T.C.
DÜZCE ÜNİVERSİTESİ
FEN BİLİMLERİ ENSTİTÜSÜ

YILAN OYUNUNDA STEGANOGRAFİ

KUBİLAY GÜNER

YÜKSEK LİSANS TEZİ
BİLGİSAYAR MÜHENDİSLİĞİ ANABİLİM DALI

DANIŞMAN
YRD. DOÇ. DR. ESRA ŞATIR

DÜZCE, 2017

T.C.
DÜZCE ÜNİVERSİTESİ
FEN BİLİMLERİ ENSTİTÜSÜ

YILAN OYUNUNDA STEGANOGRAFİ

Kubilay GÜNER tarafından hazırlanan tez çalışması aşağıdaki jüri tarafından Düzce Üniversitesi Fen Bilimleri Enstitüsü Bilgisayar Mühendisliği Anabilim Dalı'nda **YÜKSEK LİSANS TEZİ** olarak kabul edilmiştir.

Tez Danışmanı

Yrd. Doç. Dr. Esra ŞATIR

Düzce Üniversitesi

Jüri Üyeleri

Doç. Dr. Oğuz FINDIK
Karabük Üniversitesi _____

Doç. Dr. Resul KARA
Düzce Üniversitesi _____

Yrd. Doç. Dr. Esra ŞATIR
Düzce Üniversitesi _____

Tez Savunma Tarihi: 17/02/2017

BEYAN

Bu tez çalışmasının kendi çalışmam olduğunu, tezin planlanmasından yazımına kadar bütün aşamalarda etik dışı davranışımın olmadığını, bu tezdeki bütün bilgileri akademik ve etik kurallar içinde elde ettiğimi, bu tez çalışmasıyla elde edilmeyen bütün bilgi ve yorumlara kaynak gösterdiğimi ve bu kaynakları da kaynaklar listesine aldığımı, yine bu tezin çalışılması ve yazımı sırasında patent ve telif haklarını ihlal edici bir davranışımın olmadığını beyan ederim.

17 Şubat 2017

Kubilay GÜNER

TEŞEKKÜR

Yüksek lisans öğrenimimde ve bu tezin hazırlanmasında gösterdiği her türlü destek ve yardımdan dolayı çok değerli hocam Yrd. Doç. Dr. Esra ŞATIR' a en içten dileklerimle teşekkür ederim.

Bu çalışma boyunca yardımlarını ve desteklerini esirgemeyen sevgili aileme ve çalışma arkadaşlarıma sonsuz teşekkürlerimi sunarım.

17 Şubat 2017 **Kubilay GÜNER**

İÇİNDEKİLER

ŞEKİL LİSTESİ

Sayfa No

ÇİZELGE LİSTESİ

Sayfa No

KISALTMALAR

AES	Advanced Encryption Standard
ASCII	American Standard Code Information Interchange
DES	Data Encryption Standard
DSP	Digital signal processing
HKMG	Hunt-and-Kill Labirent Generating
HTML	Hyper Text Markup Language
JPEG	Joint Photographic Experts Group
LSB	Least Significant Bit
MSB	Most Significant Bit
OCR	Optical Character Recognition
XML	Extensible Markup Language

SİMGELER

A	Olası kombinasyon sayısı
B	Şifrelenecek dizi
C	Şifrelenmiş dizi
gm	Great moves – iyi hamleler
H	Entropi değeri
I	Başlangıç matrisi
m	Hamle sayısı
n	Gizli mesajın uzunluğu
P	Saldırı olasılığı
R	Sapma eğrisi
T	Eşik değeri

ÖZET

YILAN OYUNUNDA STEGANOGRAFİ

Kubilay GÜNER
Düzce Üniversitesi
Fen Bilimleri Enstitüsü, Bilgisayar Mühendisliği Anabilim Dalı
Yüksek Lisans Tezi
Danışman: Yrd. Doç. Dr. Esra ŞATIR
Şubat 2017, 38 sayfa

Steganografi, görünüşte zararsız taşıyıcılar içinde bilginin varlığını gizleme bilimi olup, mesaj varlığının tespit edilemeyeceği bir iletişim yöntemidir. Verilerin gizlenebileceği çeşitli dijital taşıyıcılar veya resimler, ses dosyaları, metin, html vb. yerler vardır. Bu çalışmada, örtme aracı olarak yılan oyunu kullanan bir oyun steganografi yöntemi tasarlanmıştır. "Vitamin" denilen yemlerin her hareketini tahmin ederek gizli verileri gizlemek hedeflenmiştir. Diğer bir deyişle, gizli verilerin birim bileşenlerine göre vitaminin koordinatları hesaplanır. Bu arada oyun platformunu karmaşıklaştırmayı ve vitamin yeri ile gizli veriler arasında DES S-kutuları kullanarak doğrusal olmayan bir ilişki kurmak planlanmıştır. Bu işlemler, önerilen şemayı muhtemel steganografik saldırılara karşı daha dayanıklı hale getirir ve çözümleme prosedürünü daha karmaşık hale getirir. Bu nedenle, güvenlik ve algılanamazlık bu çalışmanın kapsamı içerisinde ilgi odağı olarak tutulmuştur. Ayrıca, her hareketle önemli kapasite oranları elde edilmiştir. Yapılan deneylerle, bu iddialar desteklenmektedir.

Anahtar sözcükler: DES S-Kutuları, Oyun steganografisi, Oyun teorisi, Steganografi, Yılan oyunu

ABSTRACT

A SNAKE GAME STEGANOGRAPHY METHOD

Kubilay GÜNER
Düzce University
Graduate School of Natural and Applied Sciences, Department of Computer
Master's Thesis
Supervisor: Assist. Prof. Dr. Esra ŞATIR
February 2017, 38 pages

Steganography is the science of concealing the existence of information within innocuous seeming carriers and a communication method in such a way that the presence of a message can not be detected. There are a variety of digital carriers or places like images, audio files, text, html, etc. Where data can be hidden. In this study, we proposed a game steganography method using snake game as the cover medium. We aim to hide the secret data by estimating the each move of the bait called "vitamin". In other words, we compute coordinates of the vitamin according to the unit components of secret data. Mean while, we plan to complicate the game platform and establish a nonlinear relationship between the vitamin location and secret data by employing DES S-boxes. These operations render the proposed scheme more resilient against the possible steganographic attacks and make the extraction procedure more complicated. Therefore, security and imperceptibility have been kept as the focus of interest in the scope of this study. Besides, significant capacity rates have been obtained by each move. The performed experiments support these claims.

Keywords: DES S-Boxes, Game steganography, Game theory, Snake game, Steganography

1. GİRİŞ

Dijital bilgi devrimi, mesajı güvenli ve emniyetli bir şekilde göndermek için yeni zorluklar yaratmıştır. Hangi yöntem seçilirse seçilsin, en önemli soru güvenlik seviyesidir. Kriptografi, steganografi ve filigranlama gibi bilgi güvenliği konularına yönelik sayısız yaklaşım geliştirilmiştir. Filigranlama tekniğinin amacı, verideki bazı bilgileri gizleyerek belirli bir içerik üzerinde fikri mülkiyet hakları vb. için kanıt sağlamaktır. Kriptografi, bilgilerin güvenliğini sağlamak için bariz bir yaklaşım sağlar. Gizli mesajı karıştırır, böylece gizlice dinleyen kimseler için anlamsız olur. Bununla birlikte, şifrelenmiş içeriğin kendisi de dikkat çektiği için, pratikte her zaman yeterli değildir. Yeterli zaman ve araç göz önüne alındığında, şifreleme algoritması ne kadar güçlü olursa olsun kırılabilir. Dahası, bazı durumlar, iletişimin gerçekleştiğini hiç kimse fark etmeden bilgi göndermeyi gerektirir. Bu gibi durumlarda steganografi cevaptır [1].

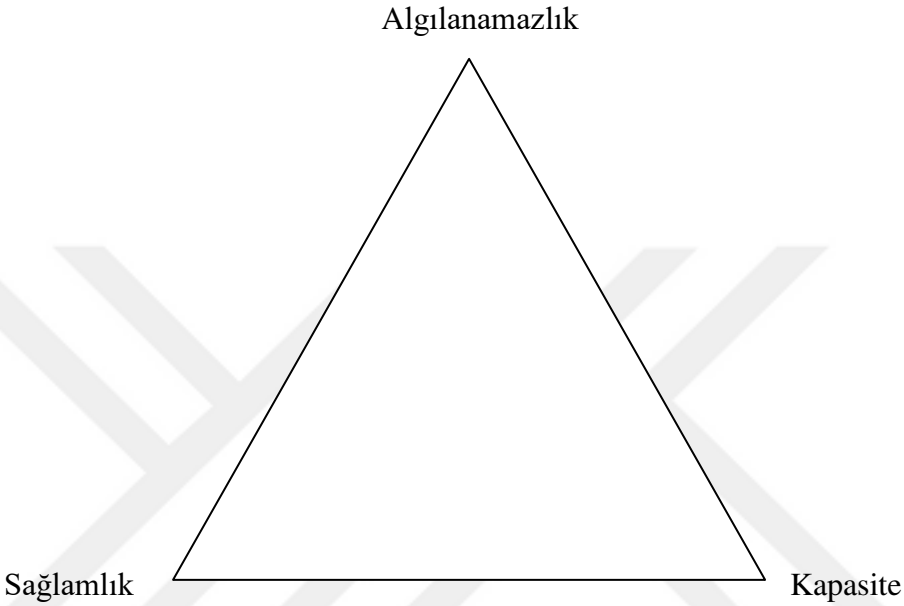
Şifreleme veriyi kullanılamaz bir formata dönüştürüp verinin aslına ulaşılmasını zorlaştırsa da yapılacak herhangi bir kripto-analiz atağını önleyemediği durumlar olabilmektedir. Ayrıca elektronik ortamlarda iki uç arasında şifreli bir iletişim yapıldığı anlaşıldığında ise iletişimi engelleme yoluna gidilebilmektedir. İşte bu noktada steganografi bilimi gündeme gelmektedir.

Veriyi diğer bir verinin içine gizleyerek veya gömerek görünmez yapma tekniğine steganografi denilmektedir. Veriyi gizleme amacıyla kullanılan bu diğer veri parçasına örten ortam ya da taşıyıcı denir. Gizlenmiş veriyi içeren bu örten ortama ise stego nesne denilmektedir ve stego nesne, saklanabilmekte ya da iletilebilmektedir. Gizli veri değişik çeşitlerde örten ortamlara gömülebilmektedir. Stego görüntü veya örten görüntü, verinin bir görüntü dosyasına gömülmesi sonucunda oluşan nesnedir. Örten metin, stego görüntü, örten ses, stego ses, örten video, stego video vb. isimlendirmelerde benzer şekilde oluşmaktadır.

Veri gizleme tekniği, mesajları görüntüler, videolar, haritalar, metin vb. gibi dijital medya ortamları içine gizlemektedir. Veri gizleme tekniği kriptolojinden farklıdır. Kriptolojide, mesajı şifrelemek için bir şifreleme düzeni kullanılmakta ve alıcıya daha güvenli ve tahmin edilemeyen bir mesaj gönderilmektedir. Ancak içeriği dolayısıyla

herkes iletişim sırasında mesaj değişiminin farkında olduğundan, kriptolojide saldırıları çekme bakımından her zaman bir tehdit vardır.

