KOCAELİ ÜNİVERSİTESİ
FEN BİLİMLERİ ENSTİTÜSÜ

MATEMATİK ANABİLİM DALI

YÜKSEK LİSANS TEZİ

DALGACIK DÖNÜŞÜMÜ TABANLI GÖRSEL KRİPTOLOJİ

NİLHAN SAYIN

KOCAELİ 2017

KOCAELİ ÜNİVERSİTESİ

FEN BİLİMLERİ ENSTİTÜSÜ

MATEMATİK

ANABİLİM DALI

YÜKSEK LİSANS TEZİ

DALGACIK DÖNÜŞÜMÜ TABANLI GÖRSEL KRİPTOLOJİ

NİLHAN SAYIN

Yrd.Doç.Dr. Hülya KODAL SEVİNDİR		
Danışman,	**Kocaeli Üniversitesi**	.....
Prof.Dr. Halis AYGÜN		
Jüri Üyesi,	**Kocaeli Üniversitesi**	.....
Prof.Dr. Cemil ÖZ		
Jüri Üyesi,	**Sakarya Üniversitesi**	.....

Tezin Savunulduğu Tarih: 31 .05.2017

ÖNSÖZ VE TEŞEKKÜRLER

Teknolojinin gereklerinden olan ve günlük hayatta kişi, kurum ve kuruluşların haberleşme ve veri aktarımı için kullandığı internet, verilerin gizliliği, bütünlüğü ve alıcıya ulaştırılması hususlarında açık bir tehdit oluşturmaktadır. Bu çalışmada, internette kötü niyetli kişilerin, gizli verilere göndericinin haberi olmadan ulaşamamaları ya da ulaşılması durumunda veri üzerinde oluşturulan şifreyi çözmeden müdahale edilememesi için bir yöntem sunulmuştur.

Tez danışmanlığımı üstlenerek, isteklerimi ve yeteneklerimi göz önünde bulundurarak çalışma konusunun belirlenmesi, araştırılması, yürütülmesi ve sunuma hazırlanması sırasında, ilgi ve desteğini benden esirgemeyen, değerli bilimsel görüş, önerileri ve tecrübelerinden yararlandığım Yrd. Doç. Dr. Hülya KODAL SEVİNDİR'e teşekkürler eder, sonsuz saygılarımı sunarım.

Tez çalışmam sırasında bilgi, tavsiye ve yardımları ile değerli zamanlarını benden esirgemeyen Öğr. Gör. Mevlüt SEVİNDİR'e, Yrd. Doç. Dr. Cüneyt YAZICI'ya ve Araş. Gör. Süleyman ÇETİNKAYA'ya teşekkür ederim.

Hem lisans öğrenimim süresince hem de lisansüstü çalışmalarım sırasında üzerimde emeği olan Kocaeli Üniversitesi Fen-Edebiyat Fakültesi Dekanı ve Matematik Bölüm Başkanı Prof. Dr. Halis AYGÜN'e teşekkürlerimi ve saygılarımı sunarım.

Tezin çalışmalarım boyunca tüm zorlukları benimle göğüsleyen, her konuda fedakarlık gösteren, maddi manevi yardımlarını esirgemeyen ve hayatımın her evresinde bana destek olan aileme teşekkürlerimi ve sevgilerimi sunarım.

Mayıs – 2017 Nilhan SAYIN

İÇİNDEKİLER

ŞEKİLLER DİZİNİ

TABLOLAR DİZİNİ

SİMGELER VE KISALTMALAR DİZİNİ

$C^{\infty}(IR)$	: IR üzerinde her mertebeden türevlenebilen sürekli fonksiyonlar uzayı
D	: Ölçekleme operatörü
E_b	: b'ye bağlı modülasyon operatörü
f	: Herhangi bir fonksiyon
$\hat{f}$	: f fonksiyonun Fourier dönüşümü
γ	: Frekans
$\|\hat{f}(\gamma)\|$	: f fonksiyonundaki γ frekansının yoğunluğu
$\mathcal{F}$	: Fourier dönüşümü
F^{-1}	: Ters Fourier dönüşümü
H	: Hilbert uzayı
H_0	: 1-periyodik fonksiyon
H_1	: H_0'a bağlı fonksiyon
I	: IR^+'nın alt kümesi
L(.)	: Lagrange enterpolasyon polinomu
$L^1(IR)$	: IR üzerinde integrallenebilir fonksiyonlar uzayı
$L^1(IR^n)$	: IR^n üzerinde integrallenebilir fonksiyonlar uzayı
$L^2(IR)$	: IR üzerinde karesi integrallenebilir fonksiyonlar uzayı
$l^2(Z)$	: Z üzerinde karesi toplanabilir diziler kümesi
sinc	: Sinüse bağlı parçalı bir fonksiyon
$\overline{\text{span}}\{D^jT_k\varphi\}_{k\in Z}$	: $\{D^jT_k\varphi\}_{k\in Z}$ ailesini geren uzay
Sup	: Supremum (üst sınırların en küçüğü)
supp	: Support (sonlu dayanak)
$\{T_k\varphi\}_{k\in Z}$	: V_0 için bir ortonormal taban
T_ψ	: Sürekli dalgacık dönüşümü
T_k	: k'ya bağlı öteleme operatörü
$\{v_j\}_{j\in Z}$	: $L^2(IR)$ nin kapalı alt uzaylarının bir dizisi
$W_\psi H$	: Heaviside basamak fonksiyonunun sürekli dalgacık dönüşümü
$\subset$	: Alt küme
Φ^*	: Analiz operatörü, Φ'nin eşlenik operatörü
$\Phi=\{\varphi_i\}_{i\in I}$	: Ayrılabilir bir H Hilbert uzayındaki vektörler ailesi
*	: Convolution (konvolüsyon)
$\times$	: Çarpma işlemi
ψ	: Dalgacık fonksiyonu
$\overline{\psi}$	: Dalgacık fonksiyonunun kompleks eşleniği
δ	: Dirac delta fonksiyonu
$\langle\cdot,\cdot\rangle$	: Euclid iç çarpımı
$\forall$	: Her

Λ : Katsayıların bir indeks kümesi
$|\ .\ |$: Mutlak değer
$\varphi^{(n)}$: n-yinci mertebeden türevlenebilir bir fonksiyon
$\|\ .\|$: Norm
$\psi_{a,t}$: Ölçeklenmiş ve ötelenmiş dalgacık fonksiyonlar ailesi
π : Pi sayısı
∞ : Sonsuz
$\|\ \|_{\infty}$: Sonsuz normu
$\sum$: Toplam sembolü
$\lceil x \rceil$: x'den büyük ya da eşit olan en küçük tamsayı

Kısaltmalar

AES : Advanced Encryption Standart (Gelişmiş Şifreleme Standardı)
AFD : Ayrık Fourier Dönüşümü
BPCS : Bit Plane Complexity Segmentation (Bit Düzlemi Karmaşıklık Bölütleme)
CBC : Cipher Block Chaining (Şifre Blok Zincirlemesi)
CFB : Cipher FeedBack (Şifre Geri Beslemeli)
CRT : Chinese Remainder Theorem (Çinli Kalan Yöntemi)
CMY : Cyan-Magenta-Yellow (Camgöbeği-Eflatun-Sarı)
DES : Data Encryption Standart (Veri Şifreleme Standardı)
DH : Diffie-Hellman Anahtar Değişimi
DT-CWT : Dual Tree Complex Wavelet Transform (Çift Ağaç Kompleks Dalgacık Dönüşümü)
DWT : Discrete Wavelet Transform (Ayrık Dalgacık Dönüşümü)
ECC : Elliptic Curve Cryptography (Eliptik Eğri Kriptografisi)
FD : Fourier Dönüşümü
GAS : General Access Structure (Genel Erişim Yapısı)
HCF : Histogram Characteristic Function (Histogram Karakteristik Fonksiyonu)
HFD : Hızlı Fourier Dönüşümü
IBM : International Business Machines (Uluslararası İş Makineleri)
IDEA : International Data Encryption Algorithm (Uluslararası Veri Şifreleme Algoritması)
JND : Just Noticeable Distortion (Sadece Gözle Görülür Bozulma)
JPEG : Joint Photographic Experts Group (Birleşik Fotoğraf Uzmanları Grubu)
KZFD : Kısa Zamanlı Dalgacık Dönüşümü
LSB : Least Significant Bit (En Az Anlamlı Bit)
MD : Message-Digest Algorithm (Mesaj Özetleme Algoritması)
MILON : Milli On-Line Kripto Cihazı
NBS : Ulusal Standartlar Dairesi
NIST : National Institute Of Standards And Technology (Ulusal Standartlar ve Teknoloji Enstitüsü)

OR	: Veya
PSNR	: Peak Signal-To-Noise Ratio (Tepe Sinyal-Gürültü Oranı)
PW	: Paley-Wiener Uzayı
RGB	: Red-Green-Blue (Kırmızı-Yeşil-Mavi)
RIPEMD	: RACE Integrity Primitives Evaluation Message Digest (RACE Bütünlük İlkeleri Değerlendirme Mesaj Özetleme Algoritması)
RSA	: Rivest Shamir Adleman
SDD	: Sürekli Dalgacık Dönüşümü
SHA	: Secure Hash Algorithm (Güvenli Özetleme Algoritması)
SSL	: Secure Socket Layer (Güvenli Soket Katmanı)
TAFD	: Ters Ayrık Fourier Dönüşümü
TSK	: Türk Silahlı Kuvvetleri
TUBITAK	: Türkiye Bilimsel ve Teknolojik Araştırma Kurumu
VCRG	: Visual Cryptogram Of Random Grids (Rastgele Izgara Görsel Kriptolojisi)
VIP	: Visual Information Pixel (Görsel Bilgi Pikseli)
XOR	: Exclusive OR (Özel Veya)
YCbCr	: Luminance - Chroma:Blue - Chroma:Red (Parlaklık - Krom Mavi - Krom Kırmızı)

DALGACIK DÖNÜŞÜMÜ TABANLI GÖRSEL KRİPTOLOJİ

ÖZET

Teknolojinin hızlı gelişimi sonucunda askeri, elektronik, banka işlemleri, kurum ve kuruluşlar arası veri alışverişi gibi daha birçok alanda kriptografi bilimi kullanılmaya başlanmıştır. Günümüzde kullanılan sistemlerde gerekli olan en önemli özelliklerden biri de verilerin sorunsuz bir şekilde iletilmesi ve veri gizliliğidir. Kriptografi, verilerin gizlilik ve güvenliğini sağlamak amacıyla, gizlilik, kimlik denetimi, bütünlük gibi özellikleri, çeşitli şifreleme, anahtarlama ve çözümleme algoritmaları kullanarak sağlayan matematiksel içerikli yöntemlerdir.

Bu tezde, dalgacık dönüşümü ile sır paylaşımından elde edilen payların kapak görüntülerine gömülmesi üzerine uygulamalar yapıldı. Görsel sır paylaşımı ile elde edilen gürültü benzeri görüntüler dikkat çektiği için, bu paylar anlamlı kapak görüntülerine dalgacık dönüşümü yardımıyla gömüldü ve payların dikkat çekmemesi sağlandı. Gerçek sır görüntüleri ile elde edilen sır görüntüleri arasında karşılaştırmalar yapılarak PSNR değerleri hesaplandı. Bu amaçla uygun kodlar yazıldı.

Anahtar Kelimeler: Dalgacık Dönüşümü, Floyd-Steinberg Algoritması, Görsel Kriptoloji, Kriptoloji, Stenografi.

VISUAL CRYPTOLOGY BASED ON WAVELET TRANSFORMATION

ABSTRACT

As a result of the rapid development of technology, many application fields of cryptography such as military, electronics, bank transactions, data exchange between institutions and organizations have begun to be used. One of the most important features required in today's used systems is that data must be transmitted without any problems and data should stay confidential. Cryptography is a mathematical method to ensure the confidentiality and security of data, providing features such as privacy, authentication and integrity using various encryption, switching and resolution algorithms.

In this thesis, applications of embedding of shares obtained from secret sharing into cover images were made via wavelet transformations. Since the noise-like images obtained with visual secret sharing attract attention, these shares were embedded with the help of wavelet transform to meaningful cover images and provided that the shares were not attracted attention. Comparisons were made between real secret images and obtained secret images and PSNR values calculated. To do so, proper MATLAB codes are written.

Keywords: Wavelet Transform, Floyd-Steinberg Algorithm, Visual Cryptology, Cryptology, Stenography.

GİRİŞ

Son yirmi yılda internet ve ağ teknolojilerinin hızla gelişmesi, kişi ve kurumların bilgi edinme gereksinimlerinin artış göstermesi ve özellikle, internetin iletişim ve haberleşme amaçlı kullanılması bilgi güvenliğinin gerekliliğini de beraberinde getirmiştir. İkinci Dünya Savaşı'ndan bu zamana kadar bilgi işlem güvenliği ve veri şifreleme sistemleri oldukça önemli bir hal almıştır. Dünyanın hemen her noktasına açık erişimin sağlandığı bir ortamda bilgi güvenliği çok büyük bir öneme sahiptir. Teknoloji geliştikçe bilgi çoğalmakta ve erişim, paylaşma, koruma gibi durumlar önem kazanmaktadır. Tüm bunların güvenli bir ortamda ve güvenli bir biçimde gerçeklenmesi için parola oluşturma, şifreleme gibi teknikler kullanılmaktadır. Dünya üzerinde bilgisayar ve bilişim teknolojilerinin kullanımının hızla yaygınlaşması, gerek kişisel gerek kurumsal bilgi ve haberleşme güvenliği için kriptolama sistemlerinin kullanımını zorunluluk haline getirmiştir.

Kriptolojinin üç ana görevi vardır. Bu görevler, verinin okunmasını engelleme, değiştirilmesini engelleme ve verinin bilinen göndericisinde değişiklik olmadığını doğrulamaktır. Her zaman üçüncü bir şahıs, internet gibi güvenli olmayan ortamlarda kişi ya da kurumlar arasındaki haberleşmeleri dinleyebilir ve bu haberleşmelerde iletilen veriler üzerinde bazı işlemler ve değişiklikler yapabilir. İletilen veriler üzerinde yapılan bu işlemler genelde verinin ulaştırılmasını engelleme (intercept), veriyi sadece okuma (read) ve veriyi değiştirme (modify) şeklindedir. Bu tip işlemlerin yapılmasını engellemek amacıyla şifreleme biliminin temelde üç ana görevi vardır.

1. Veri Güvenliği (Confidentiality): Kişi ve kurumlar arasında gönderilen verinin üçüncü şahıslar tarafından okunmasını engelleme durumudur. Yani gönderilen verinin, alıcıya giderken, iletim kanalında herhangi bir kişi tarafından okunmasının engellenmesidir. Şifreleme bu veriyi şifreleyerek yazma işlemini gerçekleştirmemizi sağlamaktadır. Böylece veriye herhangi bir kişi tarafından erişilse bile veri, düz metin olmadığı için okunması engellenmiş olacaktır.

2. Veri Bütünlüğü (Data integrity): Kişi ve kurumlar arasında gönderilen verinin üçüncü kişiler tarafından değiştirilmesini engelleme durumudur. Normal yoldan göndermiş olduğunuz veri, üçüncü kişiler tarafından değiştirilerek alıcıya tekrar gönderilebilmektedir. Şifreleme, gönderilen bu düz metin üzerinde işlem yaparak sayısal bir sonuç oluşturur. Algoritma aynı olduğundan, gönderilen yazının üzerinde herhangi bir değişiklik yapılırsa sonuç değişecektir. Gönderici ve alıcı tarafından aynı veri üzerinde aynı algoritmayla oluşturulan sayısal sonuçlar aynı olmak zorundadır. Eğer sayısal sonuçlar farklıysa, gönderilen veri, iletim kanalında değiştirilmiştir. Çünkü aynı veri üzerinde yapılacak bir değişiklik aynı sayısal sonucu vermeyecektir. Kullanılan algoritma sayesinde farklı veriler üzerinde aynı sayısal sonucun elde edilmesi çok düşük bir olasılıktır.

3. Kimlik denetimi (Authentication): Bir alıcıya ulaşan verinin, belirtilen gönderici tarafından gönderildiğinden emin olunması durumudur (Digital Signature). Üçüncü kişiler tarafından, gönderici isimleri farklı yazılarak (spam mailler gibi) kişilere veriler gönderilebilir. Şifreleme, verilere özel imzalar (signature) ekleyerek, gönderen kişinin gerçek gönderici olduğundan emin olmanızı sağlar. Gönderilen zaman dilimine göre özel algoritmalarla oluşturulan bu imzalar, alıcı kişi tarafından belirli yöntemlerle doğrulanabilir [1].

Bilgi teknolojilerine giderek artan bağımlılık, kullanıcıları güvenlik önlemleri almaya yöneltmektedir. İnternet üzerinden yapılan günlük işlemler, bireysel bankacılık işlemleri, ulaşım ve tatil rezervasyonları, sanal ortamda alışveriş gibi ekonomik ve toplumsal yaşamın her alanında olduğu kadar, ulusal güvenlik ve savunma konularında da güvenliğin sağlanması büyük önem arz etmektedir. İnternet üzerinde tam güvenliğin sağlanması olanaksızdır. Bu durumda bilgi ve haberleşme güvenliğinin yüksek oranda sağlanması gerekmektedir.

Günümüzde önem verilen husus, verinin iletilmesinden çok gizlilik içerisinde iletilmesidir. Bu tezde stenografi yöntemi kullanılarak anlamlı görüntüler içerisine gömdüğümüz veriler deşifre olsa bile kriptografi yöntemi ile geliştirdiğimiz algoritma sayesinde şifrelenmiş veriler çözüme ulaşmadan gönderilmek istenilen gizli veriye ulaşılamayacaktır.

Bölüm 1'de kriptoloji, görsel kriptoloji ve stenografinin tanım ve tarihçeleri verildi. Sır paylaşımı ve görsel sır paylaşımı hakkında bilgi verildi. Şifreleme yöntemleri ve bazı şifreleme algoritmaları tanıtıldı ve kullanılan bazı kripto makinelerinden bahsedildi. Geçmişten günümüze kriptoloji, görsel kriptoloji ve stenografideki gelişmeler anlatıldı.

Bölüm 2'de literatür çalışması yapıldı.

Bölüm 3'de tezin konusuyla ilgili teorik bilgiler verildi. Bu bağlamda Fourier ve Dalgacık Dönüşümlerinin teorileri tanıtıldı. Shamir Sır Paylaşım Şeması ve bu şemada kullanılan Lagrange İnterpolasyonu tanıtıldı. Shamir yöntemiyle gizli görüntü paylaşımı, renkli görüntüleri halftone görüntüye dönüştürmede kullanılan Floyd-Steinberg Algoritması ve stenografi uygulamasında temel alacağımız En Az Anlamlı Bit (LSB, Least Significant Bit) yöntemi tanıtıldı.

Bölüm 4'de kullanılan bilgisayarın ve programın teknik özelliklerinden bahsedildi. İki uygulamada kullanılan ikili ve renkli sır görüntüleri ve kapak görüntüleri hakkında bilgi verildi. Görüntüleri sırra çevirme ve kapak görüntülere gömme, daha sonra elde etme durumlarında kullanılan algoritma ve yöntemler verildi.

Bölüm 5'de görsel verilere Shamir algoritması uygulandı ve sır görüntülerinin payları elde edildi. Payların gömüleceği kapak görüntülere gerekli işlemler yapılarak elde edilen katmana dalgacık dönüşümü uygulandı ve paylar bu katmanlara gömüldü. Daha sonra stego görüntülerden paylar elde edilip bir araya getirilerek sır görüntüsü elde edildi.

Bölüm 6'de bu tezde elde edilen bütün sonuçlar ve öneriler tartışıldı.

Bu tez çalışmasının amacı, literatürde önemli bir yere sahip olan görsel sır paylaşımı uygulamalarından görsel kriptoloji ve stenografi aşamalarında, ikili ve RGB görüntü verileri kullanılarak, son yıllarda ortaya çıkmış ve çoklu ölçekli yöntemlerden olan dalgacık dönüşümünü uygulamaktır. Gizli görüntülerin paylaştırılmasında gizlilik son derece önemli olduğundan, dalgacık dönüşümünden elde edilen sonuçları literatüre kazandırmak oldukça yararlı olacaktır.

1. GENEL BİLGİLER

1.1. Kriptoloji

Matematiksel zor problemlere dayanan tekniklerin ve uygulamaların bir bütünü olarak, kriptoloji haberleşen kişi ya da kurumların veri alışverişini güvenli olarak yapmasını sağlamaktadır. Kriptoloji, matematik, elektronik, bilgisayar bilimleri gibi birçok disiplini kullanan özelleşmiş bir bilim dalıdır.

Hem şifre bilimi (kriptografi), hem de şifre analizini (kriptoanaliz) içeren kriptoloji, matematiğin bir dalıdır ve genellikle sayılar teorisi üstüne kuruludur. Kriptografi, Yunanca'dan dilimize geçen crypto (gizli) ve grapy (yazım) kelimelerinden türetilmiştir ve şifre yazım anlamına gelmektedir. Kriptografi, kriptolojinin çeşitli yöntemlerle dijital verilerin şifrelenerek gizliliğini ve güvenliğini korumayı hedeflemiş bir dalıdır. Şifreleme (Encryption), gizlenmek istenen veriyi (düz metin-plaintext) matematiksel algoritmaları kullanarak anlamsız bir şifreli veriye (şifreli metin-ciphertext) dönüştürme işlemidir. Bu işlemle verinin gizliliğinin her ortamda korunması amacıyla, kullanılan anahtar bilgisine sahip olmadan verinin içeriğine erişilemez. Böylece şifrelenen veriye, sadece gönderenin bildiği alıcı tarafından erişimi sağlanmış olur ve iletilen mesaja gönderim esnasında ağa müdahalede bulunan üçüncü bir şahıs tarafından erişim sağlanmaz. Şifre çözüm anlamına gelen kriptoanaliz ise kriptografi sistemleri kullanılarak üretilmiş bir kriptografik sistemi inceleyerek güçlü ve zayıf yönlerini ortaya çıkaran bir kriptoloji dalıdır. Şifrelenmiş metni düz metin haline getirme işlemi olan şifre çözme (decryption), kullanılan şifrenin zayıf yönlerinden ve şifreli metnin hakkındaki bilgilerden hareketle bütün anahtarları deneme zahmetinden kurtulmayı amaçlamaktadır.

Kriptolama ve kripto çözme işlemini gerçekleştirmek üzere kullanılan matematiksel fonksiyonlara "kripto algoritması" denir. Kriptolanmış verinin güvenliği, kullanılan algoritmanın gücüne ve anahtarların gizliliğine bağlıdır. Anahtar, 0 ve 1 rakamlarından oluşan bir bit dizisidir ve her algoritmanın anahtar boyları farklıdır. Buna ek olarak anahtar boyu arttıkça, olası anahtar sayısı artar ve saldırganın şifreyi

çözmesi zorlaşır. Ama aynı zamanda şifreleme ve şifre çözme hızı yavaşlar. Algoritmada kullanılan olası tüm anahtar topluluğuna "anahtar uzayı" denir. Kriptografi algoritması, şifrelemede kullanılan anahtarlar ve kullanılan protokoller kriptosistemin birer parçasıdır. Bir kriptografik sistem, bir araya getirilmiş birçok yöntem ile bilgi güvenliğini sağlamaktadır. Bu yöntemler üç grupta incelenebilir:

1. Anahtarsız şifreleme
2. Gizli anahtarlı şifreleme
3. Açık anahtarlı şifreleme

Şifreleme ve şifre çözme işlemi yapan sistemlere "kriptosistem" denir. Şifreleme işlemi yapan kişilere "kriptolog", şifre çözümü yapan kişilere ise "kriptoanalist" denir.

1.1.1. Anahtarsız şifreleme yöntemi

Anahtar kullanılmayan kriptografik algoritmaların kullanıldığı şifreleme yöntemine anahtarsız şifreleme denir. Diğer adıyla "Veri Bütünlüğü ve Özet Fonksiyonu" birçok güvenlik önlemini sağlamak için kullanılan bir özet fonksiyonudur. Bu fonksiyon, veriyi belirli uzunluktaki bit dizisine dönüştürür ve verideki en küçük değişiklik bile özet değerini değiştirir. Anahtarsız şifreleme yönteminin kullanıldığı kriptografi algoritmalarından bazıları GOST, HAVAL, MD2, MD4, MD5, PANAMA, RIPEMD, SHA-0, SHA-1, WHIRLPOOL şeklindedir.

1.1.2. Gizli anahtarlı şifreleme yöntemi

Gizli anahtarlı şifreleme, simetrik şifreleme veya tek anahtarlı şifreleme olarakta adlandırılır. Bu şifreleme yönteminde hem şifreleme hem deşifreleme işlemlerinde aynı anahtar kullanılır ve şifre algoritmaları daha basittir. Hem göndericide hem de alıcıda aynı anahtar bulunur ve taraflar anahtar üzerinde anlaşma yaparken anahtarın üçüncü bir kişinin eline geçmesini engellemelidirler. Sezar, Vigenere, DES, 3DES, Riverest tarafından geliştirilen RC2, RC4 ve RC5, Amerika Bileşik Devletleri tarafından kullanılan SKIPJACK, Blowfish, Twofish, IDEA (International Data Encryption Algorithm), SAFER algoritmaları gizli anahtarlı şifreleme yöntemlerinden bazılarıdır.

1.1.3. Açık anahtarlı şifreleme yöntemi

Şifreleme ve deşifreleme işlemlerinde iki farklı anahtarın kullanıldığı şifreleme yöntemidir. Asimetrik şifreleme yöntemi olarakta bilinen bu şifreleme yönteminde gizli anahtarın karşı tarafa, kimsenin öğrenmeden gönderilmesi sorunu ortadan kalkmıştır. Veri iletiminde, tarafların her birinde bir çift anahtar bulunur ve taraflarda bulunan matematiksel olarak birbirine bağlı olan bu anahtarlardan biri gizli diğeri açık anahtardır. Gizli anahtarın sadece bir sahibi vardır ve gizli anahtara sahip olan taraf kendi açık anahtarıyla şifrelenmiş bilgilerin şifresini çözebilir, kendisine ait sayısal imza oluşturulabilir ve kendi kimliğini ispat edebilir. Açık anahtar, sadece gizli anahtarın sahibi tarafından oluşturulabilir ve herkesin erişimine açıktır. Açık anahtarla, bilgiler sadece gizli anahtarın sahibi tarafından çözülebilecek şekilde şifrelenebilir ya da gizli anahtar sahibinin sayısal imzasının ve kimliğinin doğruluğu kontrol edilebilir. Açık anahtarlı şifreleme yönteminin kullanıldığı kriptografi örneklerinden bazıları Diffie-Hellman Anahtar Değişimi Yöntemi, RSA, ElGamal, Paillier, Blum-Goldwasser Kriptosistemi, Goldwasser-Micali Kriptosistemi, Okamoto-Uchiyama Kriptosistemi şeklindedir.

1.2. Şifreleme Algoritmaları

Bu bölümde Gizli Anahtarlı (Simetrik) ve Açık Anahtarlı (Asimetrik) Şifrelemede kullanılan bazı şifreleme algoritmaları incelenecektir.

1.2.1. DES (Data Encryption Standart)

1973'te Ulusal Standartlar Dairesi (NBS)'nin ulusal bir standart olabilecek kriptografik bir algoritma talebine karşılık, 1974'te IBM tarafından sunulan LUCIFER algoritması üzerinde yapılan bazı değişikliklerin ardından 1977'de DES (Data Encryption Standart) adıyla resmi şifreleme standardı olarak kabul edildi. DES, Amerika Bileşik Devletleri tarafından kullanılan, gizli anahtarlı bir şifreleme algoritmasıdır ve büyük boyutlu verilerin şifrelenmesinde kullanılır. Şifreleme işlemi, Blok Şifreleme olarak adlandırılan bir yöntemle gerçekleştirilir. Şifrelenecek blok iki parçaya bölünür ve her aşamada sadece biri üzerinde işlem yapılır. Bu işlemin sonucu bir sonraki aşamada verinin ikinci yarısını etkiler ve bu sarmal yapı şifreleme boyunca devam eder. DES, karıştırma ve yerine koyma işlemlerini

sistematik bir biçimde yaptığı için en küçük değişiklikte bile büyük farklar ortaya çıkar, tek bitlik bir değişim bile sonucu tamamen değiştirir ve bu değişim önceden tahmin edilemez.

