Scheme", *International Journal ofApplied Information Systems*, **1,**1-4.

[50] **Ehdaie, M., Eghlidos, T. andAref, M. R.**, 2008. A Novel Secret Sharing Scheme from Audio Perspective, *IEEE International Symposium on Telecommunications,* Tahran, 27-28 Ağustos, s. 13-18.

[51] **Maheswari, K., Punithavalli, M.,**2012. Modified Secret Sharing over a Single Path in VoIP with Reliable Data Delivery, *International Journal of Computer Science,* **1(3),** 221 – 226.

[52] **Maheswari, K., Punithavalli, M.,**Architecture of Multipath VoIP using Modified Secret Sharing Algorithm, *International Journal of Computer Applicaiton,* **36(3),** 12 – 18.

[53] **Nishimura, R., Abe, S. I., Fujita, N., Suzuki, Y.,** 2010. Reinforcement of VoIP Security with Multipath Routing and Secret Sharing Scheme, *Journal of Information Hiding and Multimedia Signal Processing,***1(3),** 204-219.

[54] **Sarma, M.,** 2014. SECURING VOIP COMMUNICATIONS IN AN OPEN NETWORK, *International Journal of Research in Engineering and Technology,* **3(7),** 6 – 10.

[55] **Hamdaqa, M., Tahvildari, L.,** 2011. ReLACK: A Reliable VoIP Steganography Approach, *Fifth International Conference on Secure Software Integration and Reliability Improvement*, Jeju Island, 27 – 29 June, 189 – 197.

[56] **Mazurczyk, W., Szczypiorski, K.,** *2008. Steganography of VoIP streams, On the Move to Meaningful Internet Systems: OTM 2008, Monterrey, Mexico, November 9-14, 1001 - 1018*

[57] **Yazan, E., Tatar, Y.,** 2015. Ses Dosyaları İçin Shamir'in Gizlilik Paylaşımı Yöntemine Dayalı Bir Uygulama, *3rd International Symposium on Digital Forensics and Security*, Ankara, 11-12 Mayıs, 219 – 223.

[58] **Yazan, E., Tatar, Y.,** 2015. GİZLİLİK PAYLAŞIMI YÖNTEMİNİ KULLANAN SES DOSYASI ARŞİVLEME PROGRAMI, *Ulusal Mühendislik Araştırmaları Sempozyumu 2015*, Düzce, 10-12 Eylül.

[59] **Maxfield C.,** 2004, The Design Warrior's Guide to FPGAs Devices, Tools and Flows, Elsevier

[60] http://www.fpganedir.com/FPGA/index.php**,** FPGA Nedir? 10 Eylül 2015

[61] **Aydın A.,** 2005. FPGA Yonga Mimarisi ve Kullanımı, Bitirme Ödevi

[62] **Santaş E., Karataş S.**, 2013. Her Yönüyle FPGA ve VHDL, Palme Yayınevi

ÖZGEÇMİŞ

1983 yılında Mersin'de doğdu. İlk, orta ve lise öğrenimini Mersin'de tamamladıktan sonra 2000 yılında Erciyes Üniversitesi, Mühendislik Fakültesi, Bilgisayar Mühendisliği Bölümünü kazandı. 2011 yılına kadar özel sektörde farklı firmalarda Bilgi İşlem Sorumlusu ve Yazılım Uzmanı olarak çalıştıktan sonra Adıyaman Üniversitesi Besni Meslek Yüksekokulunda Öğretim Görevlisi olarak göreve başladı. 2013 yılında Fırat Üniversitesi, Fen Bilimleri Enstitüsü, Bilgisayar Mühendisliği Bölümü, Bilgisayar Donanımı Anabilim Dalında yüksek lisans eğitimine hak kazandı. Halen öğretim görevlisi olarak görevini sürdürmektedir. Yabancı dili İngilizce'dir.