Bir veri gizleme sisteminin en önemli gereksinimleri algılanamazlık, sağlamlık ve kapasite olarak bilinmektedir. Şekil 1.1'de gösterildiği gibi bu gereksinimlerin her biri, bir veri gizleme sistemindeki sihirli üçgenin köşelerini temsil etmektedir ve bu çakışan gereksinimler arasında her zaman bir ödünleşim mevcuttur [2].



Şekil 1.1. Veri gizleme sistemindeki sihirli üçgen [2].

Bu gereksinimlerden herhangi birine yaklaşılması durumunda diğer ikisinden uzaklaşılmaktadır. Buna göre önerilen metot ile kapasite ve algılanamazlık arasındaki denge kurularak, kullanılan şifreleme algoritmaları ile de sağlamlık ve güvenlik desteklenmektedir. Bu noktada, saklanacak bilgi miktarı bakımından belli bir oranın üzerine çıkılması sağlamlık bakımından sorun teşkil etmemekte, kapasite bakımından da makul değerleri vermekte ancak algılanamazlık bakımından sorun teşkil etmektedir. Başka bir deyişle, gizlenecek bilgi miktarı arttıkça, karşı tarafa gönderilecek mesaj uzunluğu artmaktadır. Çok uzun olan mesajlar, alıcının oyundaki yeteneğine göre sorun teşkil edebilir.

Kapasite, örten ortama gömülebilen verinin bit miktarını ifade etmektedir. Güvenlik, bir gözlemcinin saklı bilgiyi çıkarma becerisiyle ilgilidir. Sağlamlık ise saklı bilgiyi modifiye etme veya yok etmeye karşı direnme imkânı ile alakalıdır [3].

Steganografi zararsız gözüken taşıyıcılar (görüntüler, ses dosyaları, metin vb.) içinde bir bilginin varlığını gizleme sanatı ve bilimi veya iletinin varlığının tespit edilemediği bir şekilde iletişim kurmaktır [4]. Tespit edilememe ve gömme kapasitesi gibi iki önemli özelliği bir steganografik algoritma tasarlarken göz önünde bulundurulmalıdır [5]. Bu iki özellik arasında her zaman bir ödünleşim vardır. Ayrıca steganografi yöntemlerinin başarısı, dikkat çekmemesi adına, taşıyıcı ortamına bağlıdır [6].

Çizelge 1.1. Steganografi, Filigran ve Kriptolojnin karşılaştırılması.

Kriter/metot	Steganografi	Filigran	Kriptoloji
Taşıyıcı	Herhangi bir sanal ortam	Çoğunlukla görüntü ya da ses dosyaları	Genelde metin bazlı bazı eklemeler ile görüntü dosyaları
Gizli veri	Yük	Filigran	Düz Metin
Anahtar	İsteğe bağlı	-	Şart
Giriş dosyaları	Kendi içinde gömülü bir dosya yoksa, en az iki tane	-	Bir
Algılama	Kör	Genelde aydınlatıcı (yani geri dönüşüm için orijinal filigran ya da örten nesne gerekli)	Kör
Doğrulama	Verinin tamamı	Genelde çapraz bağıntı ile	Veri koruma
Amaç	Gizli iletişim	Telif hakkı koruma	Veri koruma

Çizelge 1.1 (devam). Steganografi, Filigran ve Kriptolojnin karşılaştırılması.

Sonuç	Stego dosyası	Filigranlanmış dosya	Şifreli-metin
Amaç	Algılanabilirlik\ kapasite	Sağlamlık	Sağlamlık
Saldırı şekilleri	Steganaliz	Görüntü işleme	Kriptal analiz
Görünürlük	Asla	Bazen	Daima
Zayıflık	Fark edildiğinde	Değiştirildiğinde ya da kaldırıldığında	Şifre kırıldığında
Örtü ile bağıntı	Örten nesne ile zorunlu bir ilgisi bulunmamaktadır. Gizli mesaj örten nesneden çok daha önemlidir.	Genelde örten görüntünün bir niteliğini haline gelir. Örten nesne, mesajdan fazla önem taşır.	Mevcut değil
Esneklik	İstenen taşıyıcı seçilebilir	Taşıyıcı nesne seçimi kısıtlıdır.	Mevcut değil
Geçmiş	Çok eski, sayısal hali hariç.	Modern çağ	Modern çağ

Steganografide, gizli bilgi öyle bir şekilde gömülmelidir ki, gönderici ve hedeflenen alıcı dışında hiç kimse gizli bir mesajın varlığını fark edememelidir. Ayrıca, gizli mesajın varlığı neredeyse herhangi bir üçüncü şahıs tarafından tespit edilmemelidir. Yani güvenli steganografi, gizli verinin hedefe tespit edilmeden ulaştırılmasını gerektirmektedir. Çizelge 1.1'de steganografi, filigranlama ve kriptolojinin detaylı bir karşılaştırılması görülmektedir.

Verinin saklanabileceği çeşitli sayısal taşıyıcı veya yer vardır. Veri gürültü gibi algılanamaz seviyelerde dosyalara gömülü olabilir. Görüntülerin özellikleri parlaklık, kontrast ve renk dahil olmak üzere işlenebilir. Ses dosyalarına küçük yankılar veya hafif geciktirmeler eklenebilir veya üstü kapalı sinyaller yüksek genlikli sesler ile gizlenebilir. Bilgiler, satırların veya kelimelerin konumlarını değiştirerek belgelerde gizlenebilir. HTML (Hyper Text Markup Language) dosyaları yazıldığında web tarayıcıları boşlukları, sekmeleri, belli karakterleri ve ekstra satır aralarını göz ardı eder.

Bu durum bilginin gizlenmesi için bir konum olarak kullanılabilir. Örneğin, iletiler metinden her bir kelimenin ikinci harfi alınarak ve bu harfler gizli ileti üretmek için kullanılabilir. Buna boş şifre veya açık kod denir. Bilgi belgenin yerleşiminde de gizlenebilir. Örneğin, bir metin parçasındaki belli başlı kelimelerin konumları hafifçe kaydırılabilir ve bu kaydırılmış kelimelerden gizli bir mesaj oluşturulabilir. Duraksamalar ve boğaz temizlemek gibi bir dilin konuşulması tarzı kodlanabilir [7].

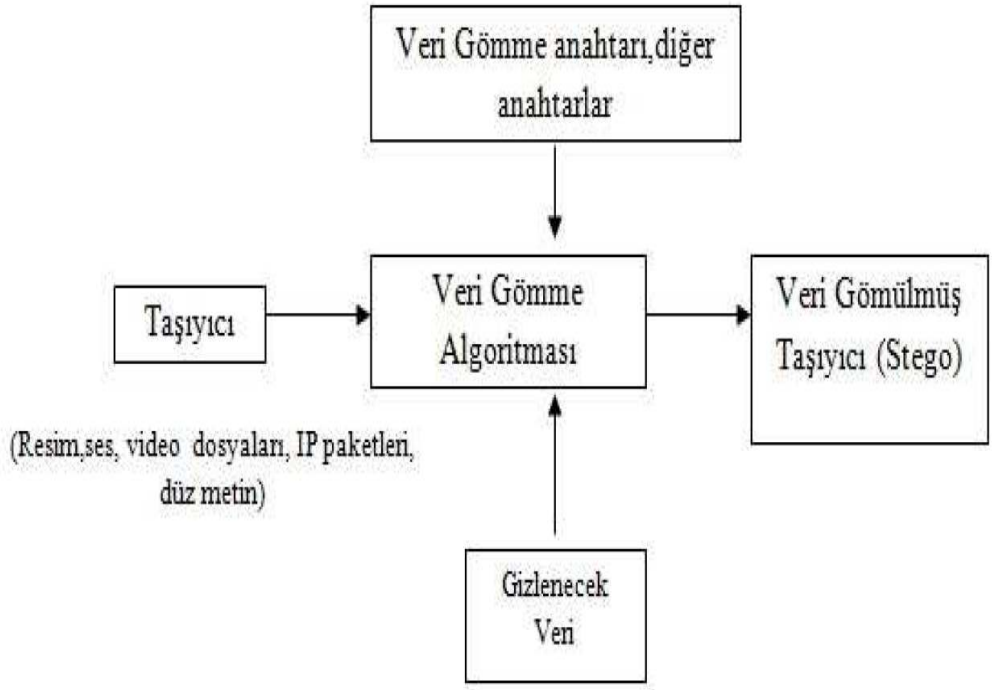
Steganografinin bilgisayar dünyasında kullanımı başlıca iki temel prensibe dayanır. İlki, veri içine veri gömmek ve ikincisi ise görüntü veya ses dosyaları içine veri gizlemektir. Bunda yararlanılan başlıca prensiplerden bir tanesi; görüntü veya ses dosyalarının içeriklerinin, görüntüye ya da sese zarar vermeksizin bir dereceye kadar değiştirilebilmesidir. Yaygınca kullanılan diğer prensip ise insan duyularının görüntü, ses ya da renkte ufak değişiklikleri fark edememesidir. Fotoğraf, ses, video gibi saklamada kullanılacak veriler, gizli veriye göre oldukça büyük olduğu için, veri gizlemek oldukça kolay olur. Gizlenecek mesajlar büyük verilerden oluşan fotoğraf gibi dosyalarda, internette ve diğer iletişim araçlarında yaygınca kullanılır. Örneğin, fotoğraflardaki her pikselde, her bir 8 bit kırmızı, yeşil ve mavi rengi gösterecek şekilde 24 bitlik bir harita kullanılır. Sadece mavi için, 2^8 tane farklı mavi renk vardır. 11111111 ve 11111110 ile gösterilen iki mavi arasındaki fark, insan gözüyle saptanabilecek türden değildir. Bu sebeple en az öneme sahip bit (LSB–Least Significant Bit) olarak adlandırılan bu teknik, steganografi içinde yaygınca kullanılır.

Steganografinin başka kişilerce çözülmesini engellemek amacıyla yapılması gereken en önemli şey; orijinal veri (örtü verisi) ile gizleme işleminden sonra oluşan veri arasındaki değişikliklerin istatistiki olarak ya da gözle fark edilemiyor hale getirilmesidir. Diğer bir deyişle, orijinal veri üzerinde eşik değerinden daha düşük değişiklikler yaparak steganografi başarıya ulaşmış olur. Bu da ancak orijinal verinin yüzeysel sinyal değerinden daha büyük (hacimli) olmasıyla sağlanabilir. Örneğin, kayıpsız sıkıştırma metoduyla verilerin sıkıştırılıp, en az zararla tekrar çıkarılmaya çalışıldığı fotoğraflarda (JPEG-Joint Photographic Experts Group gibi) steganografik kullanım oldukça yaygındır. Çünkü kayıp olmaksızın veri sıkıştırması yapmayı hedefleyerek hemen hemen tüm multimedya (müzik, video, fotoğraf) araçlarında kullanılan bu metotta, elde edilen ufacık hatalar bile steganografi yapmaya yeterli olabilir. Üstelik steganografi uygulanmış dosyalar tek başlarına masum gözükürken, fark ancak orijinali ile yan yana getirildiğinde anlaşılır.