DES, bugün kullandığımız VISA, MASTERCARD, BKM, vb. tüm kart sistemlerinin şifreleme mantığını oluşturur. Ancak kaba kuvvet saldırılarına karşı koymakta zorlanan DES, 1978 yılında IBM tarafından TRİPLE DES (3DES) adında yeni bir algoritmaya geliştirilmiştir. Trible DES algoritmasında DES işlemi üç kez yapılmaktadır bu yüzden DES yöntemine göre üç kat yavaş çalışmaktadır. Çift yönlü çalışan 3DES algoritması, şifreli bir şekilde verileri saklayabilir ve istenildiğinde bu verilerin şifresi çözülebilir. Ayrıca bu algoritma bilgisayarın donanımsal açıklarını da giderebilir. Bunların yanında güvenlik tamamen kullanılan anahtara bağlı olduğundan, anahtarın zayıflığı şifrenin çözümünü kolaylaştırır. 3DES, bankacılık işlemlerinde, elektronik ödeme işlemlerinde ve yazılım anahtarı oluşturma gibi işlemlerde kullanılmaktadır.

1.2.2. AES (Advanced Encryption Standart)

Elektronik verinin şifrelenmesi için sunulan bu standart, 2002 yılında Amerikan hükümeti tarafından kabul edilmiştir ve uluslararası alanda da şifreleme standardı olarak kabul edilmektedir. Bu şifreleme algoritması, hem şifrelemede hem de şifreli metni çözmede tek anahtarın kullanıldığı, simetrik anahtarlı bir algoritmadır. DES algoritmasının yerini almıştır.

1.2.3. Diffie Hellman anahtar değişimi

Oldukça başarılı olan simetrik algoritmaların temel sorunu, gönderici ve alıcının aynı şifreyi bilmesidir. Bu sorun Asimetrik Anahtar Algoritması denilen daha karmaşık ve iki şifre anahtarının kullanıldığı bir algoritmanın geliştirilmesine neden olmuştur. Asimetrik anahtarların iletiminde ise Diffie Hellman (DH) Anahtar Değişimi algoritması kullanılmaktadır. DH anahtar değişiminin güvenilirliği, kullanılan asal sayıların büyüklüğü üzerine kurulmuştur ve ayrık logaritmik problem kullanılan bu algoritmanın seçtiği fonksiyon her iki tarafa da aynı gizli şifreyi verir. Bu algoritma 1972 yılında Withfield Diffie ve Martin Hellman tarafından bulunmuştur.

1.2.4. RSA (Rivest Shamir Adleman)

Açık anahtarlı bir şifreleme yöntemi olan RSA'nın güvenliği tam sayıları çarpanlarına ayırmanın algoritmik zorluğuna dayanır. 1974 yılında Diffie ve Hellman tarafından üretilen açık anahtarlı şifreleme yöntemini geliştirerek, 1978'de MIT'de buldukları algoritmayı, Ronald Rivest, Adi Shamir ve Leonard Adleman, isimlerinin ilk harflerini birleştirerek isimlendirmişlerdir. Bu algoritmada iki büyük asal sayının çarpımı, seçilen başka bir değerle birlikte ortak anahtar olarak kullanılır ve seçilen asal çarpanlar saklanır. Ortak anahtar kullanılarak mesaj şifrelenebilir ancak ortak anahtar yeterince büyükse sadece asal çarpanların bilinmesi halinde şifreli mesaj çözülebilir. RSA algoritması, DES algoritmasıyla karşılaştırıldığında çok daha yavaş çalışır. Bugün 512 bitlik RSA algoritması kırılabilmektedir. Fakat bu kırma işlemi için 3000 bilgisayarın 3 gün boyunca çalışması gerekmektedir. Yine de çözülebilme ihtimaline karşılık gizli işlemler için 1024, askeri gizli işlemler için 2048 bitlik RSA algoritması kullanılmalıdır. RSA algoritması, network üzerinde bilgi transferi sırasında gizlilik ve güvenliğin sağlanması amacıyla 1994 yılında Netscape tarafından geliştirilen bir güvenlik protokolü olan SSL (Secure Socket Layer) tabanı için anahtar değiştirme algoritmasıdır. RSA, metin şifreleme dışında dijital mesajları imzalamak içinde kullanılabilir.

1.2.5. DSA (Digital Signature Algorithm)

RSA gibi açık anahtarlı bir şifreleme sistemi olan DSA algoritmasında şifrelemede ve deşifrelemede farklı anahtarlar kullanılır. NIST tarafından sayısal imza standardı olarak yayınlanan DSA algoritması, Amerika Bileşik Devletleri tarafından kullanılan dijital doğrulama standartlarının bir parçasıdır. Schnorr ve ElGamar tarafından geliştirilen algoritmalara benzer yapıdaki DSA, ayrık logaritma problemine dayanır. DSA algoritmasının RSA algoritmasından farkı şifreleme yapılamamasıdır, sadece imzalama amaçlı kullanılabilmesidir.

1.3. Kriptolojinin Tarihçesi

Günümüzde uğraş alanı artan kriptoloji, tarih boyunca bir çok dönemde de kullanılmıştır. Geleneksel dönem şifrelemelerinin ilki M.Ö. 1900'de Mısır anıtlarının üzerindeki hiyerogliflerde görülmektedir fakat bu şifrelemenin amacı gizli bir mesaj iletmek yerine anıt üzerine yazılan metnin gizemli görünmesini sağlamak ve okunuşunu zorlaştırmaktır. Bu şekildeki şifreleme için Eski Mısır'da "rebus" olarak adlandırılan bir yöntem kullanılmıştır. Rebus yönteminde okunuş sırasında her bir resmi somut bir varlığı gösteren piktogramların anlamlarını görmezden gelerek sadece ses değerlerine yoğunlaşarak mesajı daha gizemli gösterebiliyorlardı. Kriptolojinin günümüzden 4000 yıl önce Mısır'da kullanıldığı arkeologlar tarafından ortaya çıkarılmıştır ve bilinen ilk kriptolog bu dönemde yaşamış bir Mısırlı katiptir. O, efendisinin hayatını hiyeroglifleri şifreleyerek anlatmış ve bazı hiyeroglifler daha önce hiç kullanılmamıştı. Yine bu dönemlerde Mısır Medeniyetinde görülmüş olan kriptoloji izlerinden biride, rahiplerin özel bilgileri saklamak için kriptolojiyi kullanmasıdır ve bu şifrelerin günümüzdeki kriptoloji biliminin temellerini oluşturduğu söylenmektedir. Veri gizlemek için yapılan ilk şifrelemelerin bir diğeri ise M.Ö. 1500 yılında Mezopotamya'da ustaların ürettikleri çömlek tariflerini gizleme amaçlı yazdıkları metinlerde görülmektedir [2,3,4].

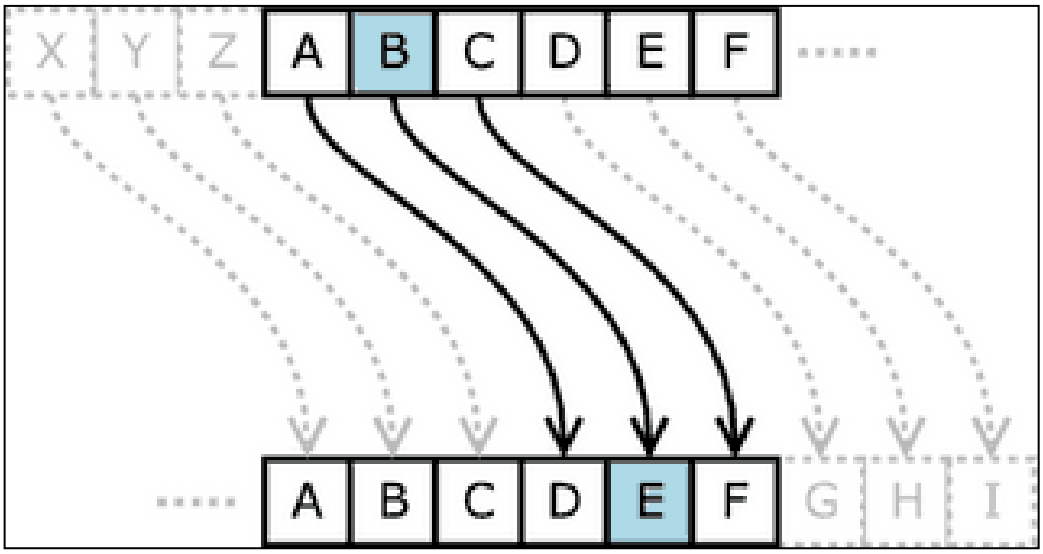
Kriptografi, bu şekilde kullanılmaya başlanmasına karşın, ilk 3000 yılda neredeyse hiç bir gelişme gösterememiştir. Dünyanın birçok yerinde birbirinden bağlantısız bir şekilde en temel biçimlerde kullanılmış fakat şifrelemelerin kullanıldığı medeniyetlerin yıkılışıyla sonraki adımlara geçememiş ve geliştirilememiştir. İnsanlık tarihinde en eski ve en gelişmiş medeniyetlerden biri olan Mısır, çeşitli iletilerinde şifrelemeyi kullanırken, bir diğer gelişmiş medeniyet olan Çin'de kriptoloji biliminin kullanımına dair bir belge ya da bulgu bulunamamıştır. Bunun nedeni olarak yazılarının şifresiz yazılmasının bile çok zor olması gösterilmiştir.

M.Ö. 5. - 6. yüzyıllarda askeri haberleşmede gerekli olan gizlilik nedeniyle kriptografi askeri alanda kullanılmaya başlandı. Askeri alandaki ilk kriptograflar Spartalılardır. Şekil 1.1.'de gösterilen "Scytale" adı verilen silindir görünümündeki bu araç, üzerinde bulunan sembollerin yerlerinin değiştirilmesiyle şifreli mesajı taşıma işlevinde kullanılmıştır. Spartalılar tarafından savaşlarda kullanılan ve sıra

değiştirmeli şifreleme türünün bir örneği olan bu yöntemin hata payı düşük ama çözülme olasılığının yüksektir [2,3].

Şekil 1.1. Scytale

Spartalıların ardından askeri alanda kriptolojiyi Roma Kralı Jül Sezar kullanmıştır. En ilkel şifreleme yöntemlerinden biri olan Sezar Şifrelemesi modüler aritmetik üzerine inşa edilmiştir. Sezar şifreleme mantığı, Şekil 1.2.'de göründüğü gibi, şifrelenmek istenen metnin her karakterinin kendisinden sonra gelen üçüncü karaktere kaydırılması şeklindedir. Bu basit şifreleme yönteminin kırılması da çok kolaydır. Sezar şifreleme kaba-kuvvet (brute-force) saldırılarıyla kolayca çözülebilir. Ayrıca, bir dilde en çok kullanılan harfler ile şifrelenmiş metinde en çok kullanılan harfler karşılaştırarak frekans analizi yapılır ve anahtar boyutu hakkında bilgi edinip şifre çözülebilir [4,5].



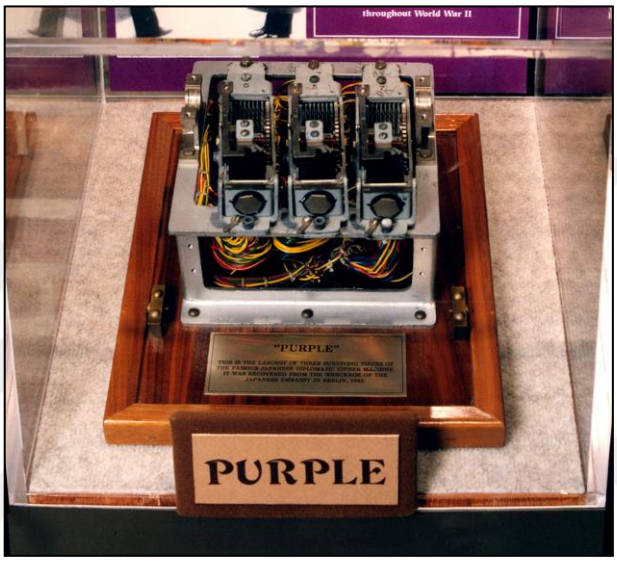
Şekil 1.2. Üç harf atlamalı Sezar şifresi

Kriptografi tarihine dair verilen genel görüşlerin aksine David Khan, The Codebreakers: The Story of Secret Writings (1967) kitabında modern dönemin, bilinen tüm kriptoanaliz yöntemlerini sistemli olarak sınflandıran Araplar arasında başladığını iddia eder. Kahn, Kur'an'ın metin incelemeleri sırasında keşfedilen sıklık çözümlemelerinin, sıra değiştirmeli şifreleme yöntemi ile kodlanan mesajların çözülmesi için esaslı bir yöntem oluşturduğunu söylemektedir. Bu yöntemin mucidi olarak ise M.S. 800'lü yıllarda yaşayan matematikçi Al-Kindi'yi göstermiştir. 9. yüzyılda Kindi, kriptoloji biliminde uygulanan tek alfabeli yerine koyma şifreleme yöntemini geliştirerek frekans analizini bulan ilk kişi olmuştur ve bu konuyla ilgili bir kitap yazmıştır fakat bu kitap kayıp durumdadır [2,3].

Blaise de Vigenère, 1586 yılında şifreleme hakkında bir kitap yazdı. İlk kez bu kitapta açık metin ve şifreli metin için otomatik anahtarlama yönteminden bahsedildi. Vigenere şifrelemesi Sezar şifrelemesinin geliştirilmiş halidir. Günümüzde bu yöntem hala DES, CBC ve CFB kiplerinde kullanılmaktadır [6].

Kriptoloji gerçek işlevini İkinci Dünya Savaşı sırasında ve sonrasında göstermiş ve en büyük gelişmelerini bu tarihlerde kaydetmiştir. İkinci Dünya Savaşı'nda Amerikan Ordusu, Najova kızılderililerinin dillerini biraz daha modernleştirerek ve zorlaştırarak savaşlarda kullanmışlardır. Ortaya çıkan gereklilikler ise yeni yöntemlerin geliştirilmesini zorunlu kılmıştır [7].

1937 yılında, Japonlar, Şekil 1.3.'de gösterilen, "97 Alfabetik Daktilo" adlı bir kripto makinesi geliştirdiler. Ancak makine kod adı olan "Purple" ile tanınmaktadır. Cihaz, iki daktilo ve 25 karakterli alfabetik denetim santraline sahip bir elektrikli rotor sisteminden oluşmaktadır. Cihazın en önemli özelliği, kullandığı ikinci elektrikli daktilo ile şifrelenmiş mesajı bir kağıt üzerine yazabilmesiydi. Amerikalı kriptolog William Frederick Friedman, İkinci Dünya Savaşı'nda Japonlar'ın Purple Machine şifreleme sistemini çözdü [8].



Şekil 1.3. Japonların Purple şifreleme makinesi

İkinci Dünya Savaşı süresince Almanlar, Arthur Scherbius tarafından icat edilen Enigma makinesini kullanmışlardır. Şekil 1.4.'te verilen ünlü Enigma şifreleme makinesi 116 bitlik bir anahtar uzunluğuna sahiptir. Rotasyonel şifreleme yöntemini kullanan, elektro-mekanik bir aygıt olarak tasarlanan Enigma makinesinin temel prensibi çoklu alfabe yöntemidir. Savaşta şifre bilimcilik yapan İngiliz Alan Turing, Enigma şifresinin yapısal zayıflıklarını kullanarak, Colossus isimli ilk tüplü bilgisayar yardımıyla Nazilerin şifreleme yöntemini çözmüş oldu [4,9].

Şekil 1.4. Almanların Enigma şifreleme makinesi

Russian Fialka, İkinci Dünya Savaşı sonrası soğuk savaş döneminde Sovyetler Birliği tarafından geliştirilen M-125 kod adlı bir şifreleme makinesidir. Şekil 1.5.'te verilen Fialka, Latin ve Rus alfabesini desteklemektedir ve Enigma mantığıyla tasarlanmıştır [10].

Şekil 1.5. Rusların Fialka şifreleme makinesi

Bu şifreleme makinelerine benzer olarak; Amerika tarafından Enigma'nın kırılması sonrasında üretilen "Sigaba", yine Amerikan ordusu tarafından ilk olarak İkinci Dünya Savaşında daha sonra da Kore Savaşında kullanılan "U.S. M-209", İkinci Dünya Savaşı sırasında İsveç ordusu tarafından Enigma makinesinin yerine üretilen "Swiss NEMA", İngilizlerin kripto makinesi "Typex", 1970 yılında bir İsveç şirketi tarafından üretilen "HC-9" yakın tarihte kullanılan şifreleme makinelerinden bazılarıdır. [10].

Günümüzde en yaygın olarak kullanılan şifreleme yöntemi ise elektronik verilerin şifrelenmesi için 2000 yılında DES (Data Encryption Standart) standardının yerine sunulan AES (Advanced Encryption Standard) şifreleme standardıdır.

Her dönemde kullanılan farklı şifreleme tekniklerine rağmen kriptoloji alanındaki asıl gelişmeler süper bilgisayarların icat edilmesiyle son dönemlere dayanmaktadır. Ama hala kullanılabilirliği kolay ve çözülmesi imkansız olan bir şifreleme tekniği geliştirilememiştir. Son yıllarda üzerinde durulan kuantum kriptografisi, şifrelemede kullanılan anahtar değişim protokolü ile ön plandadır. Bu kriptografide temel prensip, tek kullanımlık anahtarlı (one-time-pad) kriptografi tekniğinin kullanılmasıdır. Mesajın iletilmesiyle ilgilenmeyen bu teknik, mesajın şifrelenmesi ve şifrelenmiş mesajın çözülmesinde kullanılan anahtarın güvenilir bir şekilde alıcı ve verici arasında değişimi ile ilgilenir. Kuantum kriptografi tekniğinde veri iletimi

geleneksel yollarla yapılmaz yani verinin iletilmesinde elektriksel işaretler yerine fotonlar kullanılır ve güvenli iletişim için kuantum mekaniği kullanılır. Gizli dinleme, fiziksel bir nesnenin ölçülmesi olarak görülebilir bu yüzden verinin kuantum taşıyıcısı üzerinde yapılan ölçümler onu boza dolayısıyla bu türlü girişimler her zaman iz bırakır [11]. Fotonlarla yapılan bu iletim için gerekli olan iletişim kanalı için fiber optik ağ gerekmektedir. Bu yüzden kuantum kriptografi tekniği sivil yaşamda kullanılamamaktadır. Şuan için askeri alanda kısıtlı imkanlarla kullanılan kuantum kriptoloji, 10-15 yıl içerisinde sivil yaşamda da kullanılabilecek duruma gelecektir [10].

Türkiye'de kriptolojiden bahsedecek olursak, ilk ulusal kripto cihazı üretimi 1974 yılında Gebze'de TUBİTAK bünyesindeki Marmara Araştırma Merkezi'nde bulunan Elektronik Araştırma Ünitesi'nde başlatılmıştır. Yurt dışından alınan kripto cihazlarının maliyetinin yüksek olması ve güvenilirliğinin olmaması nedeniyle TSK, ulusal kripto cihazının Türkiye'de üretilmesi gerektiği kanısına varmıştır. Türkiye'de ilk defa, 23 Kasım 1976 tarihinde ulusal on-line kripto cihazının prototipi üretilmeye başlanmıştır ve 1978 yılının Şubat ayında üretim tamamlanmıştır. Şekil 1.6.'da gösterilen bu cihaza Milli On-Line Kripto Cihazı - I (MİLON-I) adı verilmiştir. TSK'nın artan güvenlik talepleri nedeniyle 1990 yılında MİLON - II ve 1995 yılında MİLON - III hizmete sunulmuştur. Günümüzde TUBİTAK bünyesinde bulunan Ulusal Elektronik ve Kriptoloji Araştırma Enstitüsü, kriptolu USB bellek, kriptolu cep telefonu, taşınabilir kriptolu çevrimdışı cihaz gibi birçok proje geliştirmektedir [10,12].

Şekil 1.6. MILON veri kripto cihazı

1.4. Sır Paylaşımı ve Görsel Sır Paylaşımı

Verinin güvenliğini sağlamak için şifreleme ve gizleme dışında farklı yöntemlerde vardır. Sır paylaşımı yöntemi, ilk defa 1979 yılında Shamir [13] ve Blakley [14] tarafından aynı zamanlarda ortaya atılmıştır. Bu yönteme aynı zamanda "(k,n) Eşik Şeması" denmektedir. Yöntemin ana fikri, gizli olan verinin "n" kişiye dağıtılmasıdır ve bu n kişiye gönderilen bilgi "pay" olarak adlandırılır. Bu pay değerlerini bir fonksiyon oluşturur ve hiç bir pay tek başına bir anlam ifade etmez. Katılımcılardan en az "k" tanesi ellerindeki pay bilgilerini bir araya getirerek gizli veriyi ortaya çıkarırlar. Böylece veri tek kişinin sorumluluğundan kurtulup bir grubun sorumluluğuna girmiş olur ve verinin güvenliği artar. Shamir tarafından önerilen sır paylaşımı yöntemi polinom tabanlıyken, Blakley tarafından önerilen sır paylaşımı yöntemi hiperdüzlem denklemlerinin geometrik özelliklerinden yararlanmaktadır. Bu alanda yapılmış diğer çalışmalar arasında sayılar teorisinin özelliklerinden olan CRT (Chinese Remainder Theorem = Çinli Kalan Yöntemi) yöntemini kullanan Mignotte ve Asmuth-Bloom yöntemleri gösterilebilir [15].

Gizli görüntülerin güvenlik sorunlarını aşabilmek için, çeşitli gizli görüntü paylaşım yöntemleri vardır. Noar ve Shamir tarafından 1994 yılında sır paylaşımı (secret sharing) adında bir teknik geliştirilmiştir. Bu yöntemde pikselleri sadece beyaz ve siyahtan oluşan ikili (binary) görüntü anlamsız iki parçalaya ayrılmaktadır ve bu iki pay bir araya getirildiğinde orijinal ikili görüntü ortaya çıkmaktadır. Bu sır paylaşımı

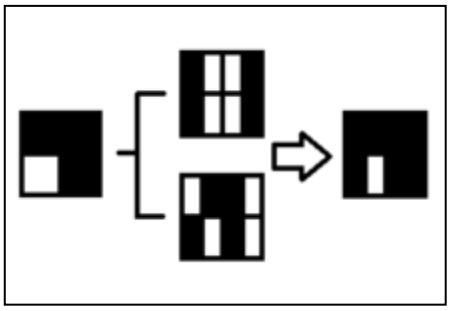
tekniğinin en önemli özelliği, herhangi bir hesaplamaya ihtiyaç duymaksızın insanın görme sisteminin sırrı ortaya çıkarmasıdır [16].

Daha sonra (k,n) eşik şeması, görsel sır paylaşımında kullanılmıştır. (k,n) görsel sır paylaşımında, görüntü üzerine görsel şifreleme teknikleri kullanılarak n tane anlamsız pay oluşturulmaktadır ve bu paylar katılımcılara dağıtılmaktadır. Bu katılımcılardan k tanesi, slayt üzerine basılmış paylarını tam olarak üst üste getirdiğinde görsel sır ortaya çıkmaktadır.

1.5. Görsel Kriptoloji ve Stenografi

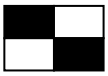
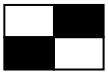
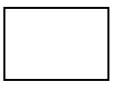
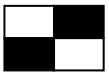
Teknolojinin gelişmesiyle birlikte insanlar arasında bilgi paylaşımı genellikle internet ağları aracılığıyla yapılmaktadır. Fakat bu gelişmelerle kişisel iletişimler dahil bütün bilgi alışverişleri takip edilebilmekte ve istenmeyen kişiler tarafından ele geçirilebilmektedir. Bu nedenle dijital ortamda bulunan verilerimizi koruma ihtiyacımız artmıştır. Özellikle askeri bilgiler, ticari tanımlamalar, devletlerarası sırlar veya şirketlerin kendi içlerindeki özel bilgilerinin ele geçirilmesi büyük sıkıntılara yol açabilmektedir. Bu sıkıntıların önüne geçebilmek için veriler saf halleriyle iletilmemeli, geri dönüşümü yapılacak şekilde şifrelenerek ya da gizlenerek gönderilmelidir. Gizli görüntülerin güvenlik sorunlarıyla başa çıkmak için, çeşitli gizli görüntü paylaşım programları geliştirilmiştir. Bu programlarda veri/görüntü şifrelenebilir ya da bir başka veri içerisine gömülerek gizlenebilir. Bu iki yöntemin birlikte kullanılması veri güvenliğini arttırmaktadır.

Özel bir şifreleme yöntemi olan görsel kriptolojinin temeli insanın görme sistemine dayanmaktadır. Görüntü parçaları uygun anahtar değeri şeklinde kullanıldığında insan görmesi ile çözülebilmektedir. Görsel şifrelemede görüntü bir kurala göre parçalara ayrılır ve bu parçalar tekrar üst üste getirildiğinde orijinal görüntü ortaya çıkar. Genellikle asetat kağıdına basılmış iki şeffaf görüntüden biri rastgele piksellerden, diğeri ise birleştiğinde gizli bilgiyi ortaya çıkaracak olan bağımlı piksellerden oluşur. Ayrı ayrı görüntülerden herhangi bir bilgi elde edilemez, fakat görüntüler hizalanmış şekilde üst üste koyulduğunda gizli bilgi açığa çıkar [17].