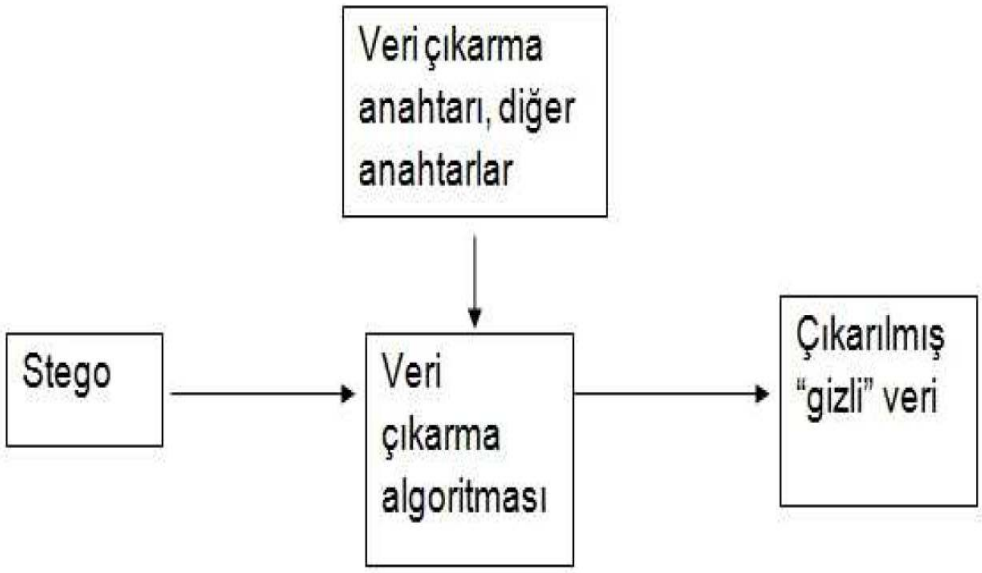
Steganografi, dijital bir taşıyıcı (müzik, fotoğraf, video gibi) içine bilgi gömme işlemi olarak tabir edilen bir dijital filigran uygulamasıdır. Zira "dijital filigran"da alıcı ve vericinin orijinal veri içine gömülü gizli bir mesajla haberleşmesi sağlanabilir. Fakat dijital filigran, ticari bir müzik ya da yazılım ürünü olan orijinal verinin steganografide olduğu gibi bozulmasına izin vermemesi nedeniyle steganografiden ayrılır.

Resim içine yazı gizlemek de yine çok kullanılan steganografik bir yöntemdir. Fotoğraf içinde renkler için ayrılan fakat kullanılmayan alanlar veri gizlemek için idealdir. Örneğin, her fotoğraf başlık ve piksellerden oluşur. Küçük bir fotoğraf bloğu olan her pikseldeki renk; 3 ana rengin (kırmızı, yeşil, mavi) karışımından elde edilir. Heksadesimal (16 tabanlı sayı sistemi) formatta FF-FF-FF ile ifade edilen beyaz renk; binary (2 tabanlı sayı sistemi) olarak 11111111-11111111-11111111 ifade edilir. Bunun en az öneme sahip bitleri değiştirilerek insan gözü algılayamadan steganografi yapılmış olur. 800*600 boyutlarında bir fotoğrafta 800×600=480.000 adet piksel, 480.000×3 bit = 1.440.000 bit = 175,7 kilobayt olduğunu düşünülürse gizlenecek veri için kalan yer oldukça fazladır [8].

Steganografide önemsenen nokta, verinin varlığının gizlenmesidir. Verinin varlığı ne kadar iyi gizlenebilirse, taşınacak veri o kadar güvendedir. Sıradan bir resim veya müzik dosyası kimsede kuşku uyandırmazken, içinde çok gizli bilgiler taşıyor olabilir. Alıcı dahil hiç kimse anahtar bilgi olmadan, verinin nerde saklandığını bilmeden, bundan kuşkulanmaz. Bu yüzden steganografide, alıcının elinde, verinin hangi kanalla taşınacağı ve mesajın nasıl çözülebileceği bilgileri olmadan verinin karşı tarafa iletilmesi hiçbir önem taşımaz. Şekil 1.2 ve Şekil 1.3'te veri gömme ve çıkarma prosedürleri görülmektedir.



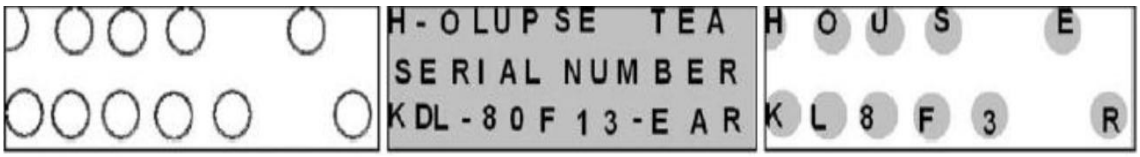
Şekil 1.2. Steganografide veri gömme prosedürü [9].



Şekil 1.3. Steganografide gizli veriyi çıkarma prosedürü [9].

Steganografi sözcüğü köken olarak "gizli yazı " anlamına gelen Yunanca kelimelerden türetilmiştir. Binlerce yıldır çeşitli şekillerde kullanılmaktadır. M.Ö. 5. yüzyılda Histaiacuss, bir kölenin başını tıraş ettirmiş, kafatasına bir mesajı dövme yaptırmış ve saçları tekrar uzadıktan sonra köle, kafasındaki mesajla birlikte gönderilmiştir.

Beş yüzyıl önce, İtalyan matematikçi Jerome Cardanre eski bir Çin gizli yazı yazma metodu keşfetmiştir. Buna göre, iki taraf arasında delikli bir kâğıt maske paylaşılmıştır. Bu maske boş bir kağıt üzerine yerleştirilmiş ve gönderici gizli mesajı deliklerin içinden yazmıştır. Daha sonra, Şekil 1.4'te görüldüğü gibi gizlenmiş metnin şüphe uyandırmaması amacıyla maskeyi kaldırılmış ve boşluklar doldurulmuştur. Bu yöntem, Cardan'a atfedilmiştir ve Cardan Grille olarak adlandırılmaktadır.



Şekil 1.4. Cardan Grille [10].

Ayrıca II. Dünya Savaşı sırasında Almanların mikro noktalar gibi çeşitli steganografik yöntemler icat ettikleri bilinmektedir. Bununla birlikte görünmez mürekkep ve boş şifreleri tekrar kullandıkları rapor edilmiştir. Örnek olarak, bir Alman casusu tarafından II. Dünya Savaşı sırasında gönderilen bir mesaj aşağıdaki gibidir:

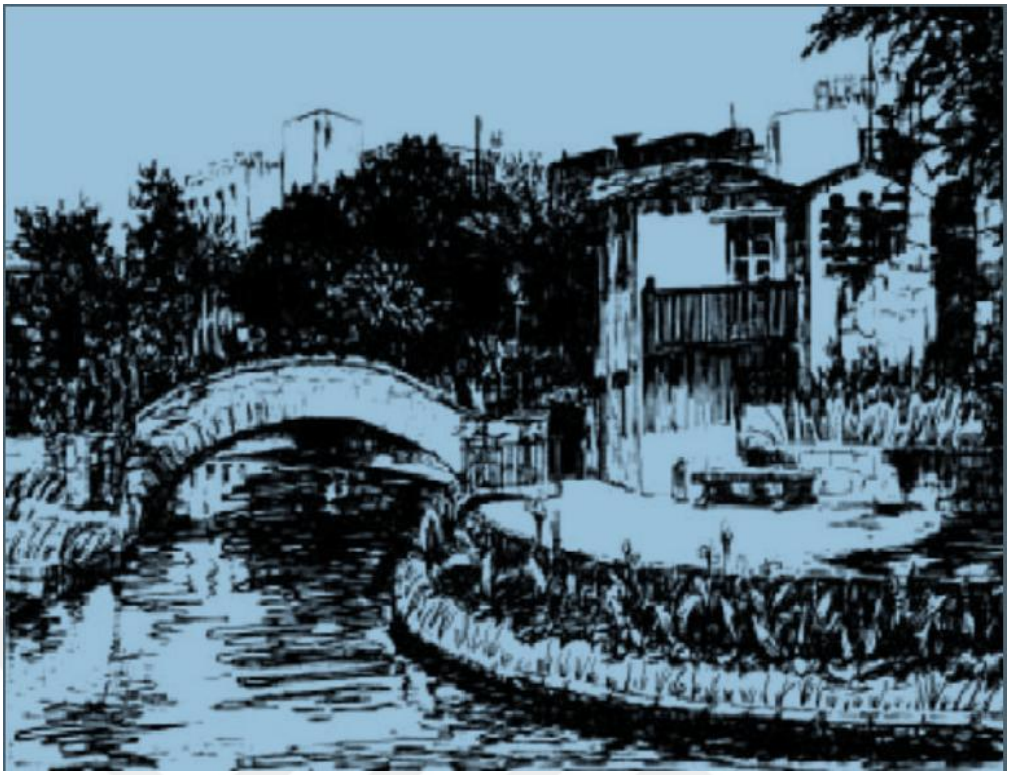
"Apparentlyneutral's protest is thoroughlydiscountedandignored. Isman hard hit. Blockadeissueaffectspretextforembargo on by-products, ejectingsusetsandvegetableoils [11]."

Bu metinde her bir kelimenin ikinci harfini ele alarak gizli mesajı çıkarmak mümkündür:

"Pershingsailsfrom NY June 1 [11]."

1945 yılında, Morse kodu Şekil 1.5'te görülen bir çizimde gizlenmiştir. Gizli bilgiler nehir kıyısında uzanan çimler üzerinde kodlanmıştır. Burada uzun çim bir çizgi, kısa çim bir noktayı göstermektedir. Buna göre gizlenen mesaj:

''Compliments of CPSA MA toourchiefColHarold R. Shaw on his visitto San Antonio May 11th 1945 [11]."



Şekil 1.5. Mors kodunun görüntü içerisine gizlenmesi [10].

Bilgisayar ve internet gücündeki gelişmelerle birlikte dijital sinyal işleme (DSP-Digital signal processing), bilgi ve kodlama teorilerinin gelişimi ile steganografi dijital platformda uygulanabilir hale gelmiştir. Bu dijital dünya alanında steganografi, çeşitli ilginç uygulamaları ortaya çıkararak dikkatleri üzerine çekmiş ve böylece devam eden evrimini garantilemiştir. Müzik dosyaları, HTML dosyaları, çalıştırılabilir dosyalar (.exe-Executable uzantılı dosyalar) ve genişleyebilir işaretleme dili XML (Extensible Markup Language) dosyaları gibi daha basit formdaki dosyaların içine bile veri gizleme işleminin yapıldığı örnekler mevcuttur [12].

Genel olarak, popülerlik nedeniyle internet üzerinden görüntü, ses ve video transferi, taşıyıcı olarak kullanılmaktadır. Bununla birlikte, internetin hızlı büyümesi nedeniyle çeşitli yeni medya uygulamaları geliştirilmiştir. Örneğin, kullanıcılar, arkadaşları ile çevrimiçi oyun oynayabilmekte, arkadaşlarının mobil cihazlarına bulmaca gönderebilmektedirler. Niwayama ve arkadaşları tarafından gerçekleştirilen çalışmada veri gizlemek için taşıyıcı ortam olarak labirent oyunları seçilmiştir. Ancak bu yöntemin iki dezavantajı vardır: Biri çok az miktardaki gömme kapasitesi, diğeri stego labirentin mükemmel olmamasıdır. Lee ve arkadaşları tarafından, bu metodun dezavantajları üzerinde çalışılmıştır. Gömme kapasitesinin artırıldığı ve mükemmel labirentin oluşturulduğu yeni bir metot önermişlerdir. Öne sürülen yöntemin ana fikri daha çok

gömme kapasitesi elde etmek için tek bir çözüm yolu yerine çok yollu bir çözüm düşünmektir [13].