Şekil 1.7. Görsel şifrelemeye örnek

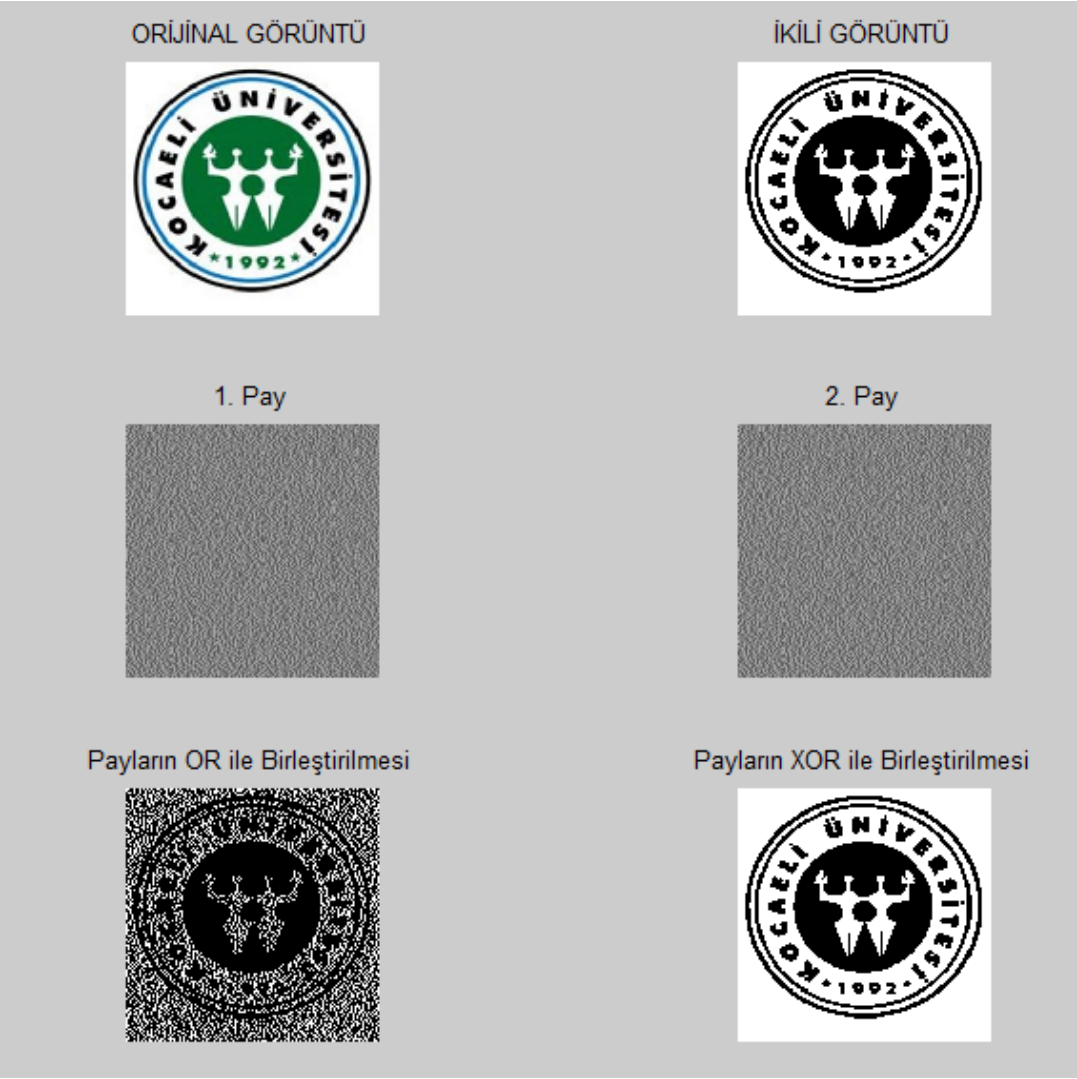
Noar ve Shamir'in önerdiği ikili (binary) bir görüntüyü iki anlamsız görüntüye paylaştırmak görsel kriptolojide bir tekniktir. İkili görüntünün piksel değerleri siyah için 0 ve beyaz için 255 sayılarıdır. Piksel değerleri sadece bu iki sayıdan oluşan bir görüntüyü OR ya da XOR işlemleriyle anlamsız iki görüntüye ayırabiliriz ve aynı şekilde bu işlemleri kullanarak orijinal veriyi elde edebiliriz. Bu iki işlem arasındaki fark, Şekil 1.8.'de gösterildiği gibi OR işleminde siyah görüntüler tamamen elde edilebilirken beyaz görüntüler elde edilememektedir. Tablo 1.1. ve Şekil 1.9.'da gösterildiği üzere, XOR işleminde böyle bir sorun yaşanmamaktadır [17].

Gizli Görüntü	1. Parça	2. Parça	1. ve 2. Parçadan Oluşan Görüntü
			
			
			
			

Şekil 1.8. Siyah ve beyaz pikselli görüntülerin OR işlemiyle paylaştırılması

Tablo 1.1. OR ve XOR yöntemlerinin karşılaştırılması

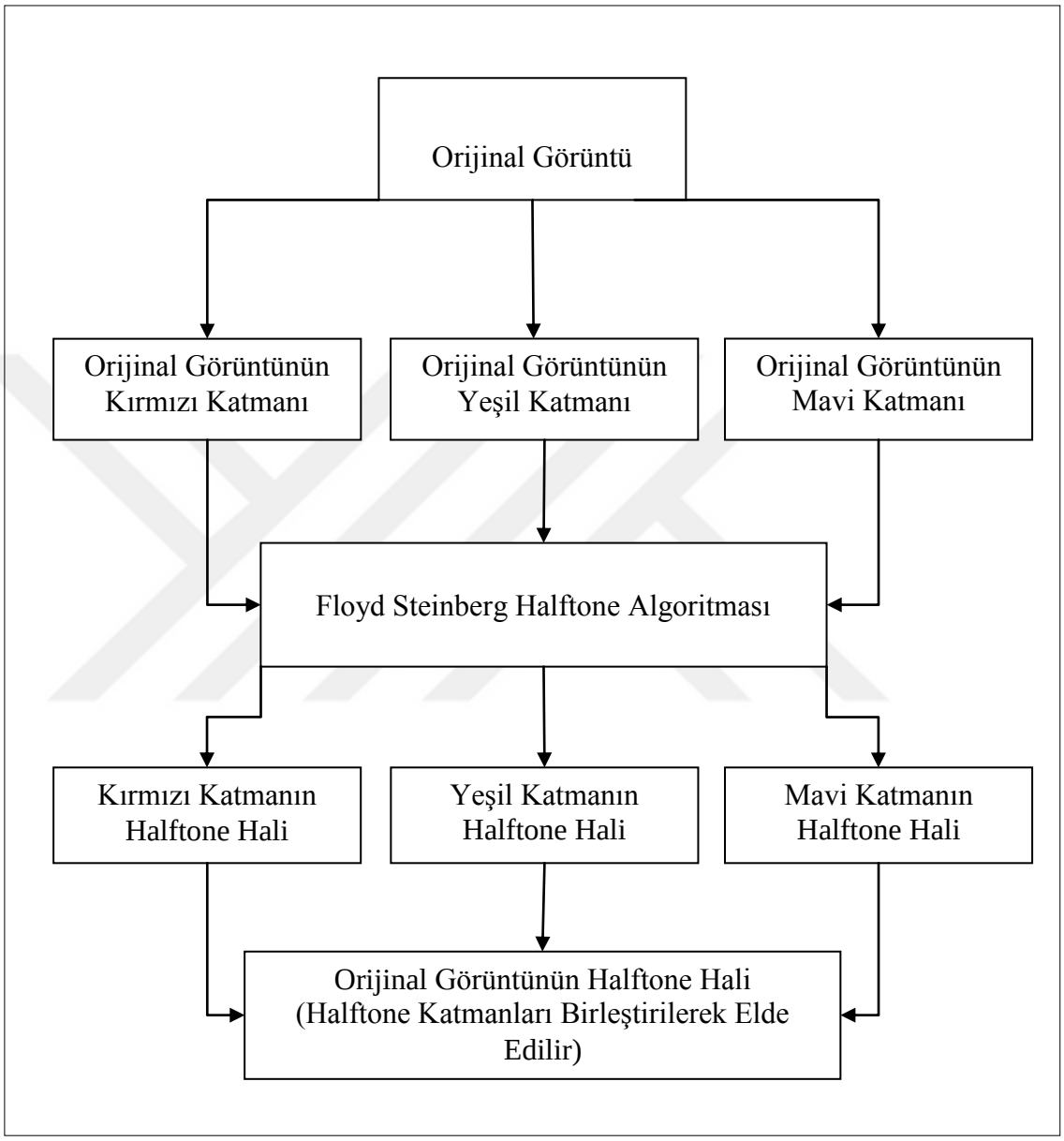
Gizli Görüntü	Parçalar	OR	XOR
0 (Beyaz Piksel)	$\begin{bmatrix}1 & 0\\1 & 0\end{bmatrix}, \begin{bmatrix}1 & 0\\1 & 0\end{bmatrix}$	$\begin{bmatrix}1 & 0\\1 & 0\end{bmatrix}$	$\begin{bmatrix}0 & 0\\0 & 0\end{bmatrix}$
1 (Siyah Piksel)	$\begin{bmatrix}1 & 0\\1 & 0\end{bmatrix}, \begin{bmatrix}0 & 1\\0 & 1\end{bmatrix}$	$\begin{bmatrix}1 & 1\\1 & 1\end{bmatrix}$	$\begin{bmatrix}1 & 1\\1 & 1\end{bmatrix}$



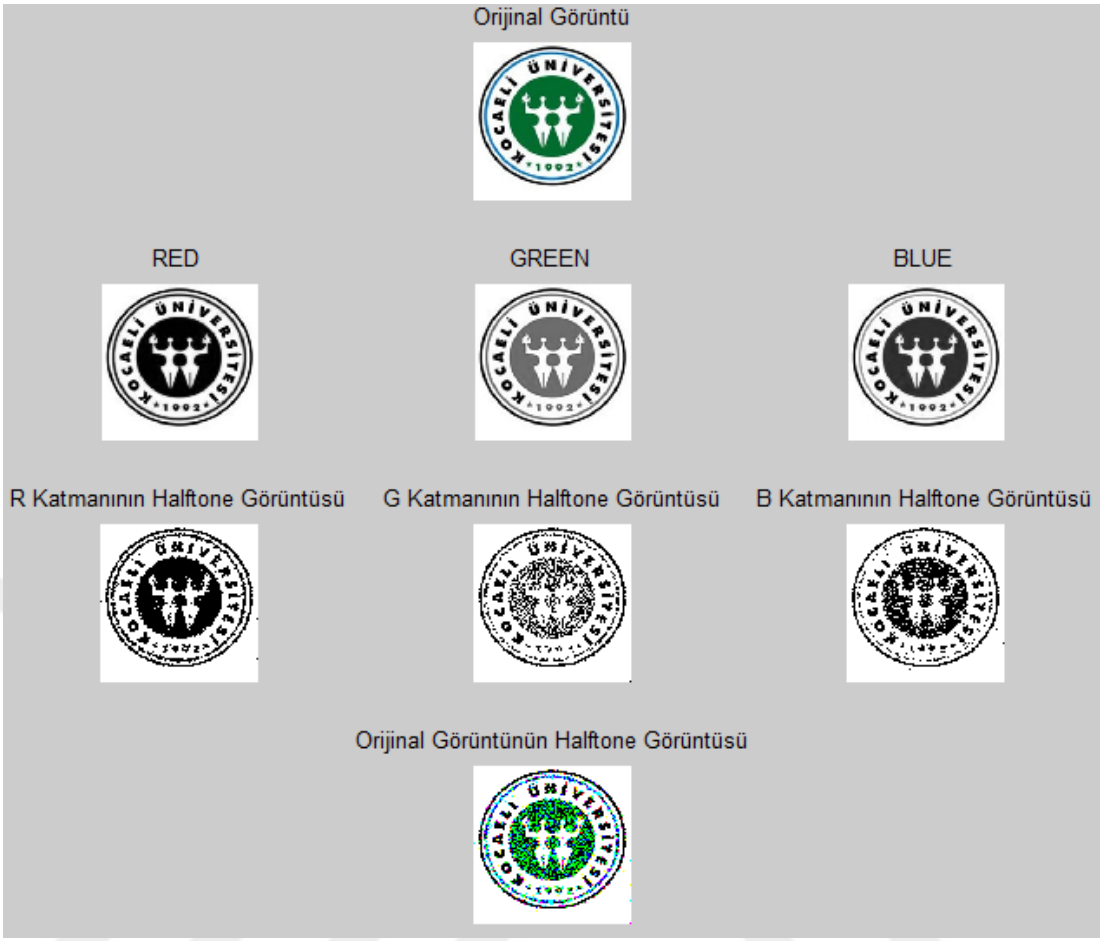
Şekil 1.9. İkili bir görüntünün OR ve XOR ile birleştirilmesi

Noar ve Shamir'in önerdikleri yöntem sadece ikili görüntülerde çalışır. Bu yüzden renkli görüntülerde aynı işlemi yapmak için görüntünün mavi, kırmızı ve yeşil katmanlarına ayrılıp, elde edilen görüntülere halftone tekniği kullanılarak görüntünün ikili görüntüye dönüştürülmesi gerekmektedir. Orijinal görüntüyü halftone görüntüye çevirirken, Şekil 1.10.'de gösterildiği gibi Floyd Steinberg Algoritmasını

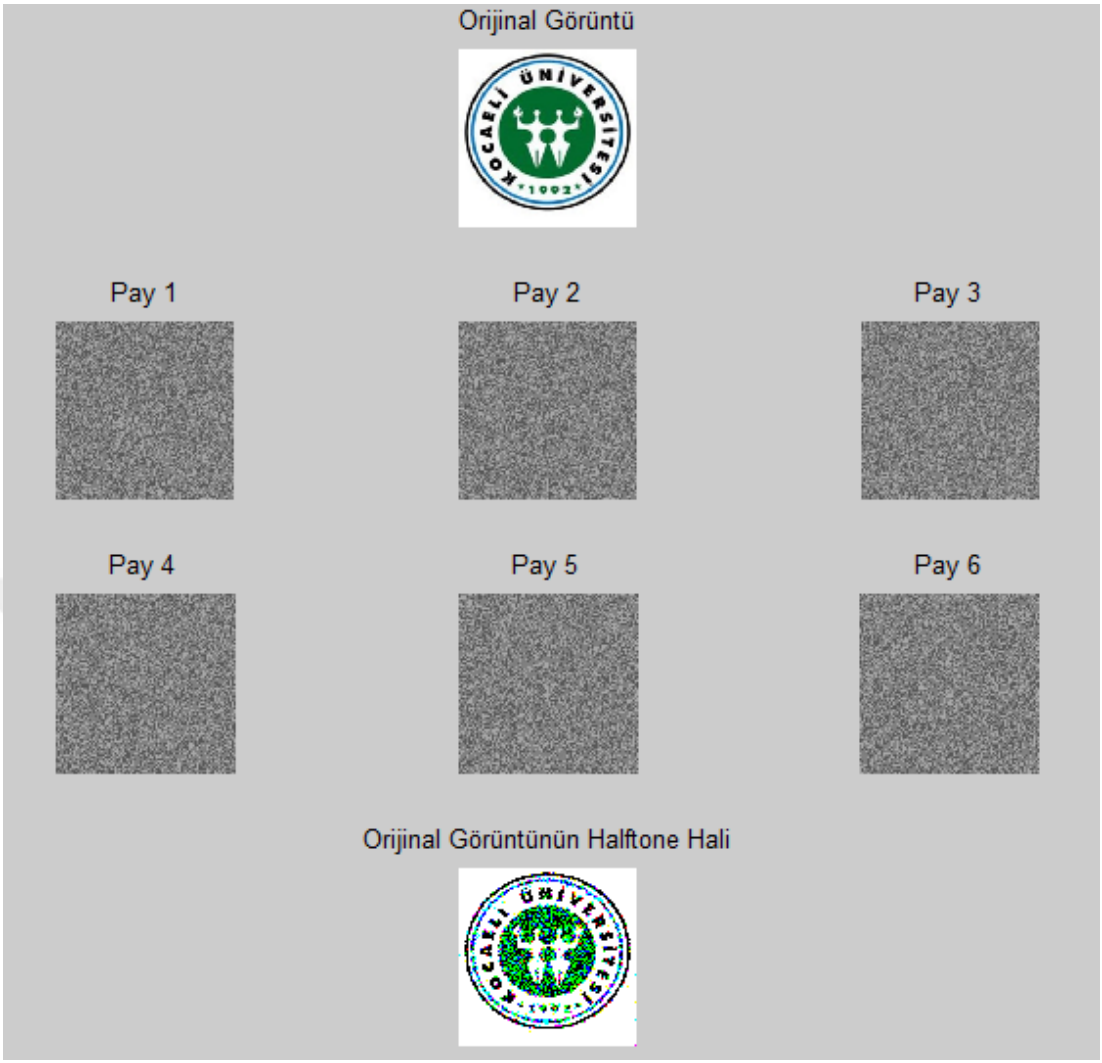
kullanabiliriz. Şekil 1.11.'de gösterildiği gibi elde edilen bu yeni görüntü Şekil 1.12.' te verildiği gibi Shamir'in yöntemiyle sırlara ayrılır, daha sonra yine Şekil 1.12.'te gösterildiği gibi aynı yöntemle birleştirerek orijinal görüntü elde edilebilir [17].



Şekil 1.10. Renkli görüntünün halftone görüntüye dönüşüm algoritması



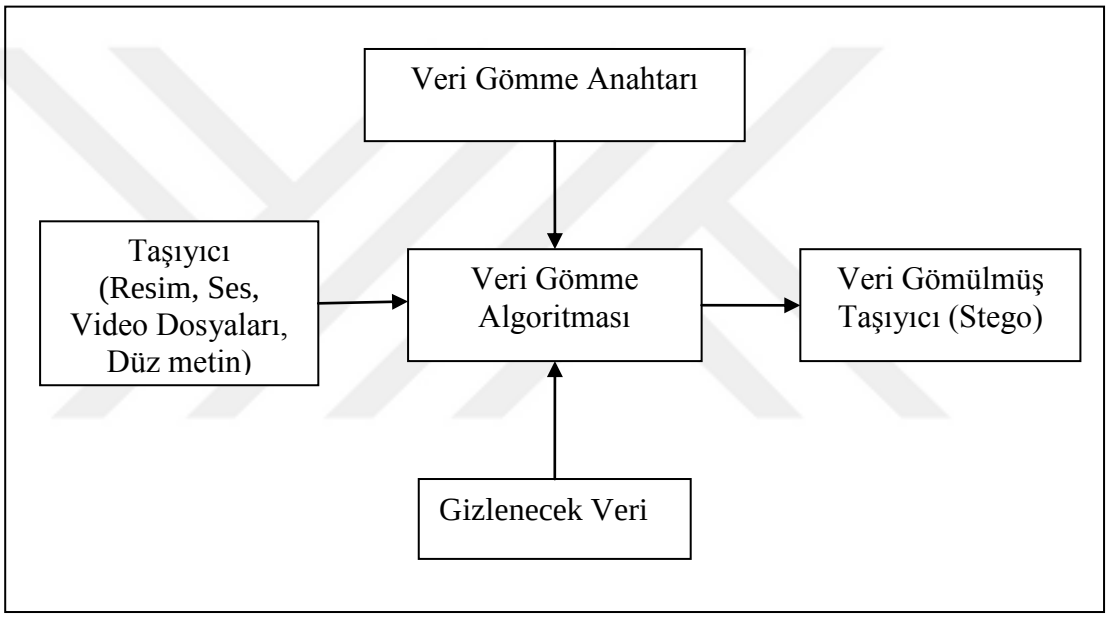
Şekil 1.11. Renkli görüntünün halftone görüntüye dönüşümü



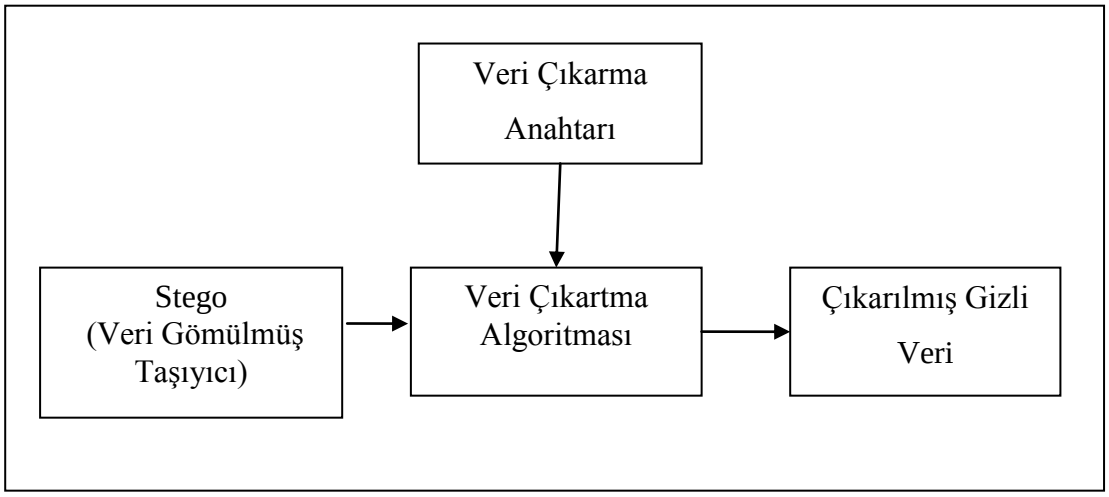
Şekil 1.12. Renkli görüntünün Shamir yöntemiyle paylara ayrılması

Stenografi ise bir verinin, görüntünün ya da sesin içine gizlenmek istenen verinin gömülerek veri güvenliğini sağlama yöntemidir. Stenografi, Yunanca "steganos" ve "grafi" kelimelerinden türetilmiş olup Türkçede "gizlenmiş ya da kaplanmış yazı" anlamına gelmektedir. Gizli veriyi içerisinde barındıran taşıyıcıya "stego" adı verilir. Kriptolojiden farklı olarak stenografide verinin şifrelenmesi önem arz etmez. Kriptografi, güvenilirliğini şifre algoritmasından alır, verinin varlığının bilinmesi önemli değildir ve verinin taşınacağı kanal önemsenmez. Stenografide amaç, iletilmek istenen verinin ve bu verinin varlığının başkalarının fark etmesini engelleyecek kadar iyi saklamaktır. Verinin varlığı ne kadar iyi gizlenirse, taşınacak veri o kadar güvendedir. Verinin taşınacağı kanal ve çözüleceği bilgiler olmadan alıcıya ulaşmasının hiç bir anlamı yoktur. Bu yüzden stenografide verinin nasıl taşınacağının saklanması gerekir.

Görüntü stenografide, bilgilerin görüntü dosyaları içerisine saklanmasının çeşitli yöntemleri vardır. Görsel kriptoloji ve stenografinin her ikisi de verilerin güvenli bir şekilde alıcıya ulaştırılması ve üçüncü şahısların eline geçmesini engellenmesi amacıyla kullanılır. Bilgi gizlemede en önemsiz bite ekleme (LSB-Least Significant Bit), maskeleme ve filtreleme, algoritmalar ve dönüşümler en çok kullanılan yöntemlerdir. Kriptoloji ve stenografinin birleştirerek aynı anda kullanılması verilerin çok daha güvenli bir şekilde alıcıya ulaşmasını sağlar. Verinin hem şifrelenmesi hem de gizlenmesi, gizliliğin tespit edilmesi halinde ortaya çıkan şifrelenmiş verinin deşifre edilmesini gerektirecektir.



Şekil 1.13. Stenografide veri gömme algoritması



Şekil 1.14. Stenografide gizli veri çıkarma algoritması

1.6. Görsel Kriptoloji ve Stenografi'nin Tarihçesi

Temeli çok eski çağlarda atılmış olsa, görsel kriptolojinin geçmişi son 23 yıla dayanmaktadır. İlk kez 1994 yılında Noar ve Shamir'in ortaya attığı görsel kriptografik yöntemin temeli, aslında ilk kez kimin tarafından yapıldığı bilinmeyen ve bizimde bilmeden kullandığımız basit bir işleme dayanmaktadır. En basit görsel kriptografi uygulaması, defterin bir sayfasına yazılıp alınan bilginin, defterin alt sayfasındaki görünmeyen izinin bir kurşun kalemle fazla bastırmadan tarayarak orijinal yazının negatifini (siyah zemin üzerine beyazla yazılmış halini) ortaya çıkarmaktır.

Sır paylaşımı kavramı, Noar ve Shamir tarafından görüntü alanında kullanılmış ve bilgisayar ile hesaba gerek olmaksızın, insanın görme sisteminin de şifreyi çözebildiği görsel şifrelemeyi geliştirmiştir [16]. Noar ve Shamir tarafından önerilen bu şema, çeşitli çalışma alanlarında geliştirilmeye çalışılmıştır. 2002 yılında Thein ve Lin, gizli görüntülerin paylaşımında Shamir'in sır paylaşım yöntemini kullanmayı önermişlerdir [18]. Gürültü şeklindeki paylar dikkat çekebileceği için, sırrın stenografi ile başka bir verinin içine gizlenmesi ve daha sonra paylaştırılması ile ilgili çalışmalar yapılmaya başlanmıştır.

Günümüzde yaygın olarak kullanılan stenografi, tarihte ilk kez M.Ö. 440 yılında Demaratus'un Yunanistan'a yaklaşan bir saldırı tehlikesini, tahta bir tablete kazıyıp üzerini bal mumu kaplamasıdır. Böylece cisim kullanılmamış bir tablete benzerdi, fakat mum eritildiğinde sır ortaya çıkardı. Diğer bir stenografi örneği ise M.Ö. 5. yy'da saçları tıraşlanan bir kölenin kafasına uyarı mesajı yazılmış ve saçları tekrar örtecek kadar uzayınca köle şehre gönderilmiştir. Köle mesajın gideceği yere ulaştığında, kölenin saçları tekrar kesilerek mesaja ulaşılmış ve mesaj dikkat çekmeden gideceği kişiye ulaştırılmıştır [19].

Bilinen ilk örnekleri bunlar olan stenografi, İkinci Dünya Savaşı'nda da sıkça kullanılmıştır. İkinci Dünya Savaşı sırasında, New York'ta bir ajan, Amerikan Ordusu'nun hareketlerini bebek siparişi gibi görünen mektuplarla Güney Amerika'daki adreslere gönderiyordu. Casusun stenografi tekniği ise düz bir yazıydı. Alıcı, yazıdaki her kelimenin ikinci harflerini birleştirdiğinde gizli mesaj ortaya

çıkıyordu. Fransızlar tarafından kullanılan görünmez mürekkepler, mektup pullarının arkasına yazılan çeşitli notlarda İkinci Dünya Savaşı sırasında kullanılan stenografi yöntemlerinden bazılarıdır [19].

Yakın tarihte ise resim, ses ve metin gibi dosya türlerinin içerisine veri saklama teknikleri geliştirilmiş ve stenografide de bilgisayarlar kullanılmaya başlanmıştır. Ses dosyaları içerisine düşük bit kodlaması (Low Bit Encoding), faz kodlaması (phase coding), yayılmış spektrum (spread spectrum) ve yankı veri saklaması (echo data hidding) yöntemleri ses stenografisinin örnekleridir. Metin içerisine boşluk kullanımı, dilin yapısı ve eş anlamlı kelimelerden faydalanarak veri saklama yöntemleri ise metin stenografisidir. 2000'li yıllardan sonra kullanılan LSB (Least Significant Bit), BPCS (Bit Plane Complexity Segmentation), dönüştürme tekniği ve permütasyon tekniği ise görüntü stenografisinin örnekleridir.

2. LİTERATÜR ÇALIŞMASI

İletişimin gizliliğinde ve güvenli mesaj iletiminde kullanılan iki önemli teknik kriptografi ve steganografidir. Bu alandaki çalışmaların nihai amacı, açık haberleşme kanalları kullanılarak verinin güvenli bir şekilde alıcıya ulaştırılmasını sağlamaktır. Bu alanda yapılan çalışmaların bir özeti bu bölümde verilmektedir.

Görüntüler üzerinde yapılan şifreleme çalışmalarının ilki olan [16]'ten sonraki çalışmalarda, 2000'li yıllara kadar Shamir algoritmasının benzer versiyonlarının kullanıldığı görülmektedir.

[18]'de bir sır görüntüsünün, n tane karanlık görüntüye paylaştırılması ve bu görüntülerden $r \leq n$ koşulunu sağlayan herhangi r tane karanlık görüntülerin, tüm sır görüntüsünü yeniden ortaya çıkarmak için kullanılabileceği önerilmiştir. Bu yöntemde her bir karanlık görüntünün boyutu, sır görüntüsünün boyutundan küçüktür. Bu özelliğin, gölge görüntülerinin depolama, iletim veya görüntü gömme gibi daha sonraki işlemlerde fayda sağlayacağı savunulmuştur.

[20]'de hareketsiz görüntülerde çeşitli stenografik teknikler, analiz ve test edilmiştir. Görüntüye büyük miktarda veri gömüldüğünde, görüntünün görünür özelliklerinin değişebileceği gösterilmiştir. RSA ve Eliptik Eğri Kriptografisi (ECC) tabanlı dijital imzalar karşılaştırılmıştır ve stenografide avantaj ve dezavantajları analiz edilmiştir.

[21]'de Harmsen tarafından renkli görüntülerde stenografi tespiti için ortaya atılan fakat gri tonlamalı görüntülerde başarısız olan Histogram Karakteristik Fonksiyonu kullanılmıştır. HCF'yi uygulamak için, alt örneklem bir görüntü kullanılarak çıktının kalibre edilmesi ve olağan histogram yerine bitişik histogramın hesaplanması gibi iki yeni yol tanıtılmıştır.