Jing Yang ve Chen değişik animasyonlarla PowerPoint dosyası içine gizli bir mesajı gömmek için bir yöntem önermişlerdir. Önerilen metotta, farklı mesajları temsil etmek için animasyonlar kullanılmıştır. Bu amaca ulaşmak için, ilk olarak animasyonlar ve mesaj parçaları arasındaki ilişkiyi kaydedecek bir kod defteri tasarlanmıştır. Buna ek olarak, bir PowerPoint dosyasındaki animasyonların otomatik olarak uygulanması imkânsızdır ve pratik değildir. Daha sonra bu oluşturulan kod defterine göre, gizli mesajın yarı otomatik olarak animasyonlara çevrilmesi amacıyla interaktif bir sistem tasarlanmıştır. Burada herhangi bir animasyon, PowerPoint dosyasının içeriğini değiştirmediğinden, bu dosyanın gerçek içeriği bozulmadan muhafaza edilebilmektedir. Ayrıca, önerilen metot format dönüştürme saldırılarına karşı dirençlidir. Ancak kullanılan animasyon sayısı fazla olmadığından bu metodun kapasitesi düşüktür [14].

Web tabanlı iletişim büyük bir miktarda bant genişliğine sahiptir ve bu nedenle gizli iletişim için kullanılabilmektedir. HTML ve XML web geliştirme için iki önemli temel ve evrensel araçlardır. Script dilleri de, dinamik web geliştirme için kullanılabilir ancak sonunda tüm tarayıcılar script kodunu HTML formatında komut dosyasına çevirmek zorundadır. Mir ve Hussain birkaç metin steganografi metodunu, XML dosyalarına uygulayarak veri gizleme gerçekleştiren bir metot önermişlerdir [15]. XML sayfası, taşıyıcı ortam olarak kullanılmıştır ve veri gizlenmeden önce güvenliğin artırılması amacıyla Gelişmiş Şifreleme Standardı (AES-Advanced Encryption Standard) algoritması ile şifrelenmiştir. XML içerisine, aynı işlevi yerine getiren etiketlerin kodlanmasıyla veri saklanabilir. Örneğin, imge etiketin için <img></img> yazımı ile <img/> yazımı aynı işlevi görmektedir. Bu durumda <img></img> 1, <img/> ise 0 olarak kodlanacak olursa aşağıda verilen XML kodu içerisine 10001001 bitlerinden oluşacak bir karakterlik bir veri saklanmış olacaktır.

<imgsrc=”resim1.jpg”></img>

<imgsrc=”resim2.jpg”/>

<imgsrc=”resim3.jpg”/>

<imgsrc=”resim4.jpg”/>

<imgsrc=”resim5.jpg”></img>

<imgsrc=”resim6.jpg”/>

<imgsrc=”resim7.jpg”/>

<imgsrc=”resim8.jpg”></img>

Sui ve Luo, hiper metin (hypertext) içerisine biçimleme (markup) etiketlerinin pozisyonlarını değiştirerek veri sakladıklarını rapor etmişlerdir [16]. HTML kodlu web sayfalarında kullanılan etiketler (tag) aracılığıyla sayfanın görüntüsü bir biçimleme programlama diliyle şekillendirilir. HTML’de etiketlerin açılış ve kapanış bölümleri bulunur. Bir metne ait birden fazla etiket varsa bunların kapanış bölümlerinin sırası önemsizdir. Diğer bir ifadeyle bunların sırası oluşan görüntüyü etkilemez.

Örneğin;

<tdwidth=”25%”><u>DÜZCE</u></td>

satırı ile

<tdwidth=”25%”><u>DÜZCE</u></td>

satırı aynı görüntüyü oluşturacaktır.

HTML etiketlerinin bu özelliğinden faydalanılarak steganografik uygulamalar geliştirilebilir.

Castiglione tarafından gerçekleştirilen çalışmada, istenmeyen (spam) e-postalar, internet üzerinden etkili, esnek ve eş zamanlı olmayan gizli iletişim kanalları uygulamak için ilginç bir fırsat sunmaktadır. İlk olarak, spam mailler birer e-postadır ve yıllarca taşıdıkları protokollere dayanmakta ve hala bu protokolleri taşımaktadırlar. Tüm e-posta yaşam döngüsü ile ilgili protokoller gizli verileri kodlamak için pek çok boşluk öneren Bilgi dönüşümü için, Amerikan Standart Kodlama Sistemi (ASCII-American Standard Code Information Interchange) kontrol dizgileri üzerine inşa edilmiştir. İkincisi, spam mailler rutin olarak çıkarılmakta ve bunun yanı sıra onları spam olarak sınıflandırmak için herhangi bir itina gerektirmemektedir. Bu, gelişmiş güvenlik duvarları ve trafik analizörleri tarafından bile algılanabilir olmayan sağlam, gizli bir iletişim imkanı sunmaktadır. Önerilen steganografik sistem, ne ilgili taşıma protokolleri ve mekanizmalarını etkilemekte ne de örten e-posta iletisi içeriğini değiştirmektedir. Buna ek olarak, son kullanıcılara kadar fark edilebilir herhangi bir performans düşüşü veya veri kaybına neden olmamaktadır [17].

Sohbet odaları vasıtasıyla iletişimin, insanların yaşamında oldukça popüler bir hale geldiğini gören Wang ve Chang 2009 yılında yeni bir metin steganografi metodu önermişlerdir. Bu metotta gizli bilgi, sohbet odalarında internet üzerinden iletişim esnasında yüz mimiklerini ifade eden küçük boyutlu görüntüler yani emolojiler içerisine gömülmektedir. Metotta öncelikle, göndericinin ve alıcının ikon tablosunun aynı olması gerekmektedir. Daha sonra, gönderici bu ikonları anlamlarına göre (gülümseme, gülme, ağlama vb.) farklı kümelere ayırmaktadır. Her bir emoloji yalnızca bir kümeye ait olabilmektedir. Sıfırdan başlayarak bir ikonun kendi kümesindeki sıra numarası, gömülecek gizli bitleri göstermektedir. Bu nedenle önerilen steganografik metot, her bir kümedeki ikon sırasını kontrol etmek amacıyla gizli bir anahtar kullanmaktadır. Gizli anahtar sadece alıcı ve gönderici tarafından tutulmaktadır. Sohbet odalarında kullanılan çok fazla sayıda ikon olduğundan bu metotla kapasite oldukça artırılsa da, bu artış büyük ölçüde önceden paylaşılan emoloji tablosuna ve her bir kümedeki ikon sayısına bağlı olacaktır [18].

Samphaiboon ve Dailey, 2009 yılında yeni bir steganografik metot geliştirmiştir. Geliştirilen metotta, gizli mesaj, televizyon ve web siteleri gibi medya ekranlarında kısa bir metin dizisi içerisinde çoklu alıcıya gönderilmektedir. Ancak bu yöntemde, uygun OCR(Optik Karakter Tanıma) biriminin kod çözücüde bulunduğu varsayılmaktadır. Metot, Tayland dili üzerinde uygulanmıştır ve gömme aşamasında, etkili birkaç metinden bite dönüşüm metodu önerilmiştir. Bu metodun en büyük avantajı, gizli mesajın aynı anda farklı yerlerdeki çoklu alıcılara yayınlanabilmesidir. Metodun dezavantajlarından birisi ise yazar tarafından, göndericinin kısa metnin iletildiği kanal üzerinde kontrole sahip olduğu varsayılmaktadır. Bir diğer kaçırılmaması gereken nokta ise görüntülenen metni tanıyabilen ve bunu makine tarafından okunabilir forma çeviren metinsel görüntü okuma biriminin var olduğunun kabulüdür [19].

Buna uygun olarak [20] MP3 sıkıştırma standartlarının sınırları içerisinde tasarlanmış en yeni sesli steganografi örneklerinden biridir. [21-23] benzer arka ve ön zemin yapılarından dolayı bir metin belgesi içine veri saklama zor olduğu için literatürdeki kısıtlı yeni metin steganografisi yöntemlerindendir. [24], [25] ise yeni bir alanın örnekleridir; veri saklama için IP paketleri kullanan ağ steganografisidir. Ayrıca [26] ve [27] gibi çok yönlü çalışmalar da vardır. [26]'da gizli ileti hiçbir animasyonun PowerPoint dosyası içeriğini değiştirmediği gerçeğinden yararlanılarak, PowerPoint'teki animasyonların kullanımı ile gömülmüştür. [27]'de JPEG görselleriyle

Word dosyaları içerisinde bilgi transferi için yeni bir sistem öne sürülmüştür.

Oyunların kullanımı ise steganografinin bir başka kullanım alanıdır. Literatürdeki bazı kısıtlı çalışmalar aşağıdaki satırlarda açıklanmıştır. Hernandez-Castro ve arkadaşları 2005 yılında gizli veriyi saklamak için oyun açıklamalarını ve hareketlerini kullanan bir oyun steganografisi sunmuştur ve Satranç, Tavla, Go vb. oyunlar üzerine yoğunlaşmışlardır. Ana fikir, belli bir eşik değerin üzerindeki tüm hareketler için oyundaki her bir hamle konumunu hesap etmek ve sonrasında gerçekte yapılan hamle seçmesi içindeki gizli iletinin bazı bitlerini şifrelemektir [28].

2009 yılında, Desoky, Chestega adında bir oyun steganografisi yöntemi öne sürdü. Chestega eğitim belgesi, oyun analizi, haber metinleri gibi satranç ile alakalı örtüleri kullanıyordu. Gizli ileti ise üç adımda saklanıyordu: Öncelikle steganografik kodun sabitlenmesi adına satranç tahtası, taşlar, hamleler vb. kodlama parametrelerinin belirlenmesi için oyunun açısı seçilir. Bu esnada, bağlantılı taraflar bu parametrelerde mutabık kalmalıdır. İkinci olarak gizli ileti bu kodlama parametreleri ile gizlenir. Taraflar bu gizli iletinin hiçbir bozulmaya sebep olmadığını ve Chestega'nın güvenilirliğinin tekniğin gizliliğine bağlı olmadığını ve stego-anahtara gerek duymadığını belirtmiştir [29].

2010'da Lee ve arkadaşları mükemmel labirent kavramı kullanarak steganografik bir yöntem tasarladı. Dikdörtgen labirent m×n labirent (m genişliğinde hücreler ve n yüksekliğinde hücreler) olarak adlandırılır. Herhangi bir iki hücre arasında sadece ve sadece bir yol varsa labirente mükemmel denir. Önerilen yöntemin esas fikri, daha fazla saklama kapasitesi elde etmek için tek bir çözüm yolundan ziyade çoklu yolları düşünmekti. İlk önce HKMG (Hunt-and-Kill Labirent Generating) algoritması ile mükemmel bir labirent oluşturuldu. Ardından, başlangıç hücreleri olarak bazı hücreleri ve çoklu yollardan ortak uç olarak birini seçtiler. Sonunda, karşılık gelen çoklu yolları elde etmek için mükemmel labirenti çözümlediler ve başlangıç hücrelerine göre yukarıdan aşağıya ve sonra soldan sağa doğru emirler verildi. Yol dizisi göz önüne alındığında, yerleştirilen hücrelerin bir dizisini elde etmek ve tüm yerleştirilebilir hücreleri bulmak için başlangıç hücresindeki her yolu izlediler. Ardından, veriler bu sıraya göre gömülmüştür [30].

2012'de Philip C.Ritchey ve Vernon J. Rego Tic Tac Toe oyununa dayanan steganografik bir yöntem öne sürmüşlerdir. Satranç gibi iki oyuncuyla oynanır.