[22]'de renkli grafik ve resimleri, gri görüntülere dönüştürmek için tersinir bir yöntem geliştirilmiştir. Gri görüntü üzerine uygulanan, düşük çözünürlüklü yüksek frekanslı yapıdaki renkleri haritalama yöntemini esas alınmıştır. Renkli görüntüleri, gri tonlamalı görüntülere dönüştürürken dalgacık dönüşümü kullanılmıştır.

[23]'de öncekilere göre daha etkili olan bir piksel genişlemesi kullanılarak, yeni bir renkli (k,n) görsel sır paylaşım şeması önerilmiştir. Bu çalışmada Blundo ve ark. [24] ile Yang ve Laih [25] makalelerinden yararlanıldığı belirtilmiştir.

[26]'da gizli görüntü paylaşımı, JND modeli ve dalgacık dönüşümünü kullanarak, renkli görüntüler için yeni bir telif hakkı koruma şeması önerilmiştir. Bu şema, filigran gömme ve filigran çıkarma olarak iki aşamadan oluşmaktadır. Deneysel sonuçlar, önerilen şemanın çeşitli saldırılara direndiğini göstermiştir.

[27]'de ölçeklenebilir gizli görüntü paylaşım şeması sunulmuştur. Bu şemada, yeniden oluşturulmuş görüntünün netliği, katılımcıların sayısı ile orantılı olacak şekilde, görüntünün n katılımcıya paylaştırılması önerilmiştir.

[28]'de siyah-beyaz piksel içeren görüntülerde mükemmel kontrastlı görsel sır paylaşımı elde ettiklerini beyan edilmiştir.

[29]'da Noar ve Shamir'in görsel kriptoloji modeli altında, piksel genişlemesi olmaksızın tek renkli (k,n) görsel sır paylaşımı ve piksel genişlemeli tek renkli genişletilmiş görsel kriptoloji şemaları önerilmiştir. Ayrıca Tuyls'un görsel kriptoloji modeli altında, siyah beyaz (k,n) görsel sır paylaşımını ve siyah beyaz (k,n) genişletilmiş görsel sır paylaşımı önerilmiştir. Önerilen şemanın deneysel sonuçları verilmiş ve önerilen şema, literatürdeki bilinen şemalarla karşılaştırılmıştır.

[30]'da gri tonlamalı görüntülere uygulanan tipik LSB gömme ve LSB eşleştirme stenografi yöntemlerini algılamak için yeni bir yöntem tanıtılmıştır. Önerilen yöntemde, gri seviye çalışma uzunluğu matrisinden çıkarılarak seçilen bazı özelliklerde yapılan değişiklikler belirlenmektedir.

[31]'de bir görüntüyü şifrelemek için rastgele ızgara görsel kriptoloji (n-VCRG) kavramlarını tanıtılmıştır. Spesifik olarak, P görüntüsü ile ilgili bir VCRG-n kümesi, asetatlara basılan n tane rastgele ızgaralardan oluşur. Yalnızca n tane asetat üst üste getirildiğinde, P görüntüsü herhangi bir bilgi işlem aygıtı olmaksızın, insan gözüyle anlaşılabilmektedir ve n'den az asetatlar P hakkında herhangi bir bilgi vermemektedirler. Çalışmada ikili, gri tonlamalı ve renkli görüntüler için VCRG-n

şifreleme şemaları tasarlanmış ve doğrulukları ispatlanmıştır. Önerilen şemada ekstra piksel genişlemesi olmamaktadır.

[32]'de renkli görüntüler için halftone tekniğine dayalı yeni bir gizli görsel şifreleme şeması önerilmiştir. Bu şemada öncelikle renkli görüntü, üç tek renkli görüntüye ayrıştırılmış ve ikinci olarak halftone tekniğiyle bu görüntüler ikili görüntüye dönüştürülmüştür. Geleneksel ikili sır paylaşım şeması kullanarak pay görüntüleri elde edilmiştir. Ayrıca gizli görüntüde görünen renklerin sayısı farklı olduğunda paylaşımların boyutunun değişmeyeceği gösterilmiştir.

[33]'de, çalışmanın yalnızca bir kaç belirli ikili gizli resim için geçerli olabileceği gösterilmektedir ve diğer durumlarda güvenliğin garanti edilemeyeceği gösterilmiştir.

[34]'de rastgele ızgaralar kullanılarak artan görsel şifreleme şeması önerilmiştir. Yöntemde, pay boyutlarının küçülmesi, depolama ve/veya yazdırma gibi işlemleri daha verimli yapılabildiği beyan edilmiştir.

[35]'de geleneksel LSB eşleşmesinin güvenliğini arttırmak için geliştirilmiş iki LSB eşleştirme yöntemi önerilmiştir.

[36]'da gizli pikseller n'li işaretleme sistemine dönüştürülmüştür ve kamufle edilmiş piksellerden orijinal pikselleri yeniden oluşturmak için kullanılan bilgi verileri hesaplanmıştır. Bu yolla kayıpsız gizli görüntülerin alınabileceği ve stego görüntüsünün orijinal görüntüye tekrar çevrilebileceği gösterilmiştir.

[37]'de renkli görüntüler için, CMY modeli, halftone tekniği ve geleneksel ikili görüntü paylaşım şemasına dayalı yeni bir görsel şifreleme şeması önerilmiştir. Bu yöntemde üretilen görüntü payları bir ağ üzerinden hedefe iletilmektedir ve üzerinde payların olduğu asetatlar üst üste getirilerek sır çözülmektedir.

[38]'de iki dikdörtgen paylaşımlı görüntü üzerinde herhangi bir piksel genişlemesi olmaksızın iki ikili gizli görüntü paylaşabilen yeni bir görsel sır paylaşımı yöntemi önerilmiştir. Sonuçlarda önerilen yaklaşımın yalnızca piksel genişlemesini değil, aynı zamanda gizli görüntüler için bir iyileştirme kalitesine sahip olduğu da gösterilmiştir.

[39]'da piksel genişlemesi, gizli görüntü sayısı, görüntü formatı ve üretilen payların türüne dayanarak görsel şifreleme şemaları incelenmiştir ve performans analizleri yapılmıştır.

[40]'da renkli görüntüler için, girişte dört resim alan ve girilen dört resimden üç tanesine karşılık gelen üç resim üreten bir sistem algoritması önerilmektedir. Önerilen kod çözme algoritması, bu üç görüntünün bazı alt bölümlerini seçmek, bunları asetatlara basmak ve üst üste birleştirerek görüntüyü açığa çıkarma işlemleri ile çalışmaktadır. Önerilen algoritmada yeniden oluşturulan görüntü, orijinal gizli görüntü ile aynı boyuttadır.

[41]'de Boolean tabanlı görsel sır paylaşımına dayanan etkili bir (n+1,n+1) çoklu gizli görüntü paylaşım şeması önerilmektedir. Bu şema sadece görüntülerin gizli tutulması için değil, aynı zamanda çoklu sırların paylaşılma kapasitesinin arttırılması için de önerilmektedir.

[42]'de Haar dalgacık dönüşümü ve Shamir yöntemi ile hızlı bir görüntü paylaşımı önerilmiştir. Önerilen paylaşımda öncelikle gizli görüntüyü çeyrek boyuta indirgemek için Haar dalgacık dönüşümünü kullanılmıştır. Daha sonra yalnızca gölge görüntüleri oluşturmak için Shamir algoritması LL alt bantlarına uygulanmıştır. Bu yöntem, hesaplama süresini azaltabilmek için yalnızca çeyrek boyutlu bir görüntüyü işlemektedir ve gizli görüntüyü geri döndürebilmektedir.

[43]'de filigran ve doğrulama kapasitelerini içeren ikili görüntüler için görsel şifrelemede yeni bir yaklaşım önerilmektedir. Önerilen yöntemde, bir nxn filigran görüntüsü, iki gölge oluşturmak için nxn gizli görüntüye yerleştirilmiştir ve yeniden oluşturulmuş görüntünün doğruluğunu kanıtlamak için nxn filigran görüntüsü kullanılmıştır.

[44]'de parmak izi görüntüleri, iris kodları ve yüz görüntüleri gibi biyometrik verilere gizlilik kazandırmak için görsel şifreleme kullanılması önerilmiştir.

[45]'de rastgele payları anlamlı kapak görüntülerine gömerek gerçekleştirilen bir genişletilmiş görsel kriptoloji şeması önerilmektedir.

[46]'da görsel sır paylaşımları için kimlik doğrulama sağlayan sunucu görüntülerinde, görüntü paylarını oluşturan görsel kriptografik gömme için bir yaklaşım sunulmuştur ve gizli paylaşımların, sunucu görüntülerine gömülerek fark edilmemelerini sağladıkları beyan edilmiştir.

[47]'de dalgacık tekniği kullanılarak, renkli görsel şifrelemenin gerçekleştirilmesinde bir yöntem oluşturulmuştur. Bu çalışmada, dalgacık tekniği, renkli görüntüyü gri görüntüye dönüştürmek için kullanılmıştır.

[48]'de siyah beyaz görsel kriptografi, halftone tekniği ve renk ayrıştırma yönteminde geçmiş çalışmalara dayalı renkli görüntülerin görsel şifrelemesi için iki yöntemi gözden geçirilmiştir.

[49]'da korsanların ilgisini çekmeyecek anlamlı paylar üreten bir renkli görsel kriptografi şeması önerilmiştir. Önerilen şema, anlamlı iki pay oluşturmak için halftone tekniği, kapak görüntüye kodlama ve gizli kodlama tablosunu kullanmaktadır.

[50]'de görsel bilgi pikseli (VIP) senkronizasyon ve hata difüzyon kavramları, yüksek görsel kalite ile anlamlı renk payları üreten bir renkli görsel şifreleme yöntemi elde etmek için kullanılmıştır.

[51]'de ayrık dalgacık dönüşümünde görsel şifrelemeye dayalı bir görüntü filigran şeması önerilmiştir.

[52]'de yeni bir rastgele ızgara tabanlı görsel paylaşım şeması sunulmuştur. Bu şemada herhangi bir piksel genişlemesi olmaksızın dört gizli görüntü iki rastgele ızgaraya şifrelenmekte ve iki rastgele ızgara birleştirilerek gizli görüntü çözülmektedir. Önerilen yöntemin sadece gizli iletişim kapasitesini arttırmakla kalmamakta, aynı zamanda piksel genişlemesi problemini de önlediği beyan edilmektedir. Böylece depolama ve iletişim masrafları önemli ölçüde azalmaktadır.

[53]'de gizli paylaşım ve stenografi kombinasyonunun gizli paylaşım düzenini nasıl daha güvenli hale getirdiği açıklanmaktadır. Şemanın güvenliği, stenografiye dayalı dört farklı sır paylaşım şemasıyla desteklenmiştir.

[54]'de gizli görüntüleri tersine çeviren görsel şifreleme kullanılarak, yeni bir gizli görüntü paylaşım şeması önerilmiştir. Bu makalede çoklu görüntüler için paylaşımların oluşturulması önerilmiştir.

[55]'de basit görsel kriptoloji şemaları ve rastgele ızgara düzenlerinin analizi ve doğruluğu temelinde görsel kriptografi ile rastgele ızgara kriptografisi karşılaştırmalı olarak incelenmiş; çeşitli algoritmalar kullanılarak yeniden yapılandırılmış görüntünün kontrastını ve dönen açılar kullanılarak çoklu görüntü şifrelemenin geliştirildiği beyan edilmiştir.

[56]'da gizli verinin dönüşüm alanına gizlenmesi için yeni bir algoritma tasarlanmıştır ve ayrık dalgacık dönüşümü temel alınmıştır. Bu algoritmada gizli görüntü paylaşımı için Haar filtresi ve dalgacık tabanlı yöntemden oluşan bir teknik sunulmuştur. Ayrık Dalgacık Dönüşümü, sırrı kapak resme gömmek için kullanılmış ve sırrın geri dönüşümü için ters dönüşüm kullanılmıştır. Önerilen tekniğin, sağlamlık, daha iyi görüntü kalitesi ve kimlik doğrulama imkanı sunduğu beyan edilmiştir.

[57]'de görsel kriptografi şeması ve farklı görsel kriptografi yaklaşımlarına genel bir bakış sunulmuştur.

[58]'de Thien ve Lin eşik sır paylaşım şemasının teorik ya da hesaplamalı olmadığı gösterilmiş ve daha önceden yapılmış (k,n) eşik gizli görüntü paylaşım şemalarının metinli görüntü paylaşımı için güvenlik kusurları açıklanarak, bu kusurlar AES şifrelemesi kullanılarak düzeltilmiştir.

[59]'da çeşitli görsel kriptografi şemaları incelenmiş ve piksel genişlemesi, gizli görüntü sayısı, görüntü formatı ve üretilen pay türü temel alınarak performans analizi yapılmıştır.

[60]'da Çift Ağaç Kompleks Dalgacık Dönüşümü (DT-CWT) ve görsel kriptografi kavramlarına dayalı telif hakkı koruması için güçlü bir görüntü filigran şeması sunulmuştur. Önerilen şemada orijinal görüntü değiştirilmeden filigran gömülmüştür.

[61]'de temel görsel şifreleme şeması yapılarına genel bir bakış sağlanmıştır ve bu çalışmaların devam ettirilmesine katkıda bulunulmuştur.

[62]'de görüntü kalitesi ve güvenlik arasındaki dengeyi farklı görsel kriptoloji şemaları karşılaştırılarak açıklanmıştır.

[63]'de (k,n) eşik sır paylaşımı şeması kullanılarak, gizli görüntü n görüntüye paylaştırılmış ve her pay bir kapak resmine gömülmüştür. Gömme tekniğinin tersi uygulanarak sırrın yeniden oluşturulması önerilmiştir.

[64]'de temel görsel şifreleme şemalarının yanında görsel şifreleme şemasından üretilen yeni teknikler hakkında genel bir bakış sağlanmıştır.

[65]'de iki aşamalı bir görsel şifreleme şeması önerilmiştir. Bu şemada birinci aşamada gönderici genel erişim yapısı (GAS) algoritması kullanılarak gizli görüntü dört paya ayrılmaktadır. İkinci aşamada her bir pay, damgalama algoritması kullanılarak, kapak görüntülere gömülmektedir ve bu gömülü görüntüler kullanıcılara dağıtılmaktadır.

[66]'da XOR-tabanlı görsel kriptoloji ile genel erişim yapısı (GAS) ve uyarlanabilir bölge artan XOR tabanlı görsel kriptoloji gibi iki tane XOR tabanlı görsel kriptoloji algoritması önerilmiştir.

[67]'de 2001'den 2014'e kadar görüntü gizlemek için farklı teknikler kullanılan çalışmalar üzerine bir literatür çalışması sunulmuştur.

[68]'de iki sır görüntüsünü piksel genişlemesi olmaksızın, iki anlamlı asetata kodlamak için önceden tanımlanmış bir kod kullanılmıştır ve döngü mekanizmasına göre, iki gizli görüntü aynı anda iki pay içine gömülebilmektedir.

[69]'da görsel kriptografi ve Boolean özelleştirilmiş OR (XOR) operatörü kavramlarına dayalı, renkli görüntüler için yeni bir bilgi gizleme düzeni önerilmiştir.

[70]'de görsel kriptografi ve genetik algoritmayı kullanılarak, veri gizleme ve ağ üzerinden iletim güvenliğini arttırmak için bir sistem önerilmiştir.

[71]'de payların boyutunu azaltmak ve görüntü aktarımını korumak için, Ayrık Dalgacık Dönüşümü (DWT) kullanılan bir sır paylaşım şeması önerilmiştir.

[72]'de görsel gizli payları gizlemek için iki boyutlu ayrık dalgacık dönüşümü kullanılmıştır.

[73]'de temel görsel kriptoloji şeması yapılarının yanı sıra bu konuda yapılmış çok sayıda genişletilmiş yapı hakkında bilgi verilmiştir.

[74]'de Ayrık Haar Dalgacık Dönüşümü kullanılarak Thein ve Lin'in sır paylaşımına dayalı bir görsel sır paylaşım şeması önerilmiştir.

[75]'de piksel genişlemesi olmaksızın, aşamalı olarak sırrın yeniden elde edilebilmesini sağlayan, kullanıcı dostu rastgele ızgaralar yöntemine dayanan bir görsel sır paylaşım şeması önerilmiştir.

[76]'da 2011-2015 yılları arasında görsel kriptografi için farklı teknikler kullanılan mevcut çalışmalarla ilgili bir literatür çalışması sunulmuştur.

[77]'de farklı görsel kriptografi teknikleri, uygulamaları ve avantajları ile ilgili detaylı analizler sunulmuştur.

[78]'de çeşitli görsel şifreleme şemaları incelenmiş ve piksel genişlemesi, gizli görüntü sayısı, görüntü formatı ve üretilen pay türü temellerine dayalı bir performans analizi yapılmıştır.

[79]'da mevcut yer değiştirme algoritmalarından daha iyi bir şifre üretmek için, yenilikçi bir yer değiştirme yöntemi önerilmiştir. Bu yöntemde karakterlerin, sayıların ve özel sembollerin/karakterlerin, renk blokları ile yer değiştirmesi önerilmiştir.

[80]'de görsel kriptografi yöntemleri ve uygulamaları ayrıntılı bir şekilde incelenmektedir.

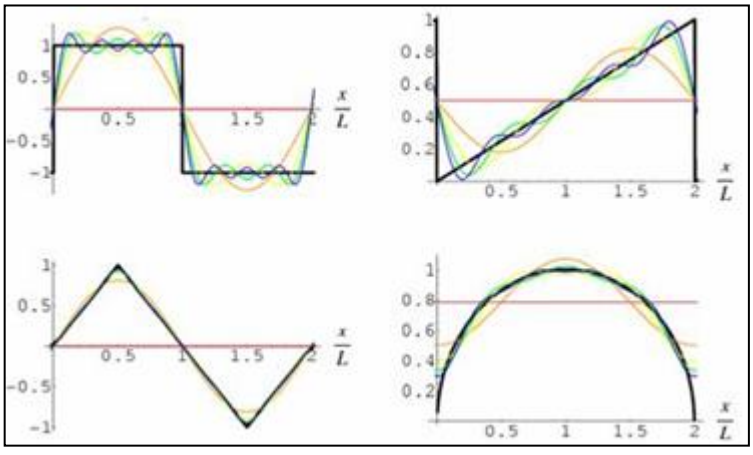
3. TEORİK BİLGİLER

Bu bölümde, tez kapsamında kullanılan dalgacık matematik dönüşümü hakkında bilgi verilecektir. Dalgacık dönüşümü Fourier tabanlı bir dönüşüm olarak inceleneceğinden önce Fourier dönüşümü hakkında bilgi verilecektir. Dalgacık dönüşümü bölümünde ise temel tanımlar, teoremler ve bazı teoremlerin ispatları verilecektir.

Bölümün devamında, uygulamalarda kullanılan sır paylaşım şeması ve algoritması hakkında bilgi verilecektir. Stenografi işleminde yararlanılan LSB (Least Significant Bit) yöntemi hakkında bilgi verilecektir.

3.1. Fourier Dönüşümü

Fransız bilim adamı olan Jean Baptise Joseph Fourier (1768-1830), sinyalleri sinüzoidal bileşenlere ayrıştırmıştır ve Fourier analizi olarak tarihe ismini yazdırmıştır. Fourier, sürekli bir sinyali, düzgün seçilmiş sinüzoidal sinyallerin toplamı biçiminde göstermeyi başarmıştır. Aşağıdaki Şekil 3.1'de dört sinyalin yaklaşık sinüzoidal bileşenleri gösterilmektedir. Bu şekillerde siyah tonda verilen sinyaller, renkli olan harmoniklerin toplamını ifade eder.



Şekil 3.1. Bazı sinyallerin sinüzoidal bileşenleri

Bir fonksiyonun ya da bir diğer deyişle sinyalin analizinde Fourier serileri, sinüs ve kosinüs fonksiyonlarının ortogonal ilişkilerini kullanarak analiz yapar. Periyodik bir fonksiyon, Fourier serileri ile aşağıdaki gibi ifade edilebilir.

$$f(x)=\frac{1}{2}a_0+\sum_{n=1}^{\infty}a_n\cos(nx)+\sum_{n=1}^{\infty}b_n\sin(nx) \tag{3.1}$$

Burada,

$$a_0=\frac{1}{\pi}\int_{-\pi}^{\pi}f(x)d(x) \tag{3.2}$$

$$a_n=\frac{1}{\pi}\int_{-\pi}^{\pi}f(x)\cos(nx)dx \tag{3.3}$$

$$b_n=\frac{1}{\pi}\int_{-\pi}^{\pi}f(x)\sin(nx)dx \tag{3.4}$$

formülleriyle katsayılar bulunur.

$f(t)=f(\frac{2\pi t}{T})$ olduğunu kabul edersek, Fourier serilerinin formülü aşağıdaki gibi olur.

$$f(t)=\frac{1}{2}a_0+\sum_{n=1}^{\infty}a_n\cos(\frac{2\pi nt}{T})+\sum_{n=1}^{\infty}b_n\sin(\frac{2\pi nt}{T}) \tag{3.5}$$

Bu eşitlikte katsayılar,

$$a_n=\frac{2}{T}\int_{-T/2}^{T/2}f(t)\cos\left(\frac{2\pi nt}{T}\right)dt \tag{3.6}$$

$$b_n=\frac{2}{T}\int_{-T/2}^{T/2}f(t)\sin\left(\frac{2\pi nt}{T}\right)dt \tag{3.7}$$

$e^{inx}=\cos(nx)+i\sin(nx)$ Euler bağıntısı kullanılırsa,

$$f(t)=\sum_{-\infty}^{\infty} c_n e^{-i\frac{2\pi nt}{T}} \tag{3.8}$$

$$c_n=\frac{1}{T}\int_{-T/2}^{T/2} f(t)e^{-i\frac{2\pi nt}{T}}\,dt \tag{3.9}$$

$$f(t)=\frac{1}{2\pi}\int_{-\infty}^{\infty} F(\omega)e^{-jwt}\,d\omega \tag{3.10}$$

$$F(\omega)=\int_{-\infty}^{\infty} f(t)e^{j\omega t}\,dt \tag{3.11}$$

olur.

Yukarıdaki formüllerde zaman bölgesinden frekans bölgesine geçiş yapılmıştır, bağıntılardaki t zamanı, ω ifadesi frekansı yani açısal hızı ifade eder. Burada e^{-jwt} karmaşık ve periyodik üstel fonksiyonu ifade etmektedir. F(ω) ise f(t) sinyalinin Fourier Dönüşümü'dür. Sinyalin yeniden elde edilmesi için frekans katsayıları belirlenen üstel fonksiyonlarla katsayıların çarpılıp zaman aralığı boyunca toplanması gerekmektedir. Böylece farklı frekanslardaki periyodik fonksiyonlar toplanarak sinyal yeniden oluşturulmaktadır [81]. Fourier dönüşümleri, periyodik olmayan sürekli sinyallere, periyodik sürekli sinyallere, periyodik olmayan ayrık sinyallere ve periyodik ayrık sinyallere uygulanır. Bu sinyallerin matematiksel karşılığı birbirinden farklı zamana göre değişen fonksiyonlardır.

Şekil 3.2. Fourier dönüşümü

Daha sonra Fourier'in fikirleri genelleştirilerek periyodik olmayan fonksiyonların da bu şekilde ifade edilebileceği benimsenmiştir.

Dr. Gabor tarafından ortaya atılan Gabor Dönüşümü, pencere fonksiyonu olarak tanımlanan bir sabit fonksiyonun zamanda ötelenmesi ile taranan herhangi bir sinyalin Fourier Dönüşümü (FD) alınarak, bölgesel frekans analizinin yapılmasına olanak sağlamıştır. Bu durumda, pencerelenmiş sinyalin Fourier dönüşümü, işaretin frekans bileşenleri yanında zaman bilgisini de içermektedir. Dönüşümde kullanılan pencere fonksiyonu, zaman ve frekans bölgelerinde (domain) sınırlı olan Gaussian fonksiyonudur. 1965'de ortaya atılan, yeni bir algoritmayla Gabor dönüşüm, değişik pencere fonksiyonlarının kullanıldığı Kısa Zamanlı Fourier Dönüşümü (KZFD) olarak genişletilmiştir [81].

3.2. Kısa Zamanlı Fourier Dönüşümü (KZFD)

Daha önce Fourier Dönüşümünün (FD) durağan olmayan sinyaller için elverişli olmadığı ifade edilmişti. Denis Gabor, 1946 yılında pencereleme yöntemini kullanarak, işaretin küçük bir parçasını zaman tanım aralığında ele almış, işareti zaman ve frekansın fonksiyonu olarak iki boyutta ifade etmiş ve haritalamıştır. Bu dönüşüm yönteminde işaretin belirli bir kesiminin durağan olduğu kabul edilebilecek bir pencereden geçirilir ve yerel bir frekans parametresiyle FD işlemi gerçekleştirilir [82]. KZFD ile FD arasında çok az bir fark bulunur. KZFD'de sinyal küçük çerçevelere (segmentler) bölünür ve bu çerçeve anlarında sinyalin durağan olduğu kabul edilir. Durağanlığın geçerli olduğu bu segmentlere pencere denmektedir ve bu çerçeveler sinyalin bir pencere fonksiyonu ile çarpılmasıyla elde edilir. FD'nin yerelleştirilmesi fikrine dayanan bu teknik ilgilenilen yerde uygun bir pencere seçilerek dönüşüm işlemi gerçekleştirilir [83,84].

3.3. Ayrık Fourier Dönüşümü (AFD)

Fonksiyonların teorik olarak tanımlı olduğu hallerde Fourier dönüşümleri rahatlıkla hesaplanabilir. Ancak uygulamada sinyallerin kesin fonksiyonel ifadeleri yoktur ve işlenmeleri için analog sinyallerden örneklenmiş sınırlı sayıda sayısal ayrık dizileri mevcuttur. Bu yüzden daha önce bahsedilen şekilde Fourier dönüşümleri hesaplanamaz.

Ayrıca bütün frekans boyutunun analog olarak gösterimi sonsuz sayıda örneklenmiş işareti gerektirmektedir bu ise uygulamada mümkün değildir. Sayısal işaretlerin Fourier dönüşümünün hesaplanılması için belirli sınırlamalı içindeki yaklaşıklıklarla verilebilir. Bir f[k] ayrık dizisinin N örneği için tanımlanan bu yeni dönüşüm, Ayrık Fourier Dönüşümü (AFD) olarak adlandırılır.

Tersi de alınabilen bu dönüşümün önemli özellikleri vardır. Ayrık Fourier Temelli dönüşümler dizinin periyodik olduğunu kabul ederler [85]. Dolayısıyla bir ayrık zaman sinyali periyodik ise bunun yaklaşık Fourier dönüşümü AFD'dir [86]. Özellikle iki AFD'nin çarpımı bunlara karşı düzen dizilerin ayrık-zaman boyutunda konvolüsyon toplamıdır [87]. Ayrıca sayısal ortamdaki birçok spektral analiz yöntemi AFD'ye dayanmaktadır.

AFD, f(k), k=0,1,…,N-1, gibi bir sonlu diziyi, F(n), n=0,1,…,N-1, gibi diğer bir sonlu diziye eşleyen önemli bir operatördür. Normalize edilmiş örnekleme frekansı 2π olmak üzere [87,88]:

$$F[n]=AFD\{f[k]\}=\sum_{k=0}^{N-1} f[k]e^{-j2\pi kn/N} \tag{3.12}$$

Ters Ayrık Fourier Dönüşümü (TAFD) ise, F[n] 'yi yeniden f[k] dizisine dönüştürür:

$$f[k]=TAFD\{F[n]\}=\frac{1}{N}\sum_{n=0}^{N-1} f[n]e^{-j2\pi kn/N} \tag{3.13}$$

3.4. Hızlı Fourier Dönüşümü (HFD)

Hızlı Fourier Dönüşümü işaret içindeki frekans bileşenlerinin güç yoğunluğunu belirlemek için kullanılır. Temeli, Fourier Dönüşümüne dayanmaktadır. Fourier Dönüşümü en basit anlatımı ile zaman uzayındaki bir ifadenin, frekans uzayına dönüştürülmesidir. Fourier tarafından bulunan bu dönüşüm ile her işaret, farklı genlik, frekans ve faz değerlerine sahip sinüs işaretlerinin bileşimi şeklinde ifade edilebilir. Dolayısıyla her işaret Fourier serisi ile ifade edilebilir ve tersine, Fourier serisi bilinen her işaret tekrar türetilebilir.

Hızlı Fourier Dönüşümü ise, Fourier Dönüşümünün hızlı bir şekilde yapılmasını sağlayan ve ilk olarak 1965 yılında Cooley ve Tukey tarafından ele alınan bir algoritmadır [89].

3.5. Dalgacık Dönüşümü

Bu bölümde dalgacık dönüşümüne ilişkin temel tanım ve teoremler verilecektir [90,91].

Tanım (3.1) $f \in L^1(IR)$ fonksiyonu için Fourier dönüşümü $\hat{f}$ ile gösterilir ve

$$\hat{f}(\gamma)= \int_{-\infty}^{\infty} f(x)\, e^{-2\pi i x\gamma} dx \tag{3.14}$$

şeklinde tanımlanır. $\|\hat{f}(\gamma)\|$ normu f fonksiyonundaki γ frekansının yoğunluğunu ölçer.

Tanım (3.2) Paley-Wiener uzayı (PW), $L^2(IR)$ nin bir alt uzayı olarak

$$PW := \left\{ f \in L^2(IR) : \operatorname{supp} \hat{f} \subseteq \left[-\frac{1}{2}, \frac{1}{2}\right] \right\} \tag{3.15}$$

şeklinde tanımlanır.

Teorem (3.1) (Shannon örnekleme teoremi, 1950)

$$\{\operatorname{sinc}(.-k)\}_{k\in Z} = \{T_k \operatorname{sinc}\}_{k\in Z} \tag{3.16}$$

şeklinde tanımlı fonksiyon dizisi Paley-Wiener uzayı için bir ortonormal taban oluşturur. Burada T_k, $T_k f(x)=f(x-k)$ şeklinde tanımlanan öteleme operatörü ve $\operatorname{sinc}(x)$ fonksiyonu da,

$$\operatorname{sinc}(x) := \begin{cases} \dfrac{\sin(\pi x)}{\pi x}, & x \neq 0 \\ 1, & x = 0 \end{cases} \tag{3.17}$$

şeklinde tanımlıdır. Ayrıca, $\forall f \in PW$ için $f = \sum_{k\in Z} f(k)\, T_k \operatorname{sinc}$ ve f fonksiyonu sürekli ise $\forall x \in IR$ için,

$$f(x)=\sum_{k\in Z} f(k)\, T_k \mathrm{sinc}(x)=\sum_{k\in Z} f(k)\, \mathrm{sinc}(x-k) \tag{3.18}$$

sağlanır.

Tanım (3.3) $f, g \in L^1(IR)$ olsun. $f * g$ konvolüsyonu aşağıdaki şekilde tanımlanan bir fonksiyondur;

$$(f * g)(y) := \int_{-\infty}^{\infty} f(y-x)g(x)dx\,. \tag{3.19}$$

Yardımcı Teorem (3.1) $(f * g)(y)$ iyi tanımlıdır ve $f * g \in L^1(IR)$'dir.

Teorem (3.2) $f, g \in L^1(IR)$ olsun. Bu durumda,

$$\widehat{f * g}\,(\gamma)=\hat{f}(\gamma)\hat{g}(\gamma) \tag{3.20}$$

dir.

Bu kısımda hedef $L^2(IR)$ için ortonormal bir taban elde etmektir.

Tanım (3.4) $D:L^2(IR)\to L^2(IR)$ ölçekleme operatörü,

$$(Df)(x)=2^{\frac{1}{2}} f(2x) \tag{3.21}$$

şeklinde tanımlanır. Bu durumu $j\in Z$ için genelleştirirsek,

$$\left(D^j f\right)(x)=2^{\frac{j}{2}} f\left(2^j x\right) \tag{3.22}$$

elde edilir. $\Psi\in L^2(IR)$ fonksiyonu için

$$\Psi_{j,k}(x) := \left(D^j T_k \Psi\right)(x)=2^{\frac{j}{2}} T_k \Psi\left(2^j x\right)=2^{\frac{j}{2}} \Psi\left(2^j x-k\right)\,,\ j,k\in Z \tag{3.23}$$

olsun.

Tanım (3.5) $\{\Psi_{j,k}\}_{j,k\in Z}=\{D^jT_k\Psi\}_{j,k\in Z}$ fonksiyonlar ailesi $L^2(IR)$ için bir ortonormal taban oluşturuyorsa Ψ fonksiyonuna bir dalgacık fonksiyonudur denir. Ψ bir dalgacık ise, $\forall f\in L^2(IR)$ için,

$$f=\sum_{j\in Z}\sum_{k\in Z}\langle f,\Psi_{j,k}\rangle\Psi_{j,k}=\sum_{j,k\in Z}\langle f,D^jT_k\Psi\rangle D^jT_k\Psi \tag{3.24}$$

sağlanır. Bu durum sadece sınırlı sayıda fonksiyonlar için geçerlidir.

Örnek (3.1) Haar dalgacığı (1910),

$$\psi(x)=\begin{cases}1 & 0\le x<\frac{1}{2}\\ -1 & \frac{1}{2}\le x<1\\ 0 & \text{Diğer Durumlarda}\end{cases} \tag{3.25}$$

$$=\chi_{\left[0,\frac{1}{2}\right[}(x)-\chi_{\left[\frac{1}{2},1\right[}(x)$$

şeklinde tanımlanan fonksiyon Haar dalgacık fonksiyonu olarak adlandırılır. Dalgacık teorisinin en önemli dayanağı dalgacık dönüşümü ile ilgili yapılan uygulamalarda önemli bir yere sahip olan çoklu çözülme analizidir.

Tanım (3.6) Bir çoklu çözülme analizi (multiresolution) $L^2(IR)$ nin kapalı alt uzaylarının bir $\{v_j\}_{j\in Z}$ dizisi ve $\varphi\in L^2(IR)$ fonksiyonu ile aşağıdaki özellikleri sağlayacak şekilde oluşturulur [91].

(i) $\ldots V_{-2}\subset V_{-1}\subset V_0\subset V_1\subset V_2\ldots$

(ii) $\overline{\cup_{j\in Z}V_j}=L^2(IR)$ ve $\overline{\cap_{j\in Z}V_j}=\{0\}$

(iii) $V_{j+1}=DV_j=\{Df : f\in V_j\}$

(iv) $\forall k\in Z$ için $f\in V_0\Rightarrow T_kf\in V_0$

(v) $\{T_k\varphi\}_{k\in Z}$ ailesi V_0 için bir ortonormal tabandır.

Yardımcı Teorem (3.2) Bir V_j uzayı için

(i) $V_j=D^jV_0$

(ii) $V_j=\overline{\text{span}}\{D^jT_k\varphi\}_{k\in Z}$

sağlanır.

İspat. $j>0$ için,

$$V_j=DV_{j-1}=D^2V_{j-2}=\ldots=D^jV_0 \tag{3.26}$$

elde edilir. $V_0=\overline{\text{span}}\{T_k\varphi\}_{k\in Z}$ özelliği kullanılırsa,

$$\begin{aligned} V_j&=D^jV_0 \\ &=D^j(\overline{\text{span}}\,\{T_k\varphi\}_{k\in Z}) \\ &=\left(\overline{\text{span}}\,\{D^jT_k\varphi\}_{k\in Z}\right) \end{aligned} \tag{3.27}$$

elde edilir. Yardımcı Teorem (3.2)'ye göre V_j uzaylarını φ fonksiyonu belirlemektedir.

Yardımcı Teorem (3.3) Çoklu çözülme analizini üreten φ fonksiyonu ele alınsın. Bu durumda,

$$\hat{\varphi}(2\gamma)=H_0(\gamma)\hat{\varphi}(\gamma) \tag{3.28}$$

olacak şekilde 1-periodik olan $H_0\in L^2(0,1)$ fonksiyonu vardır.

İspat. Tanım (3.6)'in sırasıyla (v), (i) ve (iii) özellikleri uygulanırsa,

$$\varphi\in V_0\subset V_1=DV_0 \tag{3.29}$$

dir. Buradan,

$$D^{-1}\varphi\in V_0 \tag{3.30}$$

ve buradan da,

$$\frac{1}{\sqrt{2}}D^{-1}\varphi\in V_0 \tag{3.31}$$

elde edilir. Tanım 3.6'nın (v). özelliğinden, $\{T_k\varphi\}_{k\in Z}$ ailesi V_0 için bir ortonormal tabandır. Buradan $\{T_{-k}\varphi\}_{k\in Z}$ ailesi de V_0 için bir ortonormal tabandır. $b\in IR$ için

modülasyon operatorü $E_b:L^2(IR)\longrightarrow L^2(IR)$, $(E_bf)(x):=e^{2\pi ibx}f(x)$ şeklinde tanımlıdır.

$\mathcal{F}$ ile Fourier dönüşümü gösterilsin. Buradan,

$$\frac{1}{\sqrt{2}}D^{-1}\varphi=\sum_{k\in Z}c_kT_k\varphi \tag{3.32}$$

olacak şekilde $\{c_k\}_{k\in Z}\in l^2(Z)$ katsayıları mevcuttur. Böylece,

$$\frac{1}{\sqrt{2}}\mathcal{F}D^{-1}\varphi=\mathcal{F}\sum_{k\in Z}c_kT_{-k}\varphi=\sum_{k\in Z}c_k\mathcal{F}T_{-k}\varphi \tag{3.33}$$

ve

$$\frac{1}{\sqrt{2}}\mathcal{F}D^{-1}\varphi=\mathcal{F}\sum_{k\in Z}c_kT_{-k}\varphi=\sum_{k\in Z}c_k\mathcal{F}T_{-k}\varphi=\sum_{k\in Z}c_kE_k\mathcal{F}\varphi \tag{3.34}$$

elde edilir. $\mathcal{F}D^{-1}=D\mathcal{F}$ özelliği uygulanırsa,

$$\frac{1}{\sqrt{2}}D\mathcal{F}\varphi=\sum_{k\in Z}c_kE_k\mathcal{F}\varphi \tag{3.35}$$

ya da

$$\frac{1}{\sqrt{2}}\sqrt{2}\widehat{\varphi}(2\gamma)=\sum c_kE_k(\gamma)\widehat{\varphi}(\gamma) \tag{3.36}$$

elde edilir. Buradan,

$$\widehat{\varphi}(2\gamma)=\sum c_ke^{2\pi ik\gamma}\,\widehat{\varphi}(\gamma) \tag{3.37}$$

elde edilir. $H_0(\gamma):=\sum c_ke^{2\pi ik\gamma}$ alınırsa, bu durumda,

$$\widehat{\varphi}(2\gamma)=H_0(\gamma)\widehat{\varphi}(\gamma) \tag{3.38}$$

elde edilir. H_0 1-peryodik, ve $H_0\in L^2(0,1)$'dir.

Teorem (3.3) $H_0 \in L^2(0,1)$ olmak üzere $H_1(\gamma) := \overline{H_0\left(\gamma+\frac{1}{2}\right)}\, e^{-2\pi i\gamma}$ eşitliği sağlanır.

Teorem (3.4) $\hat{\psi}(2\gamma)=H_1(\gamma)\hat{\varphi}(\gamma)$ ile ψ fonksiyonu tanımlansın. Bu durumda ψ bir dalgacıktır. Yani $\{D^j T_k \psi\}_{j,k\in Z}$ ailesi $L^2(IR)$ için bir ortonormal taban oluşturur.

Teorem (3.3)'de tanımlanan $H_1(\gamma)$ fonksiyonu aşağıdaki gibi incelensin;

$$H_o(\gamma)=\sum c_k E_k(\gamma)=\sum c_k e^{2\pi ik\gamma} \tag{3.39}$$

eşitliği kullanılırsa,

$$\begin{aligned} H_1(\gamma) &= \overline{H_0\left(\gamma+\frac{1}{2}\right)}\, e^{-2\pi i\gamma} \\ &= \overline{\sum c_k e^{2\pi ik\left(\gamma+\frac{1}{2}\right)}}\, e^{-2\pi i\gamma} \\ &= \sum \overline{c_k}\, \overline{e^{\pi ik} e^{2\pi ik\gamma}} e^{-2\pi i\gamma} \\ &= \sum c_k (-1)^k e^{-2\pi ik\gamma} e^{-2\pi i\gamma} \\ &= \sum d_k e^{2\pi ik\gamma} \end{aligned} \tag{3.40}$$

elde edilir.

Yardımcı Teorem (3.4) $H_1(\gamma)=\sum d_k e^{2\pi ik\gamma}$ için ψ dalgacık fonksiyonu aşağıdaki şekilde yazılır;

$$\psi(x)=2\sum_{k\in Z} d_k \varphi(2x+k)=\sqrt{2}\sum_{k\in Z} d_k D T_{-k}\varphi(x)\,. \tag{3.41}$$

Bir çoklu çözülme analizi φ fonksiyonunun uygun bir seçimiyle belirlenir. Bir φ fonksiyonu verildiğinde ψ dalgacık fonksiyonu $(H_0 \longrightarrow H_1 \longrightarrow \psi)$ sıralanışıyla oluşturulabilir.

Yardımcı Teorem (3.5) $\varphi \in L^2(IR)$ fonksiyonunun bir çoklu çözülme analizi oluşturduğunu varsayalım. $\psi \in L^2(IR)$ olsun ve $\{T_k\psi\}_{k\in Z}$ ailesi V_0 için bir ortonormal taban olsun. Bu durumda aşağıdaki koşullar gerçeklenir.

(i) Her $j \in Z$ için $\{D^j T_k \psi\}_{k \in Z}$ fonksiyonları V_j için bir ortonormal taban oluşturur.

(ii) $\{D^j T_k \psi\}_{j,k \in Z}$ fonksiyonları $L^2(IR)$ için bir ortonormal taban oluşturur. Bu durumda ψ fonksiyonu bir dalgacıktır.

(iii) $\{T_k \varphi\}_{k \in Z} \cup \{D^j T_k \psi\}_{j \in N, k \in Z}$ fonksiyonları $L^2(IR)$ için bir ortonormal taban oluşturur. Buradan,

$$f = \sum_{k \in Z} \langle f, T_k \varphi \rangle T_k \varphi + \sum_{j=1}^{\infty} \sum_{k \in Z} \langle f, D^j T_k \psi \rangle D^j T_k \psi \tag{3.42}$$

elde edilir.

Örnek (3.2) Haar dalgacığı

$$\Psi(x) = \begin{cases} 1, & \text{eğer } x \in [0, \frac{1}{2}) \\ -1, & \text{eğer } x \in [\frac{1}{2}, 1) \\ 0, & \text{eğer } x \notin [0,1) \end{cases} \tag{3.43}$$

$f \in L^2(IR)$, $\left[\varphi = \chi_{[0,1]}\right]$ için, (f kompakt sonlu dayanağa sahipse)

$$\begin{aligned} f &= \sum_{k \in Z} \langle f, T_k \varphi \rangle T_k \varphi + \sum_{j=1}^{\infty} \sum_{k \in Z} \langle f, D^j T_k \psi \rangle D^j T_k \psi \\ &= \sum_{k \in Z} \langle f, T_k \varphi \rangle T_k \varphi + \sum_{j=1}^{\infty} \sum_{k \in Z} 2^j \langle f, \psi(2^j x - k) \rangle \psi(2^j x - k) \\ &= \sum_{k \in Z} \langle f, T_k \varphi \rangle T_k \varphi + \sum_{j=1}^{\infty} \sum_{k \in Z} d_{j,k} \psi(2^j x - k) \end{aligned} \tag{3.44}$$

dır. Buradan,

$$d_{j,k} = 2^j \langle f, \psi(2^j x - k) \rangle = 2^j \int_{-\infty}^{\infty} f(x) \psi(2^j x - k) dx \tag{3.45}$$

elde edilir.

$$\psi(2^j x-k)=\begin{cases}1, & \text{eğer } 2^j x-k\in[0,\frac{1}{2})\\ -1, & \text{eğer } 2^j x-k\in[\frac{1}{2},1)\\ 0, & \text{eğer } 2^j x-k\notin[0,1)\end{cases}=\begin{cases}1, & \text{eğer } x\in 2^{-j}[k,k+\frac{1}{2})\\ -1, & \text{eğer } x\in 2^{-j}[k+\frac{1}{2},k+1)\\ 0, & \text{eğer } x\notin 2^{-j}[k,k+1)\end{cases} \tag{3.46}$$

Bu yüzden,

$$d_{j,k}=2^j\left(\int_{2^{-j}k}^{2^{-j}\left(k+\frac{1}{2}\right)} f(x)dx-\int_{2^{-j}\left(k+\frac{1}{2}\right)}^{2^{-j}(k+1)} f(x)dx\right) \tag{3.47}$$

olarak bulunur.

Tanım (3.7) Bir $\psi\in L^2(IR)$ fonksiyonuna $(-\infty,\infty)$ kümesi üzerinde sıfır ortalamaya sahipse, ψ 'ye bir dalgacıktır denir; yani,

$$\int_{-\infty}^{\infty}\psi(t)dt=0 \tag{3.48}$$

Uyarı (3.1) $\hat{\psi}(\omega)$, ψ'nin Fourier dönüşümü olmak üzere, $\psi\in L_2(IR)\cap L_1(IR)$ fonksiyonu için,

$$c_\psi=2\pi\int_R\frac{|\hat{\psi}(\omega)|^2}{|\omega|}d\omega<\infty \tag{3.49}$$

sağlanıyorsa, Denklem 3.49 koşuluna dalgacık kabul edilebilirlik koşulu denir.

Aşağıdaki yardımcı teorem yeni dalgacık oluşturmaya olanak sağlamaktadır:

Yardımcı Teorem (3.6) $\varphi^{(n)}\in L^2(IR)$ olmak üzere φ sıfırdan farklı ($n\geq 1$) n-yinci mertebeden türevlenebilir bir fonksiyon olsun. Bu durumda,

$$\psi(x)=\varphi^{(n)}(x) \tag{3.50}$$

bir dalgacıktır.

Örnek (3.3) (Meksika Şapkası Dalgacığı).

$$\psi(x)=(1-x^2)e^{-x^2/2} \tag{3.51}$$

denklemiyle tanımlanan fonksiyon Meksika Şapkası Dalgacığı olarak bilinir. $\psi(x)$, Yardımcı Teorem (3.6)'daki Denklem (3.50)'yi sağlar, yani,

$$\psi(x)= - \frac{d^2}{dx^2}\left(e^{-x^2/2}\right)=(1-x^2)e^{-x^2/2} \tag{3.52}$$

olur. Yardımcı Teorem (3.6)'dan $\psi(x)$ bir dalgacıktır.

Teorem (3.5) ψ bir dalgacık ve φ sınırlı integrallenebilir bir fonksiyon olsun. Bu durumda $\psi * \varphi$ konvolüsyon fonksiyonu bir dalgacıktır.

İspat.

$$\int_{-\infty}^{\infty}|\psi * \varphi\ (x)|^2dx=\int_{-\infty}^{\infty}\left|\int_{-\infty}^{\infty}\psi(x-t)\varphi(t)dt\right|^2 dx$$

$$\leq\int_{-\infty}^{\infty}\left(\int_{-\infty}^{\infty}|\psi(x-t)||\varphi(t)|dt\right)^2 dx$$

$$=\int_{-\infty}^{\infty}\left(\int_{-\infty}^{\infty}|\psi(x-t)||\varphi(t)|^{1/2}|\varphi(t)|^{1/2}\,dt\right)^2 dx \tag{3.53}$$

$$\leq\int_{-\infty}^{\infty}\left(\int_{-\infty}^{\infty}|\psi(x-t)|^2|\varphi(t)|dt\int_{-\infty}^{\infty}|\varphi(t)|\,dt\right)dx$$

$$\leq\int_{-\infty}^{\infty}|\varphi(t)|dt\int_{-\infty}^{\infty}\int_{-\infty}^{\infty}|\psi(x-t)|^2|\varphi(t)|\,dxdt$$

$$\leq\left(\int_{-\infty}^{\infty}|\varphi(t)|\,dt\right)^2\int_{-\infty}^{\infty}|\psi(x)|^2dx<\infty$$

olduğundan $\psi * \varphi \in L^2$ (IR) elde edilir.

Öte yandan, Teorem (3.2)'den,

$$\int_{-\infty}^{\infty} \frac{\left|\widehat{\psi * \varphi}\ (\omega)\right|^2}{|\omega|} = \int_{-\infty}^{\infty} \frac{|\hat{\psi}(\omega)\hat{\varphi}(\omega)|^2}{|\omega|} d\omega$$

$$= \int_{-\infty}^{\infty} \frac{|\hat{\psi}(\omega)|^2}{|\omega|} |\hat{\varphi}(\omega)|^2 d\omega \tag{3.54}$$

$$\leq \int_{-\infty}^{\infty} \left(\frac{|\hat{\psi}(\omega)|^2}{|\omega|}\ d\omega \right) \sup|\hat{\varphi}(\omega)|^2 < \infty.$$

Buradan $\psi * \varphi$ bir dalgacıktır.

Tanım (3.8) ψ dalgacığına dayalı bir $f \in L^2(IR)$ fonksiyonunun T_ψ Sürekli Dalgacık Dönüşümü, aşağıdaki şekilde tanımlanır. Burada, $a \in R\backslash\{0\}$, $b \in IR$ ve $\overline{\psi}$ kompleks eşleniği ifade eder;

$$T_\psi f(a,t) = |a|^{-1/2} \int_R f(x) \overline{\psi} \left(\frac{x-b}{a} \right) dx. \tag{3.55}$$

Uyarı (3.2)

(i) $\psi_{a,t}(x)$ fonksiyonu,

$$\psi_{a,t}(x) = |a|^{-1/2} \psi \left(\frac{x-b}{a} \right), a>0, t \in IR \tag{3.56}$$

ile verilen fonksiyonların bir ailesi olarak ele alınırsa, bu durumda, $T_\psi f(a,t)$ ifadesi

$$T_\psi f(a,t) = \langle f, \psi_{a,t} \rangle \tag{3.57}$$

şeklinde f ile $\psi_{a,t}$ nin iç çarpımı olarak yazılabilir. Burada ψ fonksiyonu ana dalgacık fonksiyonu olarak adlandırılır.

(ii) Dalgacık dönüşümü, f ile $\psi_{a,t}(x)$ nin iç çarpımı olarak ifade edildiğinden, lineerdir. $T_\psi f(a,t)$ asimptotik olarak f nin tekilliklerinin yerini işaret eder.

Örnek (3.4) IR üzerinde ψ dalgacık fonksiyonu verilsin. δ, IR üzerinde Dirac delta fonksiyonu olsun. Bu durumda, δ Dirac delta fonksiyonunun sürekli dalgacık dönüşümü aşağıdaki gibidir;

$$T_\psi \delta(a,t) = \langle \delta, \psi_{a,t} \rangle = \psi_{a,t}(0). \tag{3.58}$$

Örnek (3.5) IR üzerinde ψ dalgacık fonksiyonu verilsin. Denklem (3.59) ile tanımlanan Heaviside basamak fonksiyonunun sürekli dalgacık dönüşümü Denklem (3.60)'daki gibidir;

$$h(x)=\begin{cases}1 & , \ x\geq 0\\ 0 & , \ x<0.\end{cases} \tag{3.59}$$

$$T_{\psi}h(a,t)=\langle \hat{h},\hat{\psi}_{a,t}\rangle=\sqrt{a}\int_{R}\frac{1}{2\pi i\xi}\overline{\hat{\psi}(a\xi)}e^{-2\pi i\xi t}d\xi=\sqrt{a}\int_{R}\hat{\gamma}(\eta)e^{-2\pi i\eta\frac{t}{a}}d\eta \tag{3.60}$$

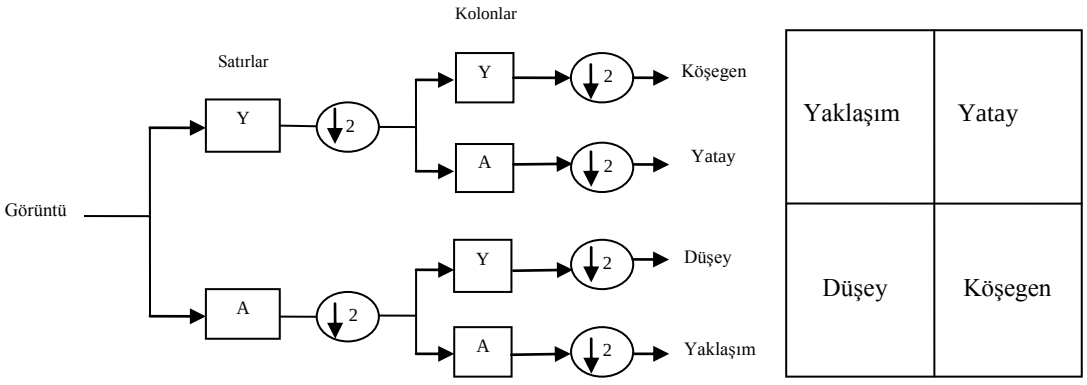
Burada,

$$\hat{\gamma}(\eta)=\frac{1}{2\pi i\eta}\overline{\hat{\psi}(\eta)} \tag{3.61}$$

şeklindedir.

3.6. İki Boyutlu (2B) Dalgacık Dönüşümleri

İki boyutlu (2B) dalgacık dönüşümleri, bir boyutlu (1B) dalgacık dönüşümlerinde uygulanan yöntemin satır ve sütun olarak genişletilmiş bir uygulamasıdır. Şekil 3.3'de bir imgenin bir defa dalgacık dönüşümüne tabi tutulması görülmektedir.



Şekil 3.3. İki boyutlu dalgacık dönüşümü

Satırlar alçak (L) ve yüksek (H) geçirgen filtrelerden geçirildikten sonra örnek azaltımı yapılır. Daha sonra, bu filtre sonuçları aynı filtre katsayıları kullanılarak tekrar alçak ve yüksek geçirgen filtrelerden geçirilir ve tekrar örnek azaltımı yapılır. Sonuçta, geçirildiği filtre tipine göre yaklaşım (AA), düşey (AY), yatay (YA) ve köşegen (YY) dalgacık dönüşümü sonucu katsayılar elde edilir. Sonuçta elde edilen

katsayılar iki boyutlu olup imge olarak sunulabilir. Bu ayrıştırma yöntemi, örnek azaltılması sonucu ayrıştırılamayacak tek bir imge elemanı kalıncaya kadar her bir alt imgeye uygulanabilir [92].

Farklı ölçeklerdeki ve frekanslardaki görüntüler çok çeşitli karakteristiklere sahiptirler. Bu nedenle dalgacık dönüşümü çok çözünürlüklü yapısı nedeniyle doku analizi için oldukça uygundur. Dalgacık dönüşümünün görüntü işlemedeki kullanımında izlenen temel yaklaşım; görüntünün iki boyutlu dalgacık dönüşümü alınması, dönüşümün filtrelenmesi ve ters dönüşümün hesaplanması şeklindedir. Görüntünün 2-boyutlu dalgacık dönüşümü frekans spektrumunu yaklaşım ve yatay, dikey ve diyagonal detay alt görüntülerine böler. Her bir alt görüntü, orijinal görüntü ile ilgili farklı özellikleri ortaya çıkaracağından, bu alt görüntülerin kendileri ya da alt görüntülerin filtrelenmiş versiyonları görüntü bölütlemede görüntüyle ilgili çok çeşitli özellikleri ortaya çıkartacaktır [93].