Kombinatoryal bir yöntemdir. Bu yöntemde oyuncunun hangi hareketi yapacağını seçmesi gerekir. Daha sonra kalan seçeneklere gizli mesaj yerleştirilir. Ayrıca gizli mesajın kapasitesi oyun stratejisine bağlıdır [31].

2014'te Ou ve Chen çevrimiçi tetris oyunlarına dayanan steganografik bir yöntem öne sürmüştür. Bu yöntemde, gizli mesaj, tetris bulmaca parçası, tetrimino dizisi kullanılarak gömülmüştür. Önerilen yöntem her oynanan oyun için ayrı bir stego edilmiş tetrimino dizisi oluşturmuştur. Yöntemin senaryosu şudur: Bir gönderici öne sürülen gömme yöntemini kullanarak internete bir tetris oyunu yükler ve herkes bu oyunu oynayabilir. Alıcı, oyun sırasında gizli mesajı almak için önerilen çıkarma yöntemini kullanır, hiçbir oyuncu veya yönetici gizli iletişimin farkında değildir [32].

Bu çalışmada, yılan oyunu içinde steganografi önerilmiştir. "Vitamin" olarak adlandırılan yemin her hamlesini hesaplayarak oyunun içine gizli veriler yüklemek amaçlanmıştır. Başka bir deyişle, gizli verilerin bitlerine göre vitaminin koordinatları hesaplanır. Aynı zamanda oyun platformunu karmaşıklaştırmayı ve DES (Data Encryption Standart-Veri Şifreleme Standardı) S-kutuları (S-Boxes–Substitution-Boxes) kullanarak oyun platformunu karmaşıklaştırma ve gizli verilerin bitlerini aynı anda şifreleme planlanmıştır. Bu işlemler, önerilen şemayı olası steganografik saldırılara karşı daha dirençli hale getirir ve çıkarım prosedürü daha karmaşıktır. Bu nedenle, güvenlik sorunu bu çalışma kapsamında güçlendirildi. Gizlenme prosedürü, vitaminin konumu yoluyla gerçekleştirildiği için oyunun algılanamazlığı, vitaminin hamlelerinin rastlantısallığına bağlıdır. Bu, S-kutularını kullanarak oyunu karmaşıklaştırmanın ana nedenidir.

Bu tez çalışmasının geri kalan kısmı beş bölüm olarak düzenlenmiştir. İkinci bölümde, kullanılan kavramlar (oyunlarda bilgi gizleme, yılan oyunu ve S-kutuları) hakkında kısa bir bilgi sunulmuştur. Bölüm 3'te önerilen şema hem gömme hem de çıkarım aşamalarını belirtmek suretiyle açıklanmıştır. Bölüm 4'te deney sonuçları ve önerilen yöntemin kapasite, algılanamazlık ve güvenlik açısından analizi yapılmıştır. Son olarak, 5. bölümde genel bir sonuca varılmıştır.

2. KAYNAK ARAŞTIRMASI

Bu bölümde çalışmanın kapsamında kullanılan metodolojilerden bahsedilmiştir. Öncelikle öne sürülen planın temelini yansıtması için oyunların içine bilgi saklama yolları açıklanmış ve kullanılan oyun platformu olan "yılan" anlatılmıştır. Son olarak S-kutuları ve kullanımı tanımlanmıştır.

2.1. OYUNLAR YOLUYLA BİLGİ GİZLEME

Bilgisayar oyunları yalnızca çocukların yaşamında değil yetişkinlerin kültüründe de önemli bir rol oynamaktadır. Araştırmalar, bir kişinin normal bir okul gününde dijital oyunları oynarken geçirdiği ortalama sürenin iki buçuk saat olduğunu belirtir [33]. Bu çalışmada, bu geniş kullanım göz önüne alınarak steganografide oyun platformu tercih edilmiştir. Bu bölümde oyunlara bilgi saklamanın temel yöntemleri araştırılmıştır. Oyun kullanarak bilgi gizleme, yeni bir oyunu baştan sona oynayarak veya daha önce oynamış bir oyuna ek bilgi ekleyerek iki yaklaşımla gerçekleştirilebilir.

2.1.1. Yeni Oyun Oynamak

Bu yöntemde, iletişim kanalının her iki parçasının da birebir aynı yazılıma erişime ve (saklı içeriği deşifre etmek için kullanılmak üzere) ortak bir gizli anahtara ve ayrıca, yazılımın iç durumunun her iki taraf tarafından da tekrar üretilebilmesini temin etmek amacıyla diğer bazı parametrelere (oyun boyutu, yazılım versiyonu vb.) sahip olması gerekir.

Ana fikir, belli bir eşik değerin üzerindeki tüm hareketler için, oyundaki belli bir T'nin (eşik değeri) üstündeki her bir hamlenin konumunu hesap etmek ve sonrasında gerçekte yapılan hamle seçmesi içindeki gizli iletinin birkaç bitini şifrelemektir. Söz gelimi, belirli bir konumda belirli eşik T'sinden (buna benzer olarak belli bir n numarası seçip en iyi n hamleleri listesinden bir hamle seçilebilir) daha kötü olmayan gm'ler (great moves - iyi hamleler) vardır. Sonrasında bu hamleler değerlerine göre (değerlendirme fonksiyonunu göz önünde tutarak) ayrılır ve i numarasının ikili temsilini şifrelemek için i. hamle seçilir. Böylece, her bir konumda log2(gm) bitlik bilgi saklanabilir. T'yi

artırarak gizlenen bitleri gömmek için, daha fazla gm olacağı için kanal kapasitesi de büyüyecektir. Bundan farklı olarak T'yi azaltmak, en iyiden büyük ölçüde sapmayan seçilmiş stratejiler için, gizli içeriğin daha yüksek görünmezliğe ulaşmasıyla sonuçlanacaktır. Ana fikir, belli bir eşik değerin üzerindeki tüm hareketler için oyundaki her bir hamle konumunu hesap etmek ve sonrasında gerçekte yapılan hamle seçmesi içindeki gizli iletinin birkaç bitini şifrelemektir. Söz gelimi, belirli bir konumda belirli eşik T'sinden (buna benzer olarak belli bir n numarası seçip en iyi n hamleleri listesinden bir hamle seçilebilir) daha kötü olmayan gm'ler, yani iyi hamleler vardır. Sonrasında bu hamleler değerlerine göre (değerlendirme fonksiyonunu göz önünde tutarak) ayrılır ve i numarasının ikili tabandaki temsilini şifrelemek için i. hamlesi seçilir.

İki oyuncu arasındaki oyunu iyi ve gerçek açılış (örneğin, oyunun başında çok kötü olmayan ama ortasında veya oyun sonunda güçlü olmayan hamleler) bilgileriyle simule etmek için rastgele dağılıma sahip veya zamanla değişen dinamik T kullanma gibi olasılıklarda mevcuttur. Alıcı bu hareketleri, aynı pozisyonda ikili veri olarak gelen hamle listesini yeniden hesaplamayla ve gerçekten oynanan hamledeki kodun araştırılmasıyla, kolaylıkla deşifre edebilir.

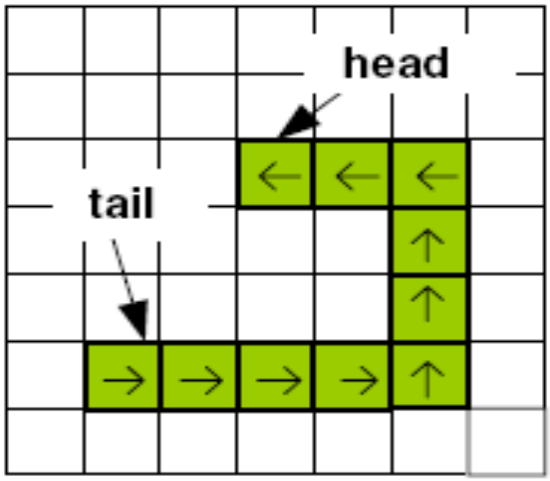
2.1.2. Oyuna Veri Eklemek

Burada temel fikir her bir hamlenin içine bazı bitler saklamak için basitçe Bölüm 2.1.1 açıklanan prosedürü izlemektir. Ancak bu yöntemdeki fark, hamlelerin oyunda gerçekten oynanan ana çizgideki değişkenlere karşılık gelmesidir. Oyundaki belli başlı konumlarda oynanmış ana çizgideki değişkenler tanıtılır. Her bir değişken birçok farklı şekilde bit gömebilir. Örneğin, değişkenin başlayacağı hamleyi, değişkenin uzunluğunu ve elbette, değişkenin her bir hamlesinde, hamlelerin içindeki gizli veriyi şifrelemek için yukarıda bahsi geçen algoritmayı kullanmayı seçebilir.

Bilgi gömmenin bir diğer olası kanalı ise oyun esnasında kullanıcı açıklamalarının dahil edilmesidir. Genellikle bu gömme tekniği yollayıcının ilkine göre çok daha fazla bilgi saklamasını sağlar. Ayrıca tespit edilmesi çoğu durumda daha zordur. Ancak daha düşük sağlamlık gibi önemli bir sorunu da vardır; gizli veriyi silmek için tüm açıklamaları silmeye yeterlidir ama bu, oyun dosyasının çekiciliğini ve yararlılığını ciddi ölçüde azaltır [6].

2.2. YILAN OYUNU

Yılan oyunda, birkaç yılan iki boyutlu bir boşlukta hareket ederek, vitamin olarak tasarlanmış bir nesneye ulaşmaya çalışır. Bir yılan, baş adı verilen özel bir ilk hücreden oluşur gövde olarak isimlendirilen diğer birkaç hücreden meydana gelmiştir. Eğer gövde de en az bir hücre varsa, dizinin son hücresine kuyruk denir. Hareket baş kısmı aracılığıyla kontrol edilir ve diğer hücreler sırasıyla önündeki komşusunu takip eder [34]. Hücreler vasıtasıyla modellenen yılan Şekil 2.1'de gösterilmiştir.



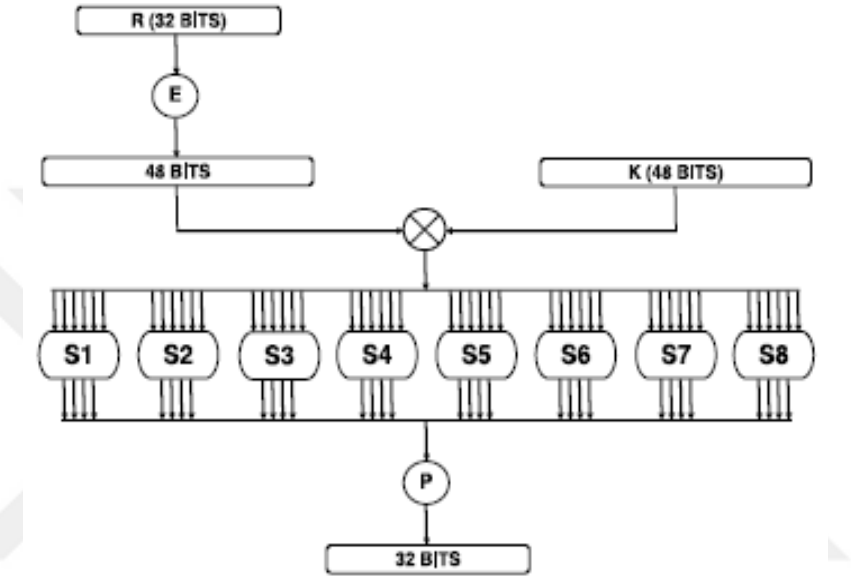
Şekil 2.1. Hücrelerden oluşan yılan biçimi [35].

Bir yılan başı vitamine ulaştığında, bu yılanın vitamini "yediği" söylenir. Bu durumda, bu yılanın gövdesi bir hücre büyür ve vitamin uzayın başka bir yerinde görünür. Hedef, önceden tanımlanmış bir uzunluğa ulaşana kadar yılanı daha uzun süre büyütmektir [34]. Bu çalışmada, oyunun bu özelliğinden yararlanılması amaçlanmıştır. Yani, gizli verilerin bitlerine göre vitaminin hareketi tahmin edilir (bkz. Bölüm 2.1.1.). Bu arada, oyun tahtasını S-kutularının yapısını göz önüne alarak daha karmaşık hale getirmek planlanmıştır. Bu işlem, önerilen şemayı muhtemel steganografik saldırılara karşı daha dayanıklı hale getirecek ve vitamin hareketleri için algılama yeteneği açısından arzu edilen rastlantısallığı artıracaktır.

2.3. S-KUTULARI

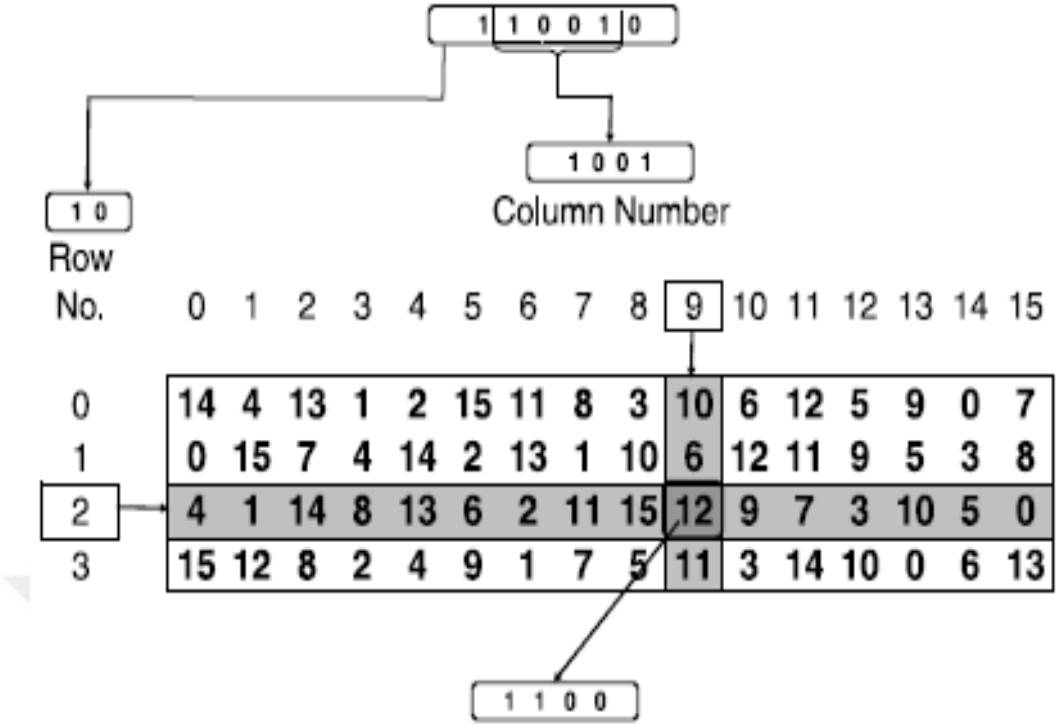
S-kutuları genellikle simetrik kripto sistemlerinde kullanılır. S-kutuları genellikle bu tür bir şifrenin tek doğrusal olmayan bileşenleridir. Bunlar güvenilirliğini ve doğrusal kripto analizini inceleyen güçlü yöntemlere karşı yerel direnç sağlar. S-kutularının

diferansiyel (farklılık gösteren) tekdüzelik değeri ve lineer olmayan tek düzelik değeri sırasıyla onun diferansiyel ve doğrusal kriptoanalizine karşı direncini ölçmede yaygın biçimde kullanılmıştır. Dolayısıyla, hem pratik hem de teorik açıdan temel soru çeşitli haritalandırma (S-kutuları) grupları için minimum değerin ne olduğudur. Ek olarak S-kutularının tasarımı için her iki değerinde küçük olduğu etkili haritalama sağlayan algoritmalara sahip olmak değerlidir. Yani S-kutularının üretimi diferansiyel ve doğrusal kripto analize karşı iyi bir direnç sağlar [36].



Şekil 2.2. DES'te S-Kutularının kullanımı.

Klasik S-kutuları, sayıların özel konfigürasyonundan oluşan tablolardır ve şifreleme sürecinde bilginin doğrusal olmayan dönüşümünün araçları olarak kullanılır. S-kutuları birçok blok şifrenin temel bileşenidir. S-kutuları sabit uzunluklu, bit süreli blok grupları üzerinde, sabit dönüşüm yardımıyla çalışırlar. Yakın zamanda kullanılan blok şifrelerin kalitesi sürekli geliştirildi veya yeni ve daha iyi yapılarla değiştirilmiştir. S-kutularının iyi bilinen uygulamalardan biri, Şekil 2.2'de gösterildiği gibi, 8 S-kutusu, S1...S8 ile çalışan DES'te kullanılmaktır. Her biri, 16 sütun ve 4 satırdan oluşan bir tabloyla gösterilen, girdi olarak 6-bit blok alan ve çıktı olarak 4 bitlik blok veren fonksiyonlardır. Bu dönüşüm Şekil 2.3'te gösterilmiştir. Bu 8 fonksiyon, toplu olarak 48 bitlik girdi bloğunu 32 bitlik çıktı bloğuna dönüştürür.



Şekil 2.3. Bir S-kutusunun iç yapısı.

Genel anlamda, bir n×k (n sıra k sütun) S-kutusu blok bit dizilerini $(b_0, b_1, \ldots, b_n) \rightarrow (b_0, b_1, \ldots, b_k)$, k ≤ n [37] koşulu altında haritalandıran $f : B^n \rightarrow B^k$ fonksiyonudur.

Bu çalışmada S-kutularını dairesel şifrelendirme sürecinden farklı bir biçimde, DES'teki gibi girdi (gizli veri bitleri) ve çıktı (oyundaki vitaminin koordinatları) arasındaki doğrusal olmayan ilişki kullanılmıştır.

3. ÖNERİLEN YILAN OYUNU STEGANOGRAFİ YÖNTEMİ

Bu bölümde, önerilen şemanın gömme ve çıkarma aşamaları adım adım açıklanmıştır.

3.1. GÖMME AŞAMASI

Adım 1: Başlangıç matrisi oluşturulur. Bu matris 6×6 boyutundadır. Böylece 36 farklı karakter eklenerek gizlenebilir.

$$I = \begin{bmatrix} i_{0,0} & \cdots & i_{0,5} \\ \vdots & \ddots & \vdots \\ i_{5,0} & \cdots & i_{5,5} \end{bmatrix} = \begin{bmatrix} a & b & c & d & e & f \\ g & h & i & j & k & l \\ m & n & o & p & q & r \\ s & t & u & v & w & x \\ y & z & 0 & 1 & 2 & 3 \\ 4 & 5 & 6 & 7 & 8 & 9 \end{bmatrix} \quad (3.1)$$

Bu matris önceden gönderici ve alıcı arasında paylaşılan genel anahtar görevini üstlenir. I matrisinin yapısı dinamiktir, her yeni gizli mesaj gönderildiğinde her karakterin konumu farklı bir hücrede olabilir. Bu işlem, çıkarma prosedürünü daha karmaşık hale getireceğinden, tasarlanan şemanın güvenliğini arttırır.

Adım 2: Konumlarına göre I aracılığıyla gizli mesajın her karakterini şifreleyerek 6 bitlik bloklar (B dizisi) oluşturulur. Gizli karakterin I matrisindeki satır ve sütun numarası ifade edilir.

$$(x)_2 = b_5 b_4 b_3 \quad (3.2)$$

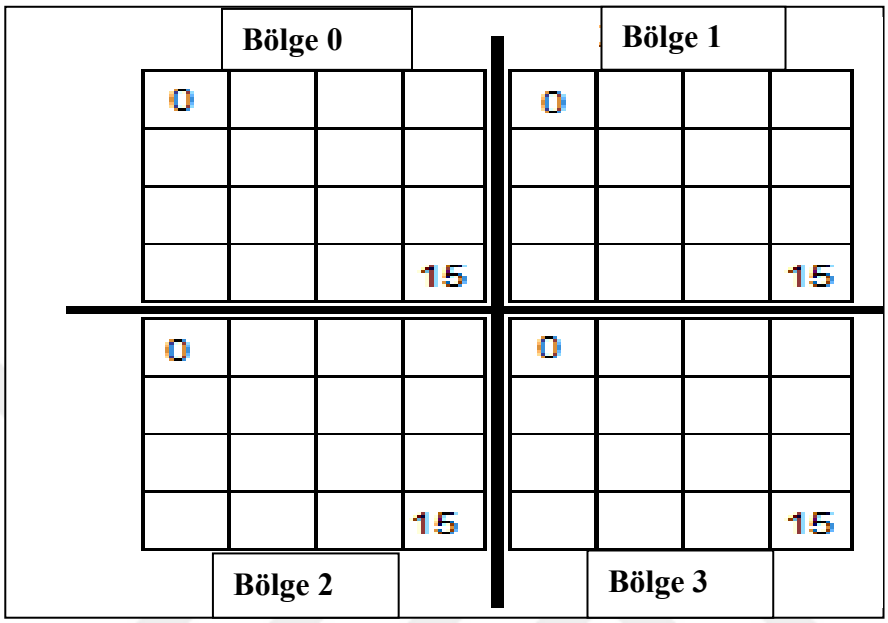
$$(y)_2 = b_2 b_1 b_0 \quad (3.3)$$

$$B = \{\forall x, y \in \{0\} \cup Z^+ | b = (x)_2 || (y)_2\} \quad (3.4)$$

B bileşenleri $b_5 b_4 b_3 b_2 b_1 b_0$ formunda olan ikili bir koordinat dizisi olarak sayılabilir. Bu dizide, üç MSB (Most Significant Bit), $b_5 b_4 b_3$, satır numarasını şifrelemek, diğer üç LSB de $b_2 b_1 b_0$, sütun numarasını şifrelemek için kullanılır. Bir başka deyişle hem satır hem de sütun numaralarını şifrelemek için üç bit kullanılmaktadır. 2^3=8, üç bit aracılığıyla temsil, toplamda 6 bit blok boyutunda olduğu için yeterli olacaktır. Bunun

yanı sıra, bu durum 8×8=64 farklı karakteri de dahil etmeye olanak sağlamaktadır. Ancak akıllı bir başlangıç yapmak adına 6×6=36 farklı karakter kullanmak tercih edilir.

Adım 3: Oyun tahtası kurulur. Önerilen şemada oyun tahtası 8×8 boyutundadır. Oyunda vitamini bulmak için toplam 64 hücre elde edilir:



Şekil 3.1. Oyun tahtasının yapısı

Oyun tahtası Şekil 3.1'de gösterildiği gibi bir yapıya sahiptir. Oyun tahtasının boyutları, DES S-kutularının çıktılarını da göz önünde bulundurarak, konum için istenilen rastlantısallığı sağlaması için tasarlanmıştır. Bu yüzden oyun tahtası, her biri 16 hücreden oluşan, 0'dan 15'e, dört farklı bölgeye ayrılmıştır (DES S-kutusunun en küçük çıktısı 0 ve en büyük çıktısı 15 olduğuna dikkat edilir). Her bir bölge aynı veya farklı S-kutuları olarak kullanılabilir. Her bölge için farklı bir S-kutusu kullanılması güvenliği ve algılanamazlığı arttırır (bkz. Bölüm 4.). Çünkü aynı gizli kalıbın saklanması durumunda elde edilen çıktılar farklı olur.