3.7. Shamir'in Sır Paylaşım Şeması

Shamir, sonlu cisim üzerinde polinom tabanlı bir sır paylaşım yöntemi önermiştir. Shamir sır paylaşım algoritmasında gizli veriyi S ile gösterelim. (k,n) eşik şeması adındaki bu yöntem için kullanıcı (k-1). dereceden bir polinom oluşturur. Gizli veri polinomun sabit terimidir ve polinomun katsayıları kullanıcı tarafından rastgele belirlenir. xy- düzleminde kullanıcı numarası olarak atanan x değerine karşılık gelen y değerleri gönderilecek olan pay değerlerini oluşturur. Yeniden yapılandırma aşamasında herhangi k tane katılımcıdan elde edilen (x,y) çiftleri Lagrange interpolasyon tekniği kullanılarak gizi veri yeniden elde edilir [15].

Önce pay değerlerini oluşturacak,

$$f(x)=\left(S+ax+bx^2+cx^3+\ldots+zx^{k-1}\right) \bmod p \qquad (3.62)$$

fonksiyonu belirlenir. Burada a,b,c,...,z katsayıları, [0,p-1] tanım aralığından rastgele seçilir. Shamir'in yönteminde p sayısı bir asal sayıdır ve sır olarak dağıtılacak olan verinin aralığını belirler. [0,255] aralığındaki en büyük asal sayı 251 olduğu için görüntülerde p, 251 olarak seçilir. Diğer verilerin saklanmasında p'nin alacağı değer

isteğe bağlıdır. Devamında n tane f(x) değerleri hesaplanır ve k tanesi seçilip, Lagrange interpolasyonu kullanılarak gizli veri elde edilir [94].

3.8. Lagrange İnterpoasyonu

(n+1) noktadaki $(x_i, y_i), i = \overline{0,n}$ değerleri bilinen f(x) fonksiyonuna, bu noktalardaki değerleri eşit olan L(x) polinomu uydurulur. L(x) polinomu ise,

$$l_i(x)=\prod_{i=0,\, i\neq j}^{k} \frac{x-x_i}{x_j-x_i}=\frac{x-x_0}{x_j-x_0}\cdots\frac{x-x_{j-1}}{x_j-x_{j-1}}\cdot\frac{x-x_{j+1}}{x_j-x_{j+1}}\cdots\frac{x-x_k}{x_j-x_k} \tag{3.63}$$

olmak üzere,

$$L(x)=\sum_{j=0}^{k} y_j l_j(x) \tag{3.64}$$

formülü ile belirlenir.

S=f(0)=L(0) olduğundan,

$$L(0)=\sum_{j=0}^{k-1} f(x_j)\prod_{\substack{m=0\\ m\neq j}}^{k-1}\frac{x_m}{x_m-x_j} \tag{3.65}$$

yaklaşımı L(0) bulmak için kullanılabilir [94].

3.9. Shamir Yöntemi ile Gizli Görüntü Paylaşımı ve Yeniden Yapılandırma Algoritması

Gizli görüntüdeki tüm piksellerde, 251'e göre mod işlemi yapılır. Böylece piksel değerleri [0,250] aralığına çekilmiş olur. Birinci pikselin değerine Shamir sır paylaşım yöntemi uygulanır ve n tane paya gönderilecek olan değerler hesaplanır. Bu işlem bütün piksel değerleri paylaştırılana kadar tekrarlanır.

Yeniden yapılandırma algoritmasında ise tüm paylardaki 1. piksel değerleri toplanır ve 251'e göre modu alınır. Bu gizli görüntüdeki 1. pikselin değerini verir. Bu işlem tüm piksel değerleri için tekrar edilir.

Teorik olarak Shamir'in sır paylaşım algoritması bu şekildedir [94].

3.10. Floyd Steinberg Halftone Algoritması

Floyd-Steinberg Titreşim Algoritması, Robert W. Floyd ve Louis Steinberg tarafından 1976 yılında ilk kez yayınlanan ve hata dağılımına dayanan bir görüntü titreşim algoritmasıdır. Genellikle görüntü işleme yazılımları tarafından kullanılır. Algoritma, hata difüzyonunu kullanarak titreşim sağlar. Yani bir pikselin artık niceleme hatasını komşu piksellere ekler [95].

Hata dağılımı tekniğini tanımlamak gerekirse, öncelikle görüntünün her bir noktası için en yakın renk bulunur. Bulunan değer ile görüntüdeki değer arasındaki fark hesaplanır. Sonra bu hata değerleri bölünüp, üzerinde işlem yapılmayan komşu piksellere dağıtılır. Komşu piksele geçildiğinde ise, daha önce komşu piksellerden gelen hata değerlerini ekleyip bu işlem tekrarlanır.

Hata dağıtımının ve görüntü taramanın birçok yolunun bulunur. Görüntüyü taramanın iki temel şekli vardır. Biri normal sağdan sola, üstten alta doğru tarama diğeri ise alternatif olarak soldan sağa, ardından sağdan sola doğru tarama şeklidir. Hata bölüştürmenin farklı yolları, desenler ya da filtreler olarak ifade edilebilir.

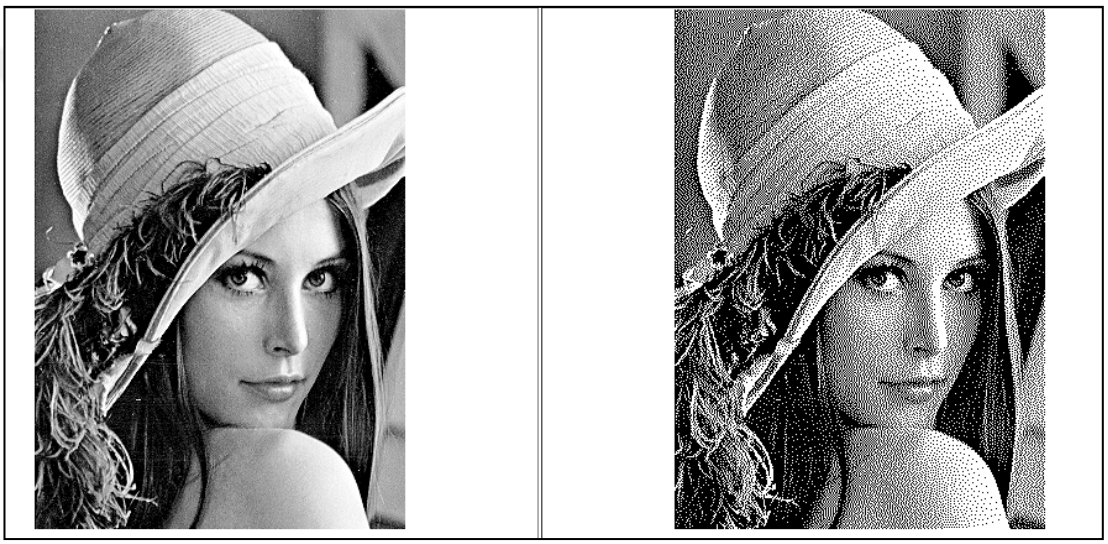
$$\begin{matrix} & x & 7 \\ 3 & 5 & 1 \end{matrix} \tag{3.66}$$

Matris (3.66)'da birinci satır Floyd Steinberg katsayılarıdır. İkinci satır hata difüzyon filtresi katsayılarıdır.

$$\begin{bmatrix} & & x & \frac{7}{16} & \cdots \\ \cdots & \frac{3}{16} & \frac{5}{16} & \frac{1}{16} & \cdots \end{bmatrix} \tag{3.67}$$

(3.67) matrisinde boş pikseller daha önce taranmış pikselleri ve x ile gösterilen piksel şuan da taranan piksel olsun. Ağırlık olarak adlandırılan sayılar, o pozisyondaki pikseller için hata dağılım oranını göstermektedir. Algoritma görüntüyü soldan sağa, yukarıdan aşağıya doğru tarar ve piksel değerlerini tek tek nicelleştirir. Burada ağırlık 16'ya katlandığından bölüm 16'dır ve sağdaki piksel hatanın 7/16'sını, alttaki

piksel hatanın 5/16'sını ve çaprazda bulunan pikseller ise hatanın 3/16'sını ve 1/16'sını alır. Niceleme hatası her zaman komşu piksellere aktarılır ve nicellenmiş pikseller bu aktarımdan etkilenmez. Dolayısıyla bir dizi piksel aşağı yuvarlanmışsa bir sonraki pikselde yuvarlak olur ve böylece ortalama olarak niceleme hatası sıfıra yakın olur. Difüzyon katsayılarının özelliği, eğer orijinal piksel değerleri, en yakın olan renkler arasında tam olarak yetersiz kalıyorsa, titreşim sonucu bir dama tahtası desenidir. Örneğin %50 gri veri, siyah beyaz bir dama tahtası deseni gibi titreştirilebilir. Optimum titreşim için, niceleme hatalarının hesabı, yuvarlama hatalarının sonucu etkilemesini önlemek için yeterli doğrulukta olmalıdır.



Şekil 3.4. Floyd-Steinberg titreşimi uygulaması

Burada giriş görüntüsünün piksel değerleri, [0,1] aralığında değişen bir formata normalleştirilmiştir ve burada 0, siyah pikseli, 1, beyaz pikseli ifade eder. Floyd-Steinberg Hata Dağılımı Algoritması'nın pseudo kodları aşağıdaki gibidir [32,37,48,96]:

```
her y için yukarıdan aşağıya
    her x için soldan sağa
        eski_piksel:=piksel[x][y]
        yeni_piksel:=bulunan_enyakın_değerdeki_renk(eski_piksel)
        piksel[x][y]:=yeni_piksel
        quant_error:= eski_piksel-yeni_piksel
        piksel[x + 1][y] := piksel[x + 1][y] + quant_error * 7 / 16
        piksel[x - 1][y + 1] := piksel[x - 1][y + 1] + quant_error * 3 / 16
        piksel[x][y + 1] := piksel[x][y + 1] + quant_error * 5 / 16
        piksel[x + 1][y + 1] := piksel[x + 1][y + 1] + quant_error * 1 / 16
```

Şekil 3.5. Floyd-Steinberg halftone algoritması pseudo kodları

3.11. Stenografik LSB (Least Significant Bit)

LSB, dijital mesajlarda stenografik uygulamalar için yeni ve en çok kullanılan tekniktir. Bunun sebebi ise verinin gömüldüğü görsel üzerindeki bozulmaların bilinen tekniklere göre oldukça az olmasıdır. Bu teknikte orijinal görüntünün piksel değerliğinin en az ağırlıklı olan son biti ardışık olarak değiştirilerek gerçekleştirilir.

Dijital formattaki renkli bir veriyi genellikle 24- bit color, 8-bir color ve 8-bit gray scale yöntemlerinden biriyle sunulur. Her pikseli 2^{24} renkten birine sahip olan 24-bit color veride, her bit (256 değer) tarafından verilen, üç rengin (R (red), G (green), B (blue)) farklı miktarı olarak ifade edilir. Her pikseli 2^8 (256) renkten birine sahip olan 8-bit color veride, renkler bir paletten seçilir. 8-bit gray scale (8 bit gri seviye) verilerde ise her piksel 2^8 (256) gri noktanın birine sahiptir.

LSB, resim dosyalarında renkleri temsil eden değerler üzerinde çalışmaktadır. Renk değerinin en düşük anlamlı biti ile gizli verinin bitleri değiştirilir. Bu işlemde

öncelikle orijinal görüntülerin RGB değerlerini çıkarılır ve her bir kanalın en az önemli biti alır. Piksel değerlikleri ikiliye (binary) çevrilerek son bitlerine gömülecek olan verinin ikili kodu yerleştirilir. Resim üzerinde gerçekleşecek bu değişim gözle görünmeyecek kadar azdır. Sonuçta ortaya çıkacak resim dosyasındaki renk değerleri ya olduğu gibi kalır ya bir artar ya da bir azalır. Ancak her üç durumda da söz konusu olan, bu durumun insan gözü tarafından algılanmamasıdır [97,98].

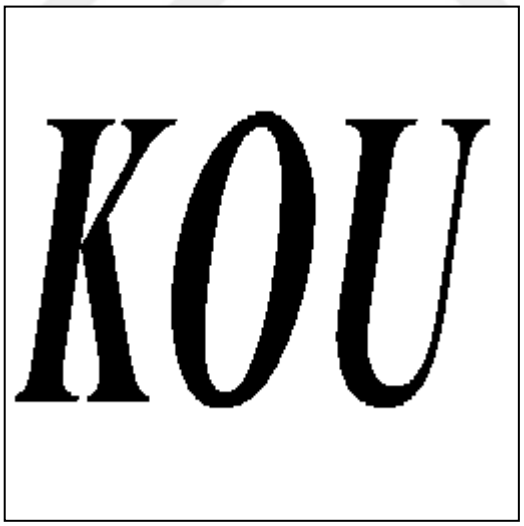
4. MALZEME VE YÖNTEM

Bu kısımda tezde kullanılan malzeme ve yöntemlerden bahsedilecektir.

Uygulamada kullanılan bilgisayar, 64 bit işletim sistemli ve Intel Core i7 2.80 GHz işlemcilidir. Uygulama geliştirilirken kullanılan program 2011 yılında yayımlanan 7.12.0 sürümlü MATLAB (R2011a) paket programıdır.

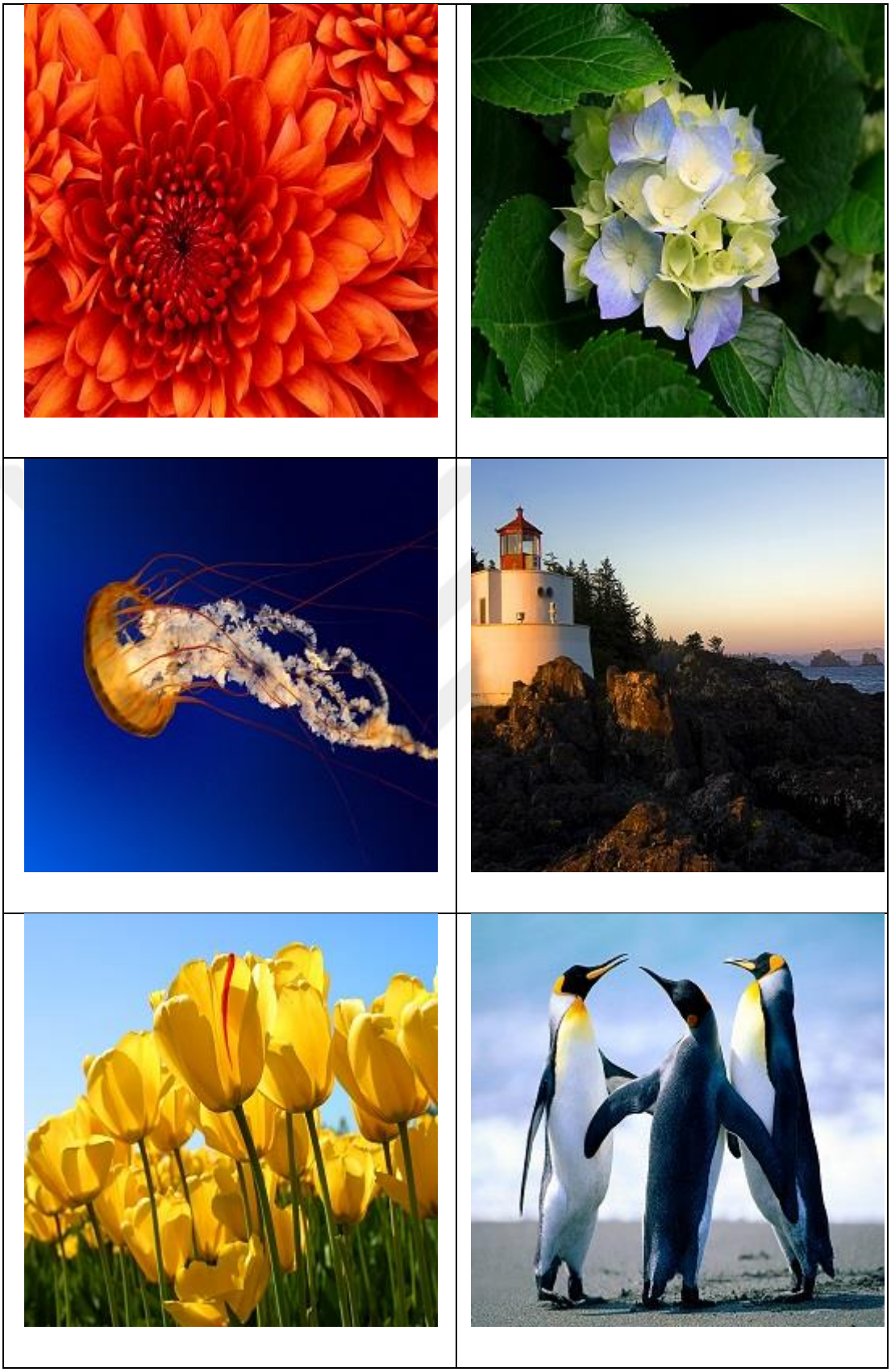
4.1. Kullanılan Görüntüler

Birinci uygulamada kullanılan görüntü Şekil 4.1.'de verilen 256x256 boyutunda, .bmp uzantılı, ikili (binary) bir görüntüdür. İkinci uygulamada kullanılan görüntü Şekil 4.2'de verilen 256x256 boyutunda, 24 bit, .jpg uzantılı, JPEG formatlı bir görüntüdür. Her iki uygulamada da kullanılan kapak (cover) görüntüler, Şekil 4.3.'te verilen 256x256 boyutunda, 24 bit, .jpg uzantılı, rastgele seçilmiş JPEG formatlı görüntülerdir.



Şekil 4.1. Birinci uygulamada kullanılacak olan ikili sır görüntüsü

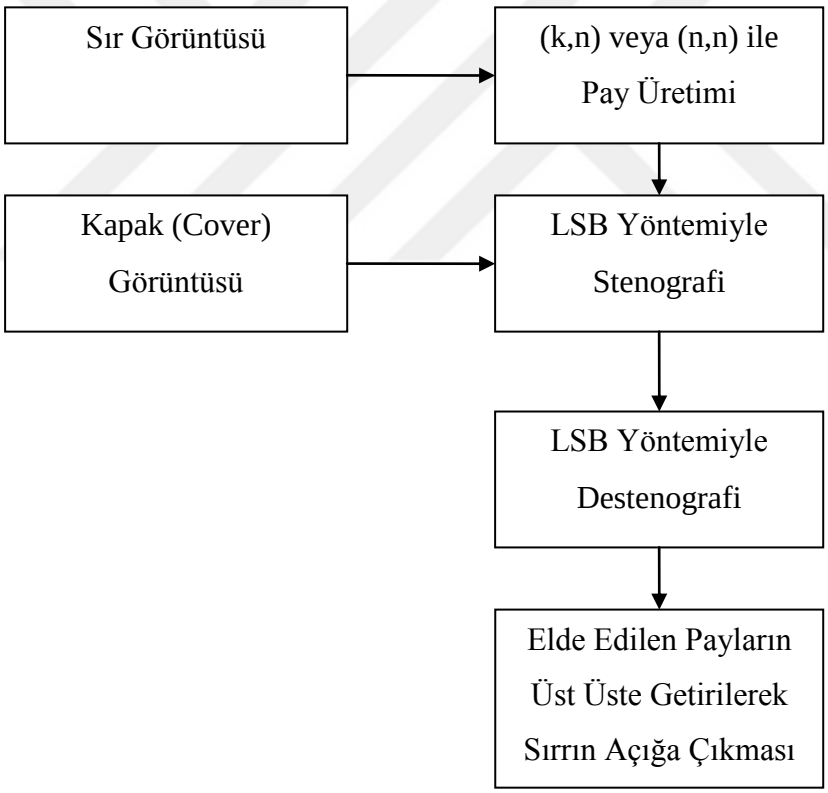
Şekil 4.2. İkinci uygulamada kullanılacak olan renkli sır görüntüsü



Şekil 4.3. Uygulamalarda kullanılan kapak görüntüleri

4.2. Kullanılan Yöntem

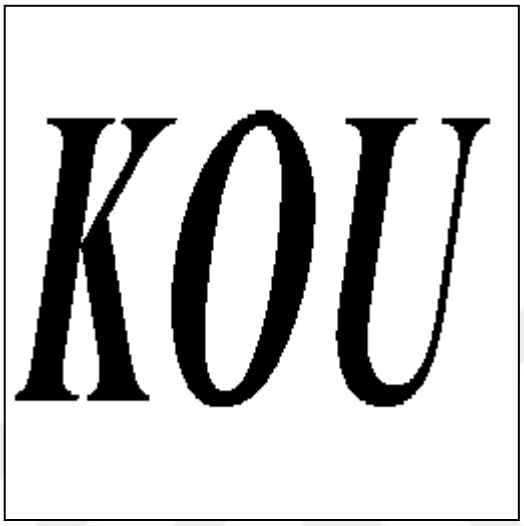
Her iki uygulamada Şekil 4.4.'te verildiği gibi sır paylaşımı, kriptografi ve stenografi kullanılacaktır. Uygulamalarda öncelikle Shamir algoritması esas alınarak paylaştırma işlemi yapılacaktır. Daha sonra görüntüleri gömme işleminde, kapak görüntüler YCbCr katmanlarına ayrılacak ve LSB (Least Significant Bit) yöntemi esas alınarak Ayrık Dalgacık Dönüşümü yardımıyla Y katmanının alt bantlarına paylar gömülecektir. İkili görüntüde sır, anlamsız iki paya ayrılacak ve bu paylar, iki kapak görüntüye gömülecektir. Renkli görüntülerde ise Floyd-Steinberg Algoritması yardımıyla görüntünün kırmızı, yeşil ve mavi katmanları halftone görüntüye dönüştürülecek ve altı paya ayrılarak altı farklı kapak görüntüye gömülecektir.



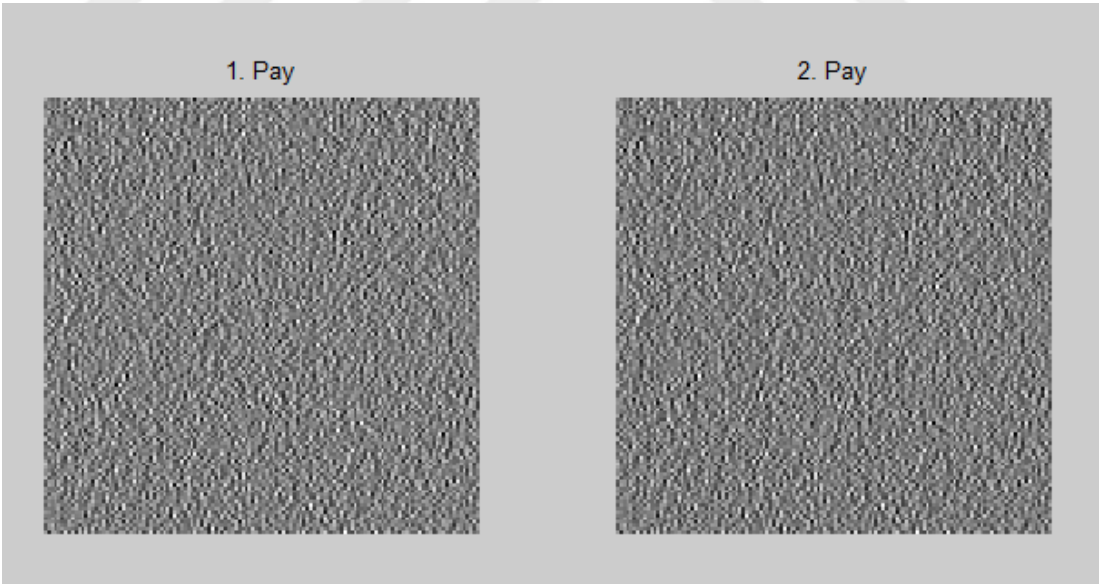
Şekil 4.4. Sır görüntüsünün saklanması ve açığa çıkarılması

4.2.1. İkili (Binary) görüntülerde sır paylaşımı ve stenografi

Kullanılan ikili görüntü, Şekil 4.5.'te verilen 256x256 boyutlu Bit Eşlem Resmi'dir. Bu görüntü öncelikle Shamir algoritması kullanılarak Şekil 4.6.'da verildiği gibi iki paya ayrılacaktır.