Adım 4: Oyun tahtasındaki vitaminin koordinatları hesaplanır. Şekil 3.1'de belirtildiği gibi, oyun tahtası dört bölgeden oluşur. $C = x'y'$ ile oyun tahtasındaki vitaminin koordinatları belirlenir. Son olarak vitaminin hücre numarası bulunur. Bu işlem aşağıdaki gibi gerçekleştirilir:

$$C = \{\forall x', y' \in \{0\} \cup Z^{+} | x' < 3\,,\ y' < 15\} \tag{3.5}$$

$$x' = (b_5 b_0)_{10} \tag{3.6}$$

$$y' = (S(b_5 b_4 b_3 b_2 b_1 b_0))_{10} \quad (3.7)$$

Burada x' 0 (00)'dan 3 (11)'e kadar oyun tahtasındaki bölge numarasını belirler. S ise S-kutusu dönüşümünü belirler. Bir başka ifadeyle, oyun tahtası üzerindeki bölgeyi hesaplayarak kenar boşluğunu daraltıp bölgedeki ilgili hücre S-kutusu dönüşümüyle tanımlanır. Bu noktada gizli karakter ve vitaminin koordinatları arasında doğrusal olmayan bir dönüşüm gerçekleştirilir. Sonuç olarak oyun tahtasındaki vitaminin dizisini temsil eden C dizisi elde edilir.

$$C = ((x'_0, y'_0), (x'_1, y'_1), \dots, (x'_n, y'_n)) \quad (3.8)$$

Burada, n gizli mesajın uzunluğunu gösterir. Gizli mesajın her karakterinin doğrudan vitaminin yeri olarak temsil edildiğine, dolaylı yoldan oyuncunun hareketine bağlı olarak temsil edildiğine dikkat edilir. Ancak uygulamada, yılan oyunu, oyuncu oyunu başarılı veya başarısız olarak bitirene kadar devam eder. Yani, n'den büyük olan hareket düzeni çıkarım için gerekli değildir. Bu sebeple gizli iletinin uzunluğu herhangi bir aksaklıktan kaçınmak ve çıkarma hesap yükünü azaltmak için alıcıya güvenli bir biçimde yollanan kaynak bileşenlerden biridir. Kısacası, gömme aşamasının sonunda oyun tahtasındaki vitaminin hücre dizisini elde etmek amaçlanmıştır.

3.2. ÇIKARMA İŞLEMİ

Adım 1: Bölge Şekil 3.1 dikkate alınarak vitaminin konum dizisi elde edilir. Bu adımda, C dizisini elde etmek amaçlanır:

$$C = ((x'_0, y'_0), (x'_1, y'_1), \dots, (x'_n, y'_n)) \quad (3.9)$$

C dizisinde x' bölge sayısını ve $C =$ o bölgedeki vitaminin hücre sayısını ifade eder. Böylece başlangıç olarak Şekil 3.1'de gösterildiği gibi oyun tahtasının dört parçaya ayrılması gerekmektedir. Çıkarmanın geri kalan kısmı, ilk olarak, sadece gönderici ve alıcı arasında paylaşılan gizli iletinin uzunluğunu göz önünde bulundurarak gerçekleştirilmelidir. Bir başka deyişle, tüm vitamin hamleleri için gösterime ve hesaplamaya ihtiyaç yoktur.

Adım 2: Matris I'deki orijinal karakterlerin ikili koordinatlarını içeren B dizisini elde etmek için diziyi çözümler. C dizisinde;

$$y' = (S(b_5 b_4 b_3 b_2 b_1 b_0))_{10} \quad (3.10)$$

Verilen Denklem (3.7) göz önünde tutarak, y''yi taban 2'de sunup orijinal bit akışını elde etmek üzere S-kutusu dönüşümünün tersi gerçekleştirilir.

$$\forall b \in B = INVS((y')_2) \quad (3.11)$$

3. Adım: B dizisini kullanarak gizli mesajın karakterleri I matrisinden çıkarılır. Bu noktada, B'yi aşağıdaki gibi bölerek C dizisi hesaplanır (gerektiği takdirde denklem (3.2) ve (3.3)'e bakınız):

$$x = (b_5 b_4 b_3)_{10} \quad (3.12)$$

$$y = (b_2 b_1 b_0)_{10} \quad (3.13)$$

Matris I'de yer alan gizli karakterin satır numarasının x ve sütun numarasının y olduğuna dikkat edilir. Önce x ve y'yi birleştirerek ve 10 tabanında 6 bit halinde göstererek en baştaki gömme aşamasında hesaplanılan B öğeleri elde edilir.

3.3. ÇIKARMA AŞAMASINDA OYUN YAPIMI İÇİN BİLGİLER

Tasarlanan şemada, gizli mesajın her karakteri vitaminin yerini direkt olarak, oyuncunun hareketini dolaylı olarak gösterilir. C dizisi bu amaçla yapılmıştır.

$$C = ((x'_0, y'_0), (x'_1, y'_1), \dots, (x'_n, y'_n)) \quad (3.14)$$

Burada, n'nin gizli mesajın uzunluğunu temsil ettiği belirtilmiştir. Vitaminin gizli mesajı yerleştirmek için n koordinat vardır. Buna göre n hamle vardır. Ancak uygulamada, yılan oyunu oyuncuyu başarılı-başarısız bitirene kadar devam eder. Bu amaçla, koordinat bilgisinin geri kalanı rastgele tanımlanır. Ama bu durum çıkarma işlemini alıcı için neredeyse çözülemez hale getirmektedir. Bu sebeple gizli iletinin uzunluğu herhangi bir aksaklıktan kaçınmak ve çıkarma hesap yükünü azaltmak için alıcıya güvenli bir biçimde yollanan kaynak bileşenlerden biridir. Alıcı, bu bilgileri dikkate alarak çıkarma işlemine devam eder. Ama bu durum çıkarma işlemini alıcı için neredeyse çözülemez hale getirmektedir. Bu sebeple gizli iletinin uzunluğu herhangi bir aksaklıktan kaçınmak ve çıkarma hesap yükünü azaltmak için alıcıya güvenli bir

biçimde yollanan kaynak bileşenlerden biridir. Oyun tahtasının dört bölüme ayrıldığı belirtilmiştir. İlgili hücreye vitamin tahsisi, bölgenin seçimi ile gerçekleştirilir ve ilgili bölgedeki hücreyi tanımlamak için S-kutusu dönüşümü (S_1-S_8) kullanılır.

$$C = \{\forall x', y' \in \{0\} \cup Z^{+} | x' = (b_5 b_0)_{10}\, , y' = (S(b_5 b_4 b_3 b_2 b_1 b_0))_{10}\} \tag{3.15}$$

Aynı S-kutusu (S_1-S_8) dört bölgenin tamamı için kullanılabilir. Ancak güvenliği artırmak için, her bölge için özel bir S-kutusu kullanılmalıdır. Bu durumda, her bölge için tanımlanmış S-kutularının sırası alıcıya gönderilmelidir. Böylece, çıkarım alıcı için kesin olur, ancak saldırgan için belirsiz olacaktır.

3.4. AÇIKLAYICI BİR ÖRNEK

Bu alt bölümde, uygulamayı kolaylaştırmak için bir mesajın gömme aşaması örneklenmiştir. Gizli mesaj "game" kelimesidir.

Adım 1: I'nın Yapımı:

$$I = \begin{bmatrix} a & b & c & d & e & f \\ g & h & i & j & k & l \\ m & n & o & p & q & r \\ s & t & u & v & w & x \\ y & z & 0 & 1 & 2 & 3 \\ 4 & 5 & 6 & 7 & 8 & 9 \end{bmatrix} \tag{3.16}$$

Adım 2: B dizisinin gizli ileti karakterlerinin I aracılığıyla ve yerlerine göre deşifre edilmesiyle yapımı. Gizli mesaj "game" olarak seçilmiştir. Denklem (3.2) ve Denklem (3.3) kullanılarak x, y ve B dizisi aşağıdaki gibi hesaplanır:

“g” için (1. Satır, 0. Sütun)

$$b = (x)_2 || (y)_2 = (1)_2 || (0)_2 = 001000 \tag{3.17}$$

“a” için (0. Satır, 0. Sütun)

$$b = (x)_2 || (y)_2 = (0)_2 || (0)_2 = 000000 \tag{3.18}$$

“m” için (2. Satır, 0. Sütun)

$$b = (x)_2 || (y)_2 = (0)_2 || (0)_2 = 010000 \tag{3.19}$$

“e” için (0. Satır, 4. Sütun)

$$b = (x)_2 || (y)_2 = (0)_2 || (4)_2 = 000100 \quad (3.20)$$

$$B = \{001000,000000,010000,000100\} \quad (3.21)$$

Adım 3: Oyun tahtasının yapımı (Şekil 3.1).

Adım 4: Denklem (3.6), Denklem (3.7) aracılığıyla vitaminin ve C dizisinin koordinatlarını aşağıdaki şekilde hesaplanır.

$$C = ((x_0', y_0'), (x_1', y_1'), (x_2', y_2'), (x_3', y_3')) \quad (3.22)$$

$$x_0' = (b_5 b_0)_{10} = (00)_{10} = 0\ (Zone\ 0) \qquad \text{(Bölge 0)} \quad (3.23)$$

$$y_0' = (S_5(b_5 b_4 b_3 b_2 b_1 b_0))_{10} = (S(001000))_{10} = (0111)_{10} = 7\ (cell\ 7\ ) \quad (3.24)$$

$$x_1' = (b_5 b_0)_{10} = (00)_{10} = 0\ (Zone\ 0) \qquad \text{(Bölge 0)} \quad (3.25)$$

$$y_1' = (S_5(b_5 b_4 b_3 b_2 b_1 b_0))_{10} = (S(000000))_{10} = (0010)_{10} = 2\ (cell\ 2\ ) \quad (3.26)$$

$$x_2' = (b_5 b_0)_{10} = (01)_{10} = 1\ (Zone\ 1) \qquad \text{(Bölge 1)} \quad (3.27)$$