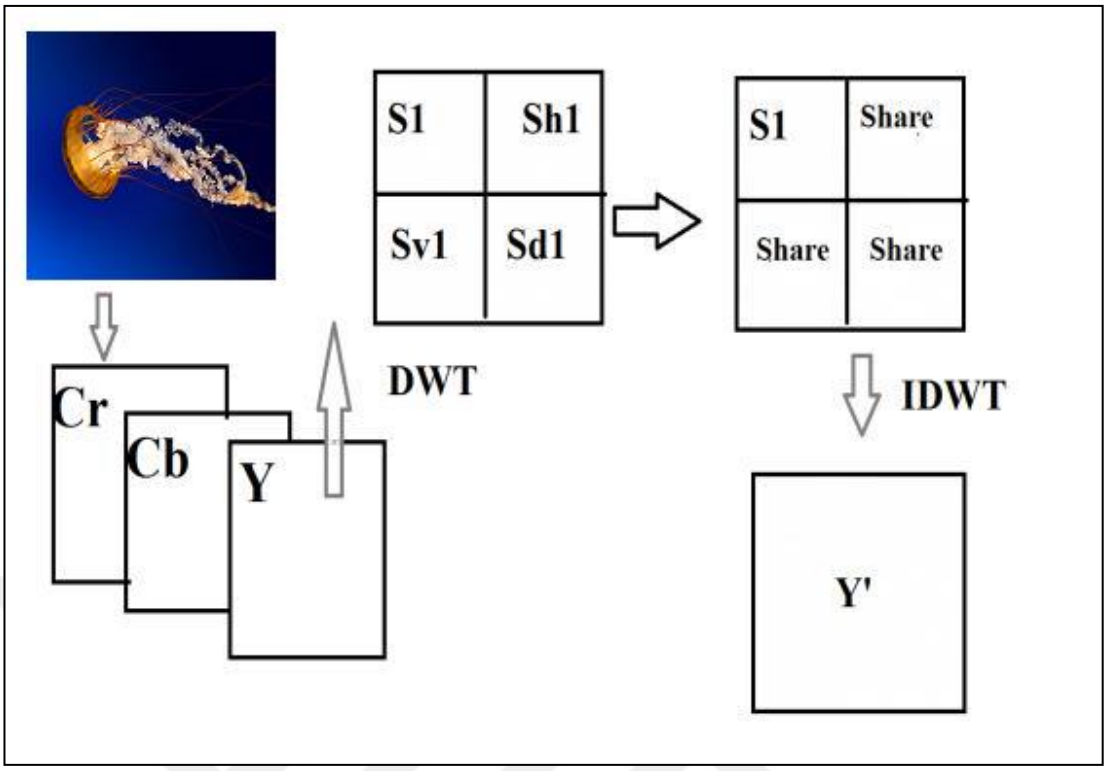


Şekil 4.5. İkili sır görüntüsü

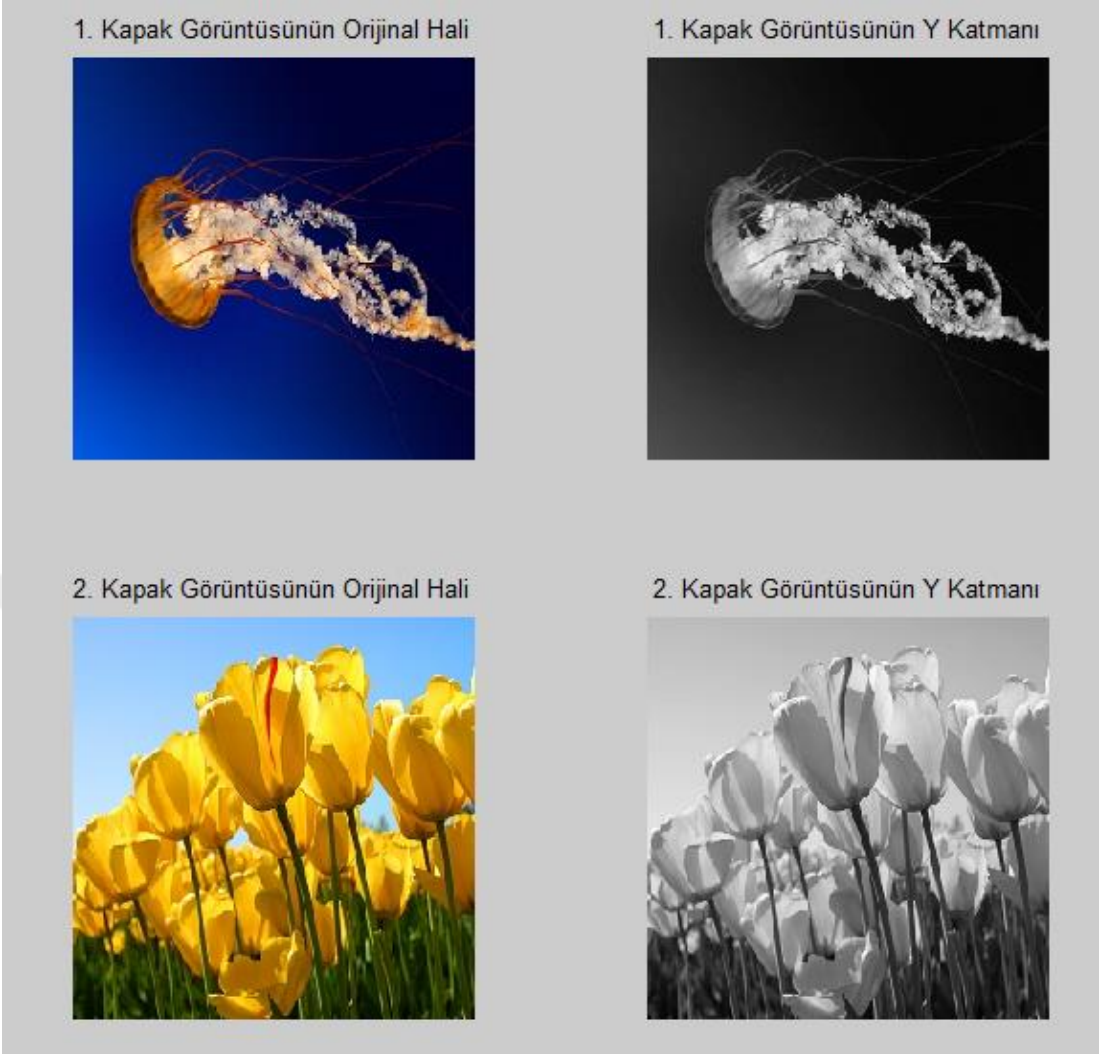


Şekil 4.6. MATLAB 7.12.0 programı kullanılarak elde edilen paylar

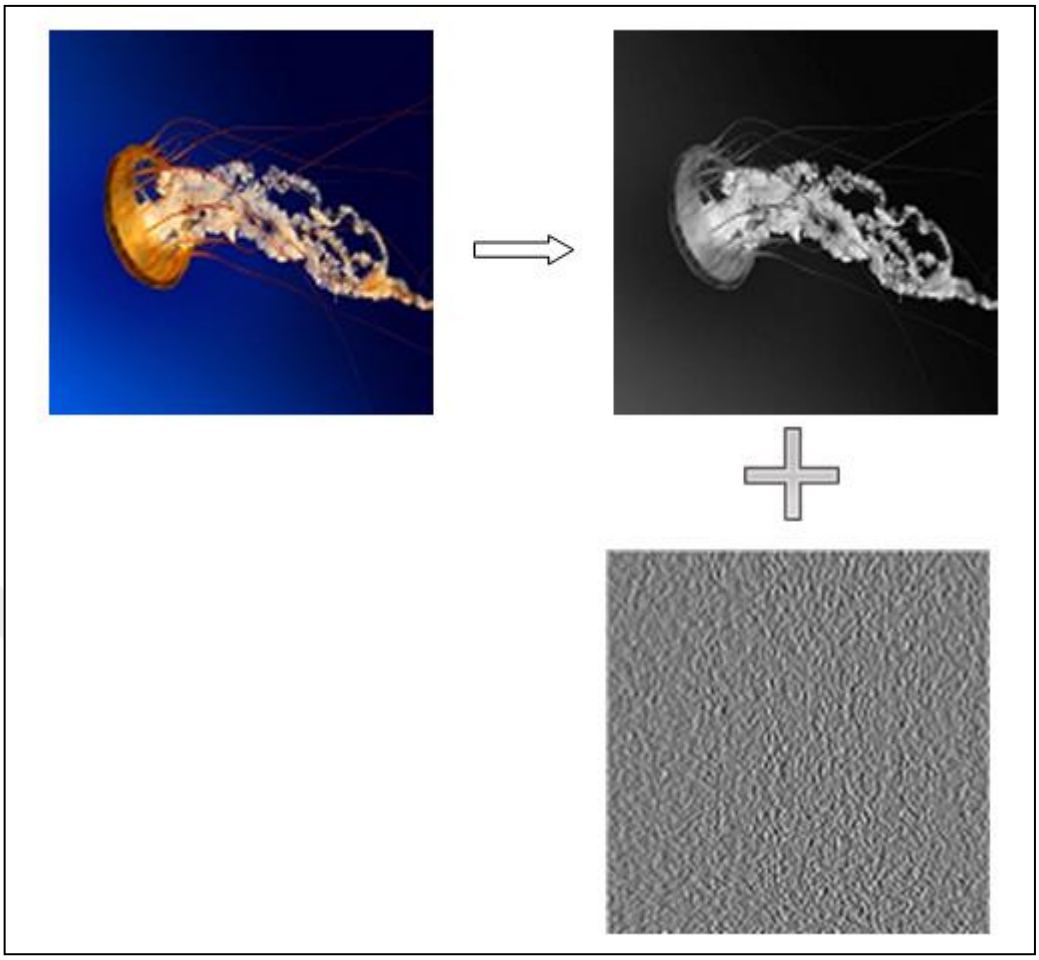
Kapak görüntüleri YCbCr katmanlarına ayrılacaktır ve Şekil 4.7.'de verildiği gibi LSB yöntemine dayanılarak ve Ayrık Dalgacık Dönüşümü (DWT) kullanılarak, paylar görüntülerin Y katmanlarına gömülecektir.



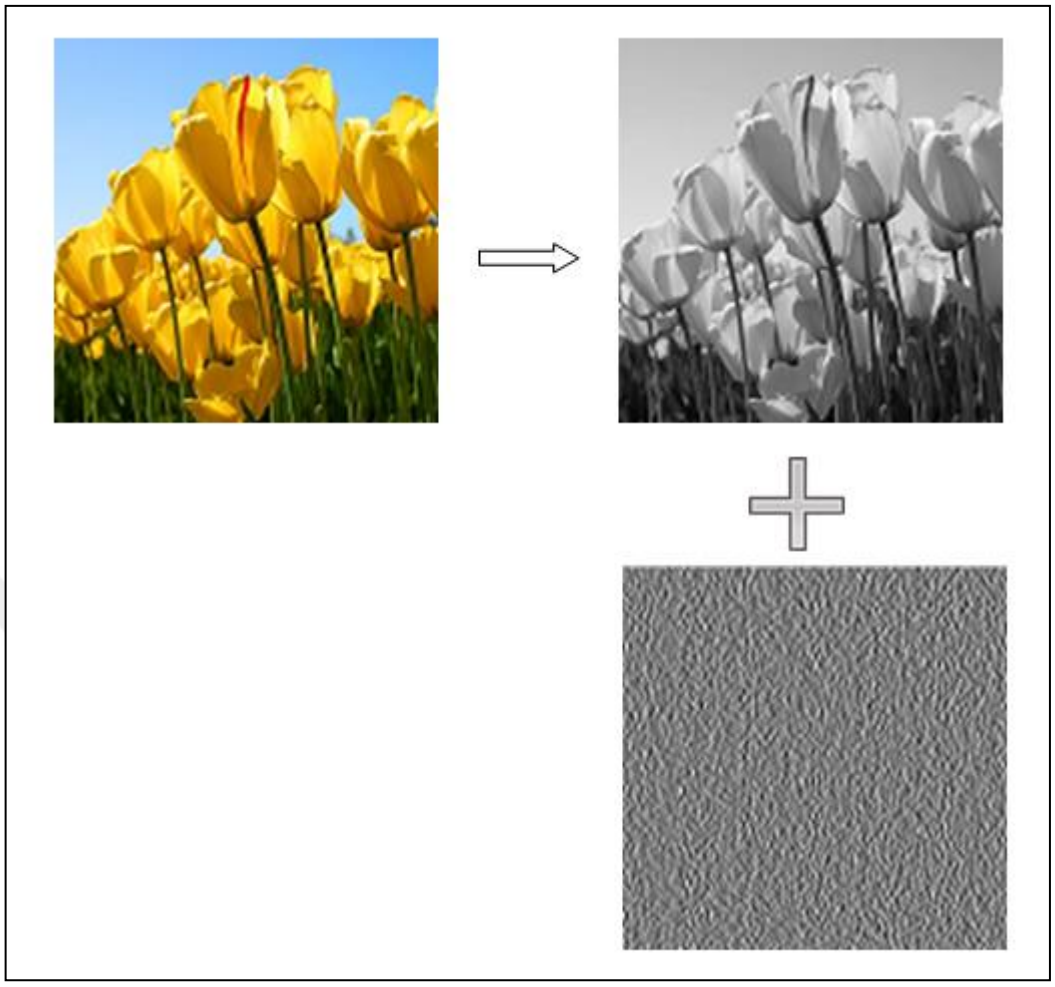
Şekil 4.7. Renkli görüntülere pay gömme



Şekil 4.8. Kapak görüntüleri ve görüntülerin Y katmanları



Şekil 4.9. Birinci kapak görüntüsünün Y katmanına pay gömme

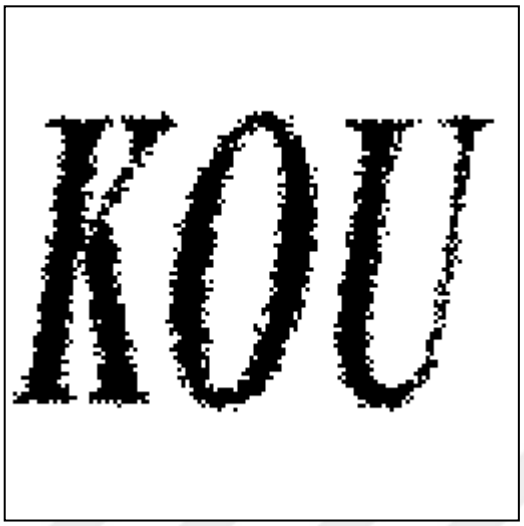


Şekil 4.10. İkinci kapak görüntüsünün Y katmanına pay gömme

Şekil 4.11. Payların gömülü olduğu kapak görüntülerinin Y katmanları

İçerisinde sırların gömülü olduğu görüntülere ters DWT uygulanacak ve payların gömülü olduğu birinci Y katmanının alt bantlarından her biri birinci pay, ikinci Y

katmanının alt bantlarından her biri ikinci pay olacaktır. Birinci pay ile ikinci pay XOR yöntemiyle birleştirilince Şekil 4.12.'deki gibi sır açığa çıkacaktır.



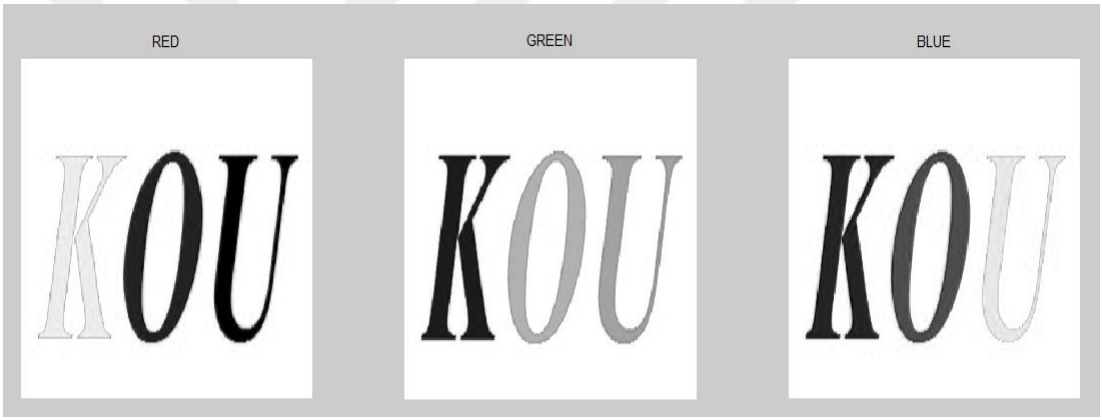
Şekil 4.12. Payların bir araya getirilmiş hali

4.2.2. Renkli görüntüde sır paylaşımı ve stenografi

Renkli görüntülerde kırmızı, yeşil ve mavi 0 ile 255 arasındaki değerlerle ifade edilir. 0 değeri bu üç temel renkten hiç birinin bulunmadığını, 255 değeri de bu renklerin miktarının maksimum olduğu belirtilmektedir. Böylece her dizinin "gri seviyeleri" belirli bir pozisyondaki pikselin kırmızı, yeşil ve mavi resimlerinin bileşenlerinin şiddetini belirler. RGB görüntülerde kırmızı, yeşil ve mavi rengi temsil eden 0-255 arası değer verilmiştir. (0, 0, 0) ile beyaz, (255, 255, 255) ile siyah, (255, 0, 0) ile kırmızı, (0, 255, 0) ile yeşil ve (0, 0, 255) ile mavi renk temsil edilmektedir.

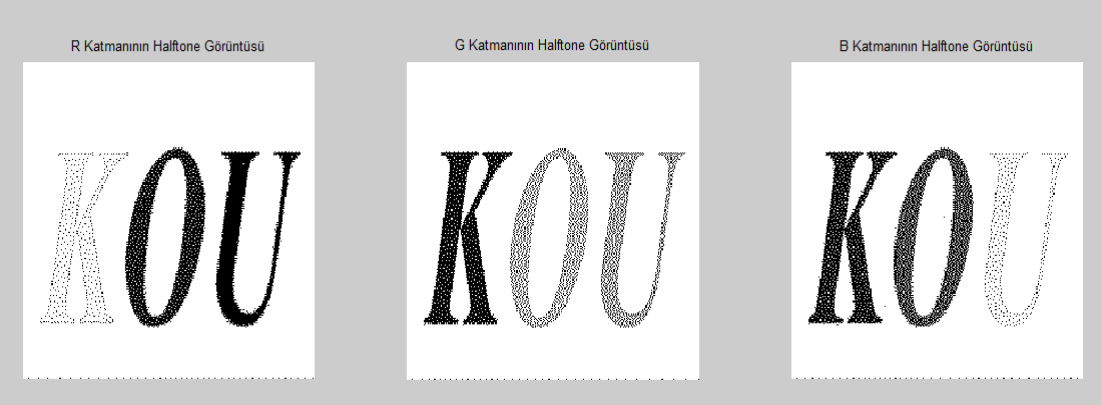
Renkli görüntülerdeki piksel değerleri [0,255] aralığında olduğu için öncelikle görüntüyü katmanlarına ayırarak, değerler sadece 0 ve 255 olarak düzenlenmektedir. Kullanılan ikili görüntü, Şekil 4.13.'te verilen 256x256 boyutlu JPEG formatlı RGB görüntüsüdür. Bu görüntünün katmanlarına ayrılmış hali Şekil 4.14.'te verilmiştir.

Şekil 4.13. Uygulamada kullanılacak olan renkli sır görüntü



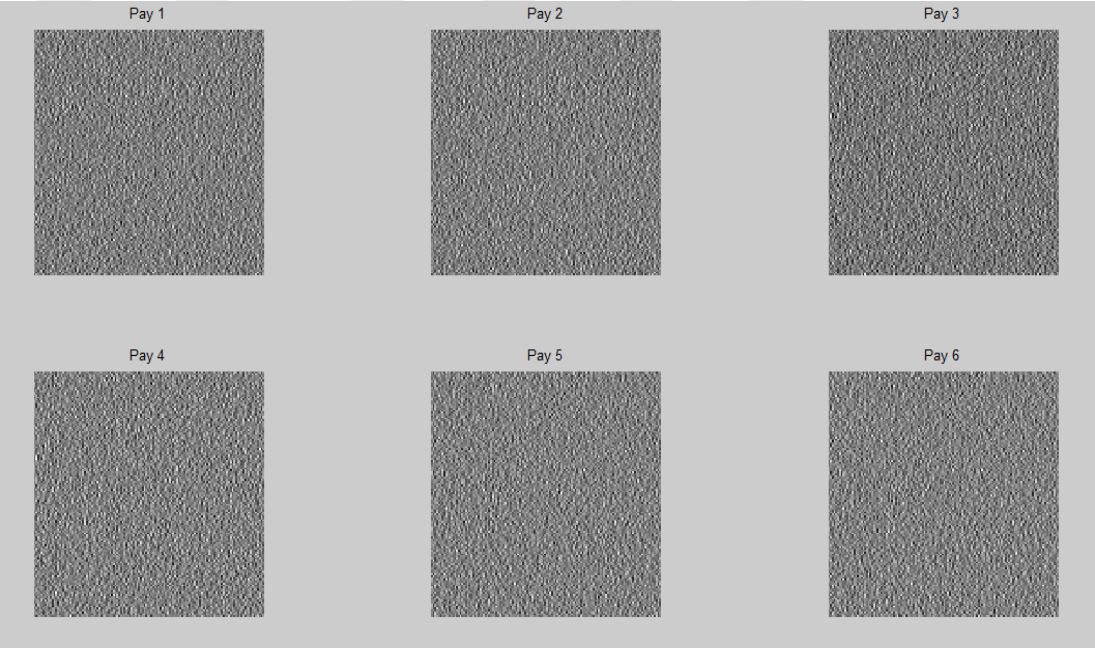
Şekil 4.14. Renkli sır görüntüsünün RGB katmanlarına ayrılmış hali

Daha sonra RGB görüntünün katmanları, Şekil 4.15.'te gösterildiği gibi Floyd-Steinberg algoritması kullanılarak, değerleri sadece 0 ve 1'den oluşan ikili (binary) görüntüye dönüştürülmektedir.



Şekil 4.15. Sır görüntüsünün RGB katmanlarının halftone hali

İkili formata dönüştürülmüş olan sır görüntüsünün katmanları, Shamir algoritmasına kullanılarak Şekil 4.16.'daki gibi altı paya ayrılmaktadır.

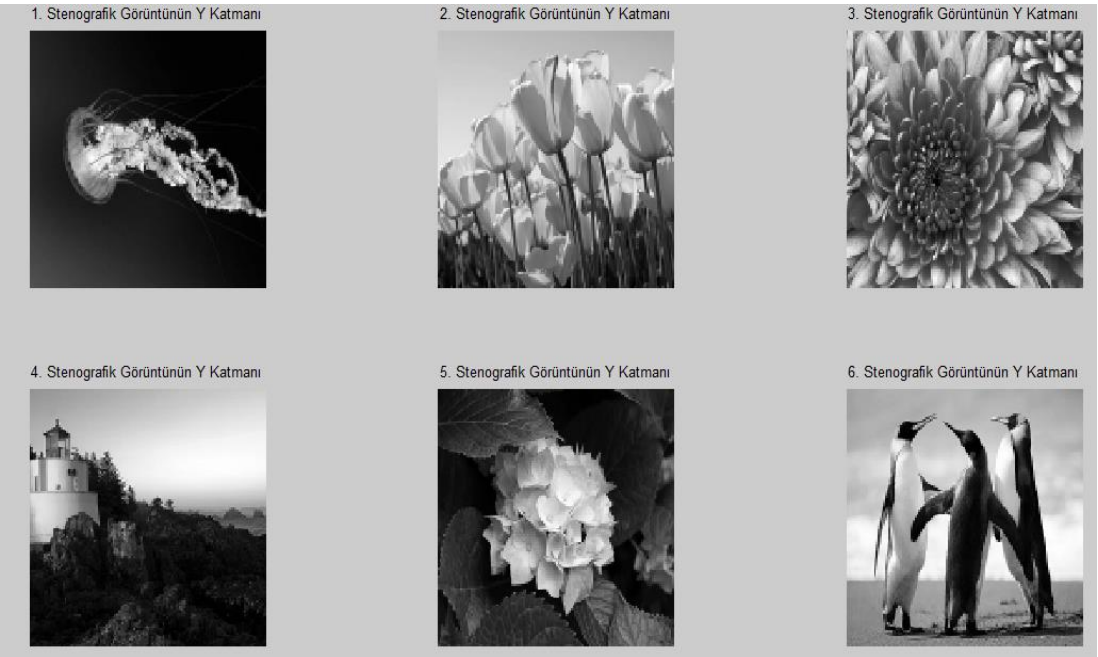


Şekil 4.16. Sır görüntüsünün payları

Payların gömüleceği 6 tane RGB kapak (cover) görüntüleri, Şekil 4.17.'deki gibi LSB yöntemi esas alınarak YCbCr katmanlarına ayrılır.

Şekil 4.17. Kapak görüntüleri ve Y katmanları

Ayrık Dalgacık Dönüşümü (DWT) kullanılarak, Şekil 4.18.'deki gibi kapak görüntülerinin Y katmanlarının alt bantlarına paylar gömülür.



Şekil 4.18. Pay gömülmüş kapak görüntülerinin Y katmanları

İçerisinde sırların gömülü olduğu görüntülere ters DWT uygulanacak ve payların gömülü olduğu Y katmanlarının alt bantlarından her biri birer pay olacaktır. Paylar XOR yöntemiyle birleştirildiğinde, Şekil 4.19.'da verildiği gibi sır açığa çıkacaktır.

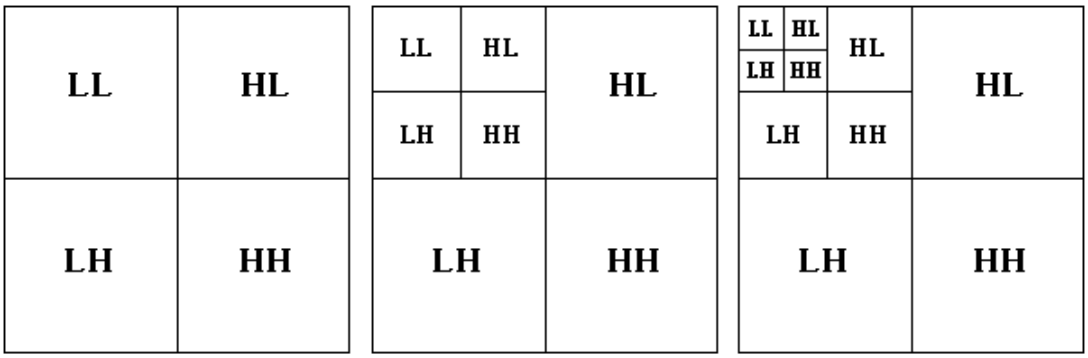
Şekil 4.19. Payların birleştirilmiş hali

5. BULGULAR VE TARTIŞMA

Bu tezde, görsel verilerden Shamir algoritması kullanılarak elde edilen payların, seçilen kapak görüntülerinin Y katmanına dalgacık dönüşümü uygulandıktan sonra elde edilen alt bantlarına gömülmesi ve ters dalgacık dönüşümü ile payların tekrar elde edilip, XOR yöntemiyle birleştirilmesi sonucunda elde edilen görüntü üzerindeki değişiklikler ve sır görüntüsü ile elde edilen görüntü arasındaki farklılıklar incelendi. Kullanılan görsel veriler MATLAB paket programında uygun kodlar yazılarak sonuçlar elde edildi. MATLAB paket programındaki dalgacık kodlarından yararlanıldı. Dalgacık dönüşümünün 2-boyutlu veriler için uygunluğunun ilk aşama olarak incelenmesi uygun görüldü. Sır görüntüsü olarak ikili ve RGB olmak üzere iki görüntü analiz edildi ve sır paylaşımından elde edilen sonuçların PSNR değerleri hesaplandı.

5.1. Görsel Verilerin Dalgacık Dönüşümü ile Kapak Görüntüye Gömülmesi

Bu bölümde, sır görüntüsünden elde edilen payları, kapak görüntülerinin ilgili katmanına gömmek için kullanılacak olan 1., 2. ve 3. seviye ağaç modelinin çoklu çözülme analizi Şekil 5.1'de gösterildi. İki uygulamada da kullanılan altı tane kapak görüntüsünden LSB yöntemi esas alınarak elde edilen Y katmanına 1. seviyede Haar dalgacık dönüşümü uygulandı. Bu dönüşüm sayesinde elde edilen alt bantlardan yaklaşım (A1) kısmı sabit kalırken, detay (D1) alt bantları yerine sır görüntülerinin payları gömüldü. Ters dalgacık dönüşümüyle katman tekrar elde edilerek katılımcılara verilecek olan, içlerinde sır gömülmüş stego görüntüler elde edildi.



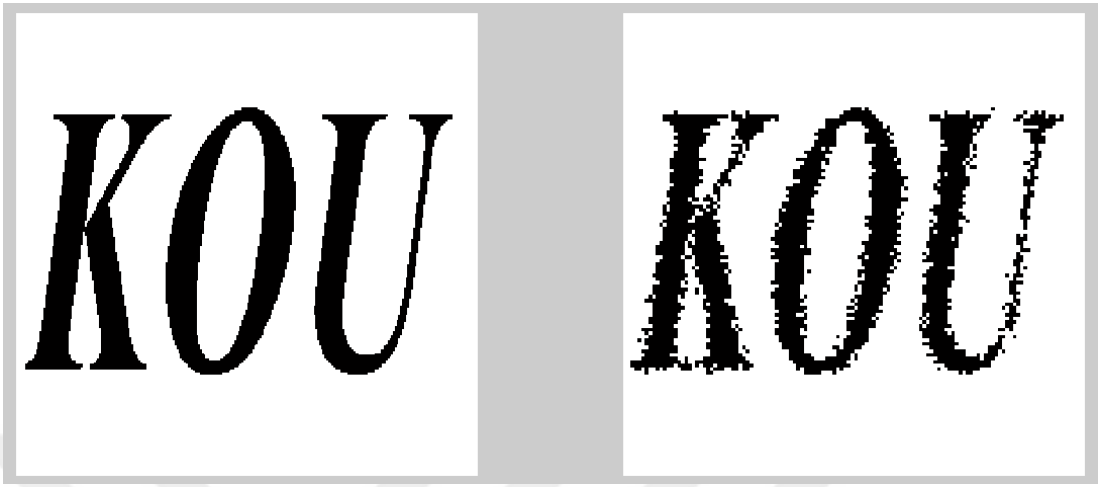
Şekil 5.1. Çoklu çözülme analizinde dalgacık dönüşümü ile 1., 2. ve 3. seviyede ağaç modeli

6. SONUÇLAR VE ÖNERİLER

Algoritmanın analizi, ikili ve 24 bit RGB olmak üzere 256x256 boyutunda iki sır görüntüsü ve rastgele seçilen altı tane, 24 bit, 256x256 boyutunda, RGB kapak görüntüleri kullanılarak analiz edildi. Algoritma bir dalgacık araç kutusu yardımıyla MATLAB da geliştirildi.