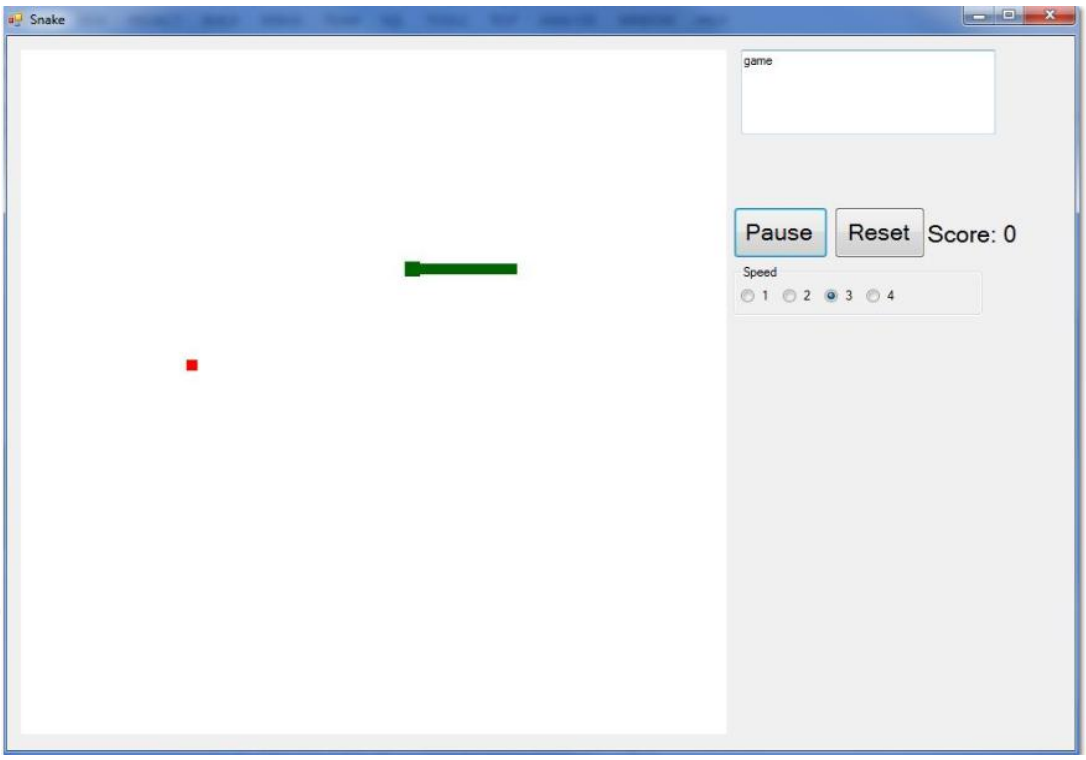
$$y_2' = (S_5(b_5 b_4 b_3 b_2 b_1 b_0))_{10} = (S(010000))_{10} = (1000)_{10} = 8\ (cell\ 8\ ) \quad (3.28)$$

$$x_3' = (b_5 b_0)_{10} = (00)_{10} = 0\ (Zone\ 0) \qquad \text{(Bölge 0)} \quad (3.29)$$

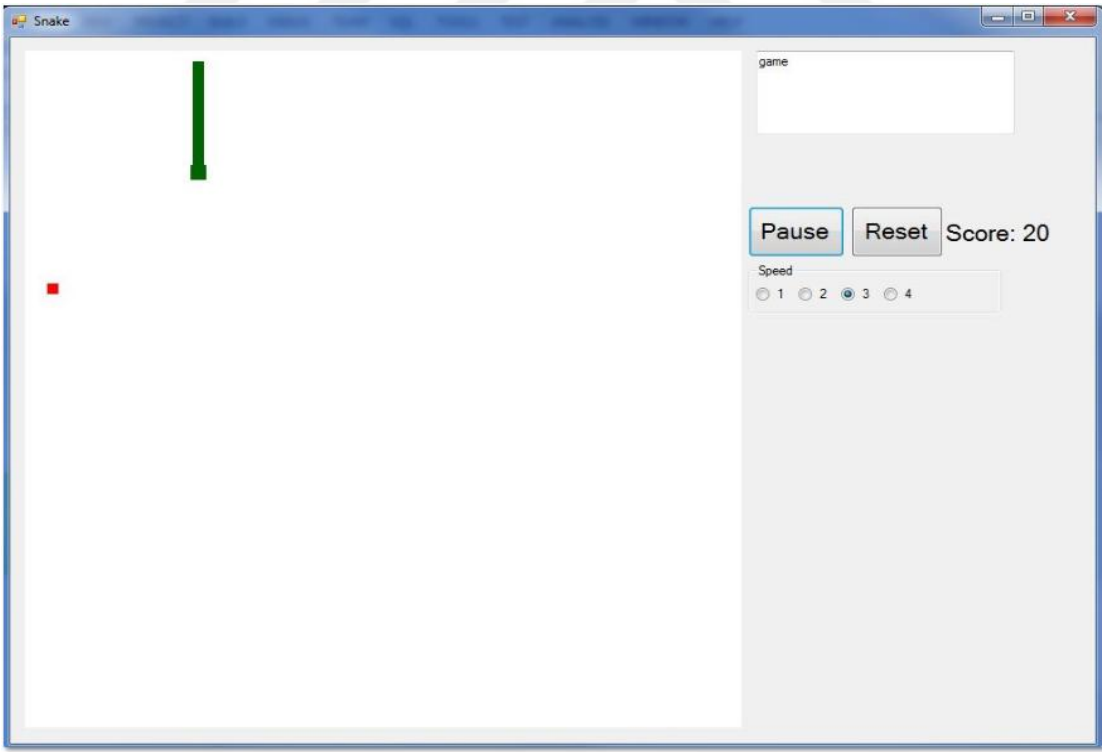
$$y_3' = \left(S_5(b_5 b_4 b_3 b_2 b_1 b_0)\right)_{10} = \left(S(000100)\right)_{10} = (0100)_{10} = 4\ (cell\ 4\ ) \quad (3.30)$$

$$C = \big((0,7), (0,2), (1,8), (0,4)\big) \quad (3.31)$$

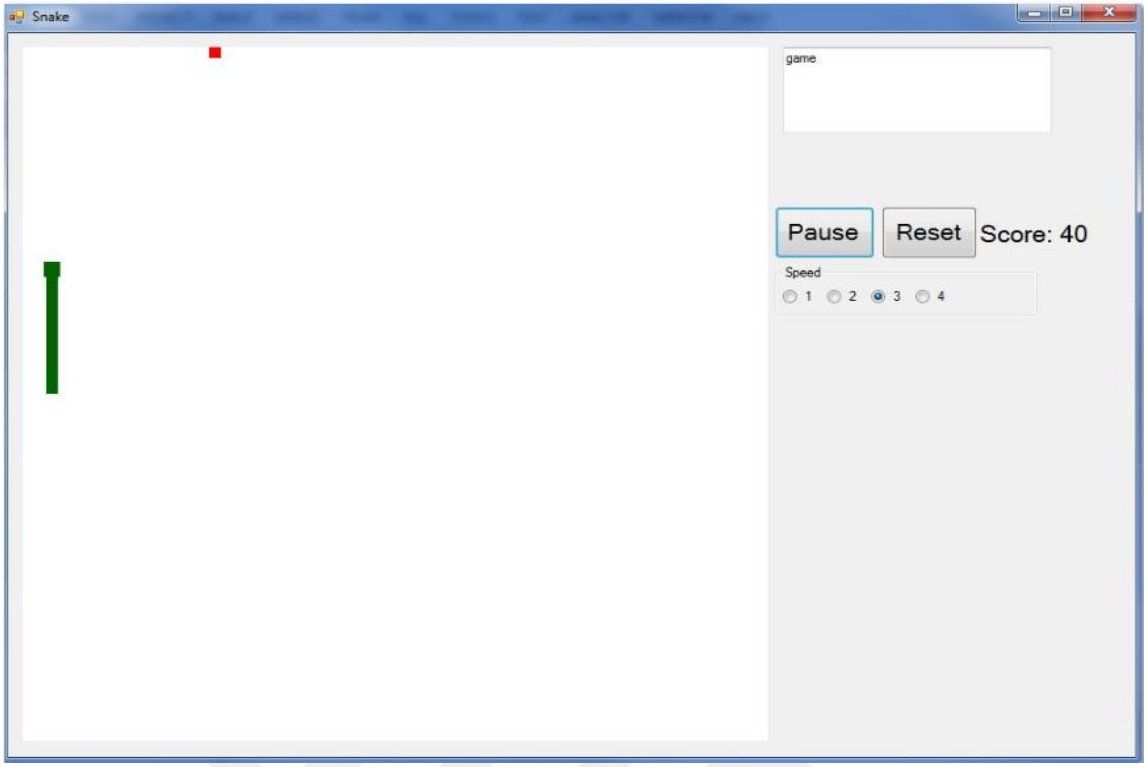
Şekil 3.2’de gizli mesajın (“game”) oyun çıktılarını belirten şekiller gösterilmiştir:



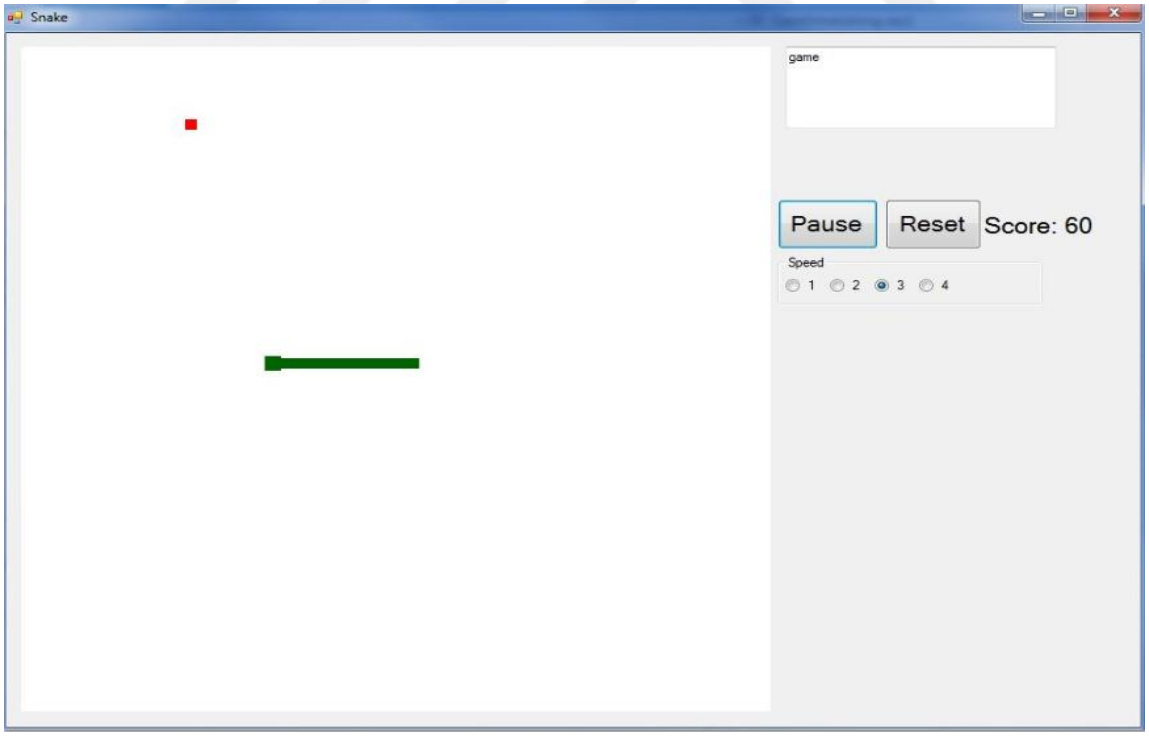
Şekil 3.2 (a).“g” için vitaminin konumu.



Şekil 3.2 (b).“a” için vitaminin konumu.



Şekil 3.2 (c). “m” için vitaminin konumu.



Şekil 3.2 (d). “e” için vitaminin konumu.

4. DENEYSEL SONUÇLAR

Bu bölümde, kapasite, algılanamazlık ve güvenlik açısından önerilen metot analiz edilmiştir ve incelenmiştir. Bu çalışmanın kapsamında olan deneyler Winstein Lexical Steganography veri seti kullanılarak elde edilmiştir [37].

4.1. KAPASİTE (YETERLİLİK) ANALİZİ