Çalışmada ikili görüntüye Shamir algoritması uygulayarak iki pay elde edildi. 24 bit, 256x256 boyutlu, RGB kapak görüntülerinden iki tanesi rastgele seçildi. RGB kapak görüntüleri MATLAB uygulamasında yazılan kodlarla YCbCr formatına dönüştürüldü ve LSB uygulaması esas alınarak kapak görüntüleri Y, Cb ve Cr katmanlarına ayrıldı. Bu katmanlardan her bir kapak görüntüsünün Y katmanına dalgacık dönüşümü uygulandı ve Y katmanlarının yatay, dikey ve köşegen alt bantlarına sır görüntüsünün paylarından biri gömüldü. Ters dalgacık dönüşümü kullanılarak kapak görüntüleri tekrar elde edildi ve sır paylaşım şeması esas alınarak katılımcılara paylaştırıldı. Katılımcılar, ellerindeki görüntülerden dalgacık dönüşümü yardımıyla elde ettikleri payları bir araya getirerek sır görüntüsünü elde ederler. Elde edilen paylar OR işlemiyle birleştirildiğinde, pay görüntülerindeki siyah ve beyaz piksellerin denk geldiği pikseller siyah olduğu için sır görüntüsünün bazı pikselleri beyaz olması gerekirken siyah olabilmektedir. Bunun sonucu olarak elde edilen görüntü, kısım kısım siyah beyaz gürültüye sahip olmaktadır. Bu nedenle OR işlemi yerine XOR işlemini kullandık. XOR işleminde siyah beyaz görüntülerin birleştiği piksellerde beyaz görüntü elde edilmekte ve sadece iki siyah pikselin birleştiği piksellerde siyah piksel elde edilmektedir ve bu yöntemle elde edilen görüntüde oluşan gürültü giderilmektedir. Siyah ve beyaz piksel sayılarına bakıldığında, ikili sır görüntüsünde 53465 siyah piksel ve 12071 beyaz piksel bulunmaktadır. Elde edilen ikili görüntüye bakıldığında, bu görüntünün de aynı sayıda siyah ve beyaz piksele sahip olduğu görülmektedir. Yani sır görüntüsünün paylara ayrılması, kapak görüntülere gömülmesi ve tekrar elde edilerek XOR yöntemiyle bir araya getirilmesiyle elde edilen görüntüde piksel kaybı olmamaktadır. Sır görüntüsü ve

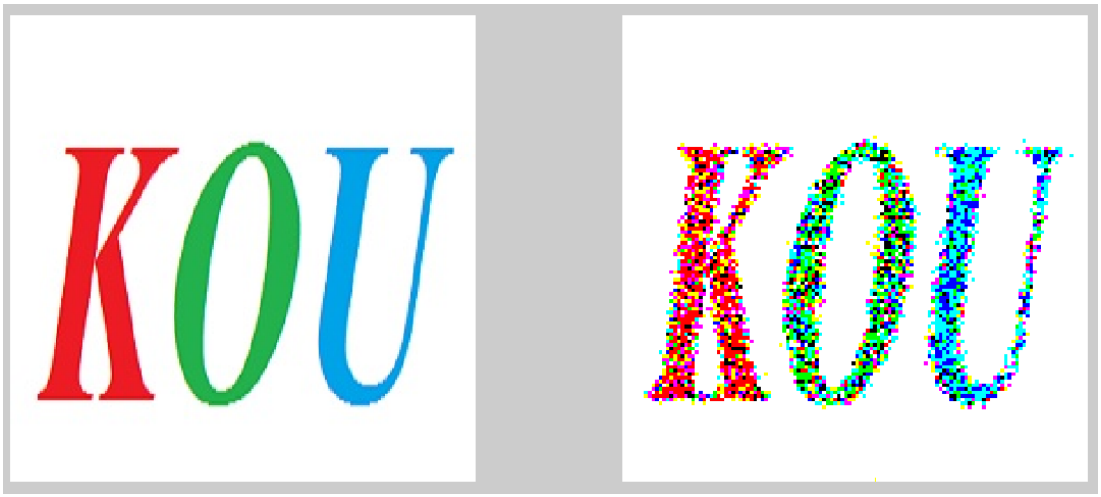
elde edilen görüntü arasındaki PSNR değeri 61.9855 olarak elde edilmiştir. Bu değer iki görüntünün benzerliğini yüksek oranda kanıtlar niteliktedir.



(a) (b)

Şekil 5.2. (a) İkili sır görüntüsü, (b) Payların bir araya gelmesiyle elde edilen görüntü

Çalışmada 24 bit RGB sır görüntüsünü, MATLAB uygulamasında ayrı ayrı R, G ve B katmanlarına ayrıldı. Sır görüntüsünün ayrılan her katmanına Floyd-Steinberg algoritmasını uygulayarak katmanların halftone hali elde edildi. Bu aşamada R, G ve B katmanlarına halftone uygulamasıyla, üç katmanda ikili görüntülere dönüştürülmüştür. Shamir'in algoritmasını kullanarak, üç halftone katmanı sırlara ayrıldı. Her katmandan iki pay elde edildiği için toplamda altı sır payı elde edildi. Bu altı sır payının gömüleceği 24 bit, 256x256 boyutlu altı RGB kapak görüntüsü rastgele seçildi. Bu RGB kapak görüntülerinin her biri, MATLAB uygulamasında yazılan kodlarla YCbCr formatına dönüştürüldü ve LSB uygulaması esas alınarak Y, Cb ve Cr katmanlarına ayrıldı. Bu altı kapak görüntüsünden her birinin Y katmanına dalgacık dönüşümü uygulandı ve Y katmanlarının yatay, dikey ve köşegen alt bantlarına, sır görüntüsünün altı payından biri yerleştirildi. Ters dalgacık dönüşümü kullanılarak kapak görüntüleri tekrar elde edildi ve sır paylaşım şeması esas alınarak katılımcılara paylaştırıldı. Altı katılımcıdan alınan stego görüntülerin alt bantlarında bulunan paylar, dalgacık dönüşümü yardımıyla elde edildi. Elde edilen paylar XOR işlemiyle birleştirilerek sır görüntüsü yeniden elde edildi.



(a) (b)

Şekil 5.3. (a) RGB sır görüntüsü, (b) Payların bir araya gelmesiyle elde edilen görüntü

Sır görüntüsü ve elde edilen görüntü arasındaki PSNR değeri 12.7909 olarak elde edilmiştir. Bu değer, PSNR değeri için başarılı sayılan ≥20 koşulundan düşüktür. Fakat elde edilen sır görüntüsü, ilk sır görüntüsünü de açığa çıkarmaktadır. Çalışmamızın sonucunda, metin görüntüleri daha başarılı olurken, fazla detaylı görsel açıdan zengin görüntüler metin görüntüleri kadar başarılı olamamaktadır.

Çalışmamızın sonucunda, ikili ve RGB görüntülerin gömülmesinde dalgacık dönüşümünün kullanılabileceği görüldü. İleriki aşamalarda pay gömülmesinde ve sırrın tekrar açığa çıkarılmasında dalgacık dönüşümüyle alınan sonuçların iyileştirmesi üzerine çalışmalar yapılacaktır. 1-boyutlu verilerde dalgacık dönüşümü optimaldır. Dalgacık dönüşümü kullanılarak yapılan her uygulamadan elde edilen sonuçların, Shearlet dönüşümü kullanılarak daha iyi elde edilebileceği düşünülmektedir. Bu nedenle çalışmamızın devamında, 2-boyutlu veriler için dalgacık dönüşümü yerine Shearlet dönüşümünü kullanarak görsel sır paylaşımı, kriptografi ve stenografi uygulamaları yapılacaktır.

KAYNAKLAR

[1] http://www.hhportal.com/kriptoloji/4395-kriptolojiye-giris.html, (Ziyaret Tarihi: 6 Nisan 2017).

[2] https://tr.wikipedia.org/wiki/Kriptoloji, (Ziyaret Tarihi: 6 Nisan 2017).

[3] http://www.bilgiustam.com/kriptoloji-nedir/, (Ziyaret Tarihi: 6 Nisan 2017).

[4] http://www.acikbilim.com/2014/11/dosyalar/kriptoloji-tarihine-yolculuk-turler-ornekler.html, (Ziyaret Tarihi: 6 Nisan 2017).

[5] https://cod3xblog.wordpress.com/2015/01/14/kriptoloji-ve-uygulamali-orneklerders-1/, (Ziyaret Tarihi: 6 Nisan 2017).

[6] https://tr.wikipedia.org/wiki/Vigenere_sifrelemesi, (Ziyaret Tarihi: 6 Nisan 2017).

[7] http://adlibilimler.org/kriptoloji-gizlilik-ve-guvenligin-temel-yapi-tasi/, (Ziyaret Tarihi: 10 Nisan 2017).

[8] https://www.sondakika.com/haber/haber-japon-isi-11-gizli-silah-7124330/, (Ziyaret Tarihi: 10 Nisan 2017).

[9] http://www.savaskartal.com/2010/04/15, (Ziyaret Tarihi: 15 Nisan 2017).

[10] http://www.temizkod.com/kriptoloji-nedir/, (Ziyaret Tarihi: 15 Nisan 2017).

[11] http://tr.wikipedia.org/wiki/Kuantum_kriptografi, (Ziyaret Tarihi: 15 Nisan 2017).

[12] http://www.turkhackteam.org/kriptografi-sifreleme/1193443-kriptografi-hakkinda-bilgiler-t3rmin4tor.html, (Ziyaret Tarihi: 6 Nisan 2017).

[13] Shamir A., How To Share A Secret, *Communications of the ACM*, 1979, **22**(11), 612–613.

[14] Blakley G. R. Safeguarding Cryptographic Keys, *Proceedings AFIPS 1979 National Computer Conference*, 1979, **48**, 313–317.

[15] Demir M., Ulutaş M., Odabaş E., Asmuth Bloom Sır Paylaşım Tekniğinin Hızlandırılması İçin Koşut Programlama, *TMMOB Elektrik Mühendisleri Odası Fırat Üniversitesi Elektrik-Elektronik ve Bilgisayar Sempozyumu,* Elazığ, Türkiye, 5-6-7 Ekim 2011.

[16] Naor M., Shamir A., Visual Cryptography, *The Proceedings Of The Conference on Advances in Cryptology EUROCRYPT'94*, 1994, **950**, 1-12.

[17] https://akgulomer.wordpress.com/2011/01/23/veri-guvenligi-1/, (Ziyaret Tarihi: 30 Nisan 2017).

[18] Thien C. C., Lin J. C., Secret Image Sharing, *Pergamon Computers & Graphics*, 2002, **26**, 765-770.

[19] http://ab.org.tr/ab13/bildiri/59.pdf, Bilgin M., Stenografi, (Ziyaret Tarihi: 1 Mayıs 2017).

[20] Lenti J., Steganographic Methods, *Periodica Polytechnica Ser. El. Eng.*, 2000, **44**, 249-258.

[21] Ker A. D., Steganalysis of LSB Matching in Grayscale Images, *IEEE Signal Processing Letters*, 2005, **12**(6), 441-444.

[22] de Queiroz R. L., Braun K. M., Color to Gray and Back: Color Embedding Into Textured Gray Images, *IEEE Transactions On Image Processing*, 2006, **15**(6), 1464-1470.

[23] Shyu S. J., Efficient Visual Secret Sharing Scheme for Color Images, *Elsevier Pattern Recognition*, 2006, **39**, 866-880.

[24] Blundo C., Bonis A. D., Santis A. D., Improved Schemes For Visual Cryptography, *Designs, Codes And Cryptography*, 2001, **24**(3), 255-278.

[25] Yang C. N., Laih C. S., New Colored Visual Secret Sharing Schemes, *Designs, Codes And Cryptography*, 2000, **20**(3), 325-336.

[26] Hseieh S. L., Jian J. J., Tsai I. J., Huang B. Y., A Color Image Watermarking Scheme Based on Secret Sharing and Wavelet Transform, *Systems, Man and Cybernetics IEEE International Conference on*, DOI: 10.1109/ICSMC.2007.4414071.

[27] Wang R. Z., Shyu S. J., Scalable Secret Image Sharing, *Elsevier Signal Processing: Image Communication*, 2007, **22**, 363-373.

[28] Yang C. N., Wang C. C., Chen T. S., Visual Cryptography Schemes with Reversing, *The Computer Journal*, 2008, **51**(6), 710-722.

[29] Liu F., Wu C. K., Lin X. J., Colour Visual Cryptography Schemes, *IET Information Security*, 2008, **2**(4), 151-165.

[30] Seyedhosseini M., Ghaemmaghami S., Detection of LSB Replacement and LSB Matching Steganography Using Gray Level Run Length Matrix, *Fifth International Conference on Intelligent Information Hiding and Multimedia Signal Processing*, DOI: 10.1109/IIH-MSP.2009.68.

[31] Shyu J. S., Image Encryption By Multiple Random Grids, *Elsevier Pattern Recognition*, 2009, **42**, 1582-1596.

[32] Qiao W., Yin H., Liang H., A Kind of Visual Cryptography Scheme For Color Images Based on Halftone Technique, *International Conference on Measuring Technology and Mechatronics Automation*, DOI: 10.1109/ICMTMA.2009.294.

[33] Leung B. W., Ng F. Y., Wong D. S., On The Security Of A Visual Cryptography Scheme For Color Images, *Elsevier Pattern Recognition*, 2009, **42**, 929-940.

[34] Wang R. Z., Lana Y. C., Lee Y. K., Huang S. Y., Shyu S. J., Chia T. L., Incrementing Visual Cryptography Using Random Grids, *Elsevier Optics Communications*, 2010, **283**, 4242-4249.

[35] Liu G., Zhang Z., Dai Y., Improved LSB-Matching Steganography For Preserving Second-Order Statistics, *Journal Of Multimedia*, 2010, **5**(5), 458-463.

[36] Lin P. Y., Chan C. S., Invertible Secret Image Sharing With Steganography, *Elsevier Pattern Recognition Letters*, 2010, **31**, 1887–1893.

[37] Saichandana B., Srinivas K., Kumar R. K., Visual Cryptography Scheme For Color Images, *International Journal Of Computer Engineering And Technology (IJCET)*, 2010, **1**(1), 207-212.

[38] Lin T. L., Horng S. J., Lee K. H., Chiu P. L., Kao T. W., Chen Y. H., Run R. S., Lai J. L., Chen R. J., A Novel Secret Sharing Scheme For Multiple Secret Without Pixel Expansion, *Elsevier Expert Systems With Applications*, 2010, **37**(12), 7858-7869.

[39] Revenkar P. S., Anjum A., Gandhare W. Z., Survey Of Visual Cryptography Schemes, *International Journal Of Security And Its Applications*, 2010, **4**(2), 49-56.

[40] Abdulla S., New Visual Cryptography Algorithm For Colored Image, *Journal Of Computing*, 2010, **2**(4), 21-25.

[41] Chen T. H., Wu C. S., Efficient Multi-Secret Image Sharing Based On Boolean Operations, *Elsevier Signal Processing*, 2011, **91**, 90-97.

[42] Yang C. H. T., Huang Y. H., Syue J. H., Reversible Secret Image Sharing Based on Shamir's Scheme With Discrete Haar Wavelet Transform, *International Conference on Electrical and Control Engineering (ICECE)*, DOI: 10.1109/ICECENG.2011.6057938.

[43] Wang Z. H., Chang C. C., Tu H. N., Li M. C., Sharing A Secret Image In Binary Images With Vertification, *Journal Of Information Hiding Ang Multimedia Signal Processing*, 2011, **2**(1), 78-90.

[44] Ross A., Othman A., Visual Cryptography For Biometric Privacy, *IEEE Transactıons On Information Forensics And Security*, 2011, **6**(1), 70-81.

[45] Liu F., Wu C., Embedded Extended Visual Cryptography Schemes, *IEEE Transactıons On Information Forensics And Security*, 2011, **6**(2), 307-322.

[46] Verma J., Khemchandani V., A Visual Cryptographic Technique To Secure Image Shares, *International Journal of Engineering Research and Applications (IJERA),* 2012, **2**(1), 1121-1125.

[47] Nerella S. K., Gadi K. V., Chaganti R. S., Securing Images Using Colour Visual Cryptography And Wavelets, *International Journal of Advanced Research in Computer Science and Software Engineering*, 2012, **2**(3), 163-168.

[48] Makhijani R. K., Panjwani L. D., A Review of Color Visual Cryptographic Schemes, *International Journal Advanced Networking and Applications*, 2012, **3**(5), 1379-1384.

[49] Priyanka C., VenkataRamana T., Somashekar T., Analysis of Secret Sharing & Review on Extended Visual Cryptography Scheme, *International Journal of Engineering Inventions*, 2012, **1**(10), 43-51.

[50] Patil S., Rao J., Extended Visual Cryptography For Color Shares Using Random Number Generators, *International Journal of Advanced Research in Computer and Communication Engineering*, 2012, **1**(6), 399-410.

[51] Singh T. R., Singh K. M., Roy S., Image Watermarking Scheme Based On Visual Cryptography In Discrete Wavelet Transform, *International Journal of Computer Applications*, 2012, **39**(1), 18-24.

[52] Chen T. H., Tsao K. H., Lee Y. S., Yet Another Multiple-Image Encryption By Rotating Random Grids, *Elsevier Signal Processing*, 2012, **92**(9), 2229-2237.

[53] Patil S., Tajane K., Sirdeshpande J., Analysing Secure Image Secret Sharing Schemes Based On Steganography, *International Journal Of Computer Engineering & Technology*, 2013, **4**(2), 172-178.

[54] Banumathi C., Pearly A. A., Secret Sharing Using Visual Cryptography Based on Reversed Images, *International Journal Of Engineering Sciences & Research Technology*, 2013, **2**(4), 941-945.

[55] Deepa G., The Comparative Study on Visual Cryptography and Random Grid Cryptography, *IOSR Journal of Computer Engineering*, 2013, **12**(2), 4-14.

[56] Girdhar A., Kuar A., Secret Image Sharing Scheme with Steganography and Authentication Based on Discrete Wavelet Transform, *International Conference on Innovations in Engineering and Technology*, DOI: 10.15242/IIE.E1213594.

[57] Nikam P., Kinage K., Survey On Visual Cryptography Schemes, *International Journal of Science and Research*, 2013, **4**(1), 703-705.

[58] Guo T., Liu F., Wu C. K., Yang C. N., Wang W., Ren Y. W., Threshold Secret Image Sharing, *International Conference on Information and Communications Security*, 2013, **8233**, 404-412.

[59] Ramya J., Parvathavarthini B., An Extensive Review On Visual Cryptography Schemes, *International Conference on Control, Instrumentation, Communication and Computational Technologies*, DOI: 10.1109/ICCICCT.2014.6992960.

[60] Benyoussef M., Mabtoul S., El Marakki M., Aboutajdine D., Robust Image Watermarking Scheme Using Visual Cryptography In Dual-Tree Complex Wavelet Domain, *Journal of Theoretical and Applied Information Technology*, 2014, **60**(2), 372-379.

[61] Soradge N., Thakare K. S., A Review On Various Visual Cryptography Schemes, *International Journal of Computer Science and Business Informatics*, 2014, **12**(1), 45-54.

[62] Madhavi D., Devasastry A. V., A Survey on Perceived Visual Quality and Secured Visual Cryptography Schemes, *International Journal of Computer Applications*, 2014, **86**(2), 27-29.

[63] Patil S., Deshmukh P., Enhancing Security In Secret Sharing With Embedding Of Shares In Cover Images, *International Journal Of Advanced Research In Computer And Communication Engineering*, 2014, **3**(5), 6685-6688.

[64] Mursi M. F. M., Salama M., Mansour M., Visual Cryptography Schemes: A Comprehensive Survey, *International Journal Of Emerging Research In Management & Technology*, 2014, **3**(11), 142-154.

[65] Bharanivendhan N., Amita T., Visual Cryptography Schemes For Secret Image Sharing Using GAS Algorithm, *International Journal of Computer Applications*, 2014, **92**(8), 11-16.

[66] Wu X., Sun W., Extended Capabilities For XOR-Based Visual Cryptography, *IEEE Transactions On Information Forensics And Security*, 2014, **9**(10), 1592-1605.

[67] Raut R. R., Bijwe K. B., A Survey Report On Visual Cryptography And Secret Fragment Visible Mosaic Images, *International Journal Of Application Or Innovation In Engineering & Management (IJAIEM)*, 2014, **3**(10), 216-220.

[68] Lee J. S., Chang C. C., Huynh N. T., Tsai H. Y., Preserving User-Friendly Shadow And High-Contrast Quality For Multiple Visual Secret Sharing Technique, *Elsevier Digital Signal Processing*, 2015, **40**, 131-139.

[69] Wei S. C., Hou Y. C., Lu Y. C., A Technique For Sharing A Digital Image, *Elsevier Computer Standards & Interfaces*, 2015, **40**, 53-61.

[70] Patil Y., Use Of Genetic Algorithm And Visual Cryptography For Data Hiding In Image For Wireless Network, *International Journal Of Computer Applications*, 2015, **113**(1), 21-23.

[71] Rashwan A., Wang H., Partial Image Secret Sharing Using Discrete Wavelet Transform, *Computer Science and Engineering*, 2015, **5**(1A), 1-7.

[72] Lekshmi S. J., Anil A. R., Secure Visual Secret Sharing Based On Discrete Wavelet Transform, *ICTACT Journal On Image And Video Processing*, 2015, **6**(1), 1072-1075.

[73] Islam N., Kikan S., A Survey: Novel Study For Visual Cryptography In Discrete Wavelet Transforms, *International Journal Of Advanced Research In Computer Science and Software Engineering*, 2015, **5**(5), 481-483.

[74] Thepade S. D., Patil R. S., Novel Reversible Image Secret Sharing Based On Thien and Lin's Scheme Using Discrete Haar Wavelet Transform, *International Conference On Pervasive Computing (ICPC)*, DOI: 10.1109/PERVASIVE.2015.7087037.

[75] Lin C. H., Lee Y. S., Chen T. H., Friendly Progressive Random-Grid-Based Visual Secret Sharing With Adaptive Contrast, *Elsevier Journal Of Visual Communication & Image Representation*, 2015, **33**, 31-41.

[76] Kumar M. S., Shilpa A., Vijayalakshmi J. R., A Survey On Visual Cryptography Techniques, *International Journal Of Application Or Innovation In Engineering & Management (IJAIEM)*, 2016, **5**(2), 100-112.

[77] http://www.iosrjournals.org/iosrjce/papers/conf.15013/Volume%201/2%20.06-12.pdf?id=7557, (Ziyaret Tarihi: 25 Nisan 2017).

[78] http://www.iosrjournals.org/iosrjce/papers/ICETEM/Vol.%201%20Issue%203/CSE-04-15-18.pdf, (Ziyaret Tarihi: 25 Nisan 2017).

[79] Bali A., Ansari S., Khan K., Shaikh W., Securing Informative Text Using Color Visual Cryptography, *International Journal Of Computer Applications*, 2016, **136**(5), 30-33.

[80] Shaikh R., Siddh S., Ravekar T., Sugaonkar S., Visual Cryptography Survey, *International Journal Of Computer Applications*, 2016, **134**(2), 10-12.

[81] Erdoğan H., Gülal E., Akpınar B., Ata E., Asma Köprülerin Titreşimlerinin GPS İle İzlenmesi, *TMMOB Harita ve Kadastro Mühendisleri Odası 12. Türkiye Harita Bilimsel ve Teknik Kurultayı,* Ankara, Türkiye, 11-15 Mayıs 2009.

[82] Miner N. E., *An Introduction to Wavelet Theory and Analysis*, 1rd ed., Sandia Hall, California, 1998.

[83] Polikar R., The Story of Wavelets, *IMACS/IEEE CSCC'99 Proceedings*, Florida, USA, 25-29 July 1999.

[84] Batar H., EEG İşaretlerinin Dalgacık Analiz Yöntemleri Kullanılarak Yapay Sinir Ağları İle Sınıflandırılması, Yüksek Lisans Tezi, Kahramanmaraş Sütçü İmam Üniversitesi, Fen Bilimleri Enstitüsü, Elektrik-Elektronik Mühendisliği Anabilim Dalı, Kahramanmaraş, 2005, 197467.

[85] Torrence C., Compo P. C., A Practical Guide To Wavelet Analysis, *Bulletin of American Meteorological Society*, 1998, **79**(1), 61-78.

[86] Roberts R. A., Mullis C. T., *Digital Signal Processing*, 1rd ed., Addison-Wesley Publishing Company, USA, 1987.

[87] Rangayyan M. R., *Biomedical Signal Analysis*, 1rd ed., CRC Press, Alberta, Canada, 518, 2002.

[88] Kumdereli Ü. C., Tıp Bilişimi Ve Veri Madenciliği Uygulamaları: EEG Sinyallerindeki Epileptiform Aktiviteye Veri Madenciliği Yöntemlerinin Uygulanması, Yüksek Lisans Tezi, Trakya Üniversitesi, Fen Bilimleri Enstitüsü, Bilgisayar Mühendisliği Anabilim Dalı, Edirne, 2012, 318331.

[89] http://en.wikipedia.org/wiki/Haar_wavelet, (Ziyaret tarihi: 04 Mayıs 2015).

[90] Christensen O., An Introduction to Wavelet Analysis, Benedetto J. J., *Functions, Spaces, and Expansions*, 1rd ed., Springer Science & Business Media, Boston, 159-180, 2010.

[91] Christensen O., A Closer Look at Multiresolution Analysis, Benedetto J. J., *Functions, Spaces, and Expansions*, 1rd ed., Springer Science & Business Media, Boston, 181-201, 2010.

[92] Ergen B., Baykara M., Dalgacık Ve Dalgacık Paket Ayrıştırması İle İmgelerden Gürültü Temizlemesi Analizi, *e-Journal of New World Sciences Academy*, 2011, **6**(2), 518-526.

[93] Demirhan A., Güler İ., Beyin MR Görüntülerinin Analizi İçin Dalgacık Dönüşümü Ve Sinir Ağlarının Kullanılması (Using Wavelet Transform And Neural Networks For The Analysis Of Brain MR Images), *Signal Processing and Communications Applications Conference (SIU)-18th*. *IEEE*, DOI: 10.1109/SIU.2010.5651477.

[94] https://github.com/bilalcorbacioglu/Secret-Sharing, (Ziyaret Tarihi: 1 Mayıs 2017).

[95] https://en.wikipedia.org/wiki/Floyd–Steinberg_dithering, (Ziyaret Tarihi: 10 Nisan 2017).

[96] http://en.wikipedia.org/wiki/Floyd%E2%80%93Steinberg_dithering, (Ziyaret Tarihi: 10 Nisan 2017).

[97] https://en.wikipedia.org/wiki/Least_significant_bit, (Ziyaret Tarihi: 10 Nisan 2017).

[98] http://bilgisayarkavramlari.sadievrenseker.com/2009/06/05/steganografi-ve-lsb/, (Ziyaret Tarihi: 10 Nisan 2017).

KİŞİSEL YAYIN VE ESERLER

Uluslararası Bildiriler:

[1] Sevindir H., **Sayın N.**, On Visual Secret Sharing Based On Wavelet Transform, *IWW 2016 8th International Conference On Image Processing, Wavelet And Applications*, Istanbul, Turkey, 22-24 September 2016.

[2] Sevindir H., **Sayın N.**, Yazıcı C., Çetinkaya S., Colour Visual Cryptography Based On Discrete Wavelet Transform, *IWW 2016 8th International Conference On Image Processing, Wavelet And Applications*, Istanbul, Turkey, 22-24 September 2016.

ÖZGEÇMİŞ

1991 yılında İstanbul/Üsküdar'da doğdu. İlk, orta ve lise öğrenimini Kocaeli'de tamamladı. 2009 yılında girdiği Kocaeli Üniversitesi Fen-Edebiyat Fakültesi Matematik Bölümü'nden 2013 yılında mezun oldu. 2014 yılında Kocaeli Üniversitesi Fen Bilimleri Enstitüsü Matematik Anabilim Dalı Yüksek Lisans Programı'nda yüksek lisans öğrenimine başladı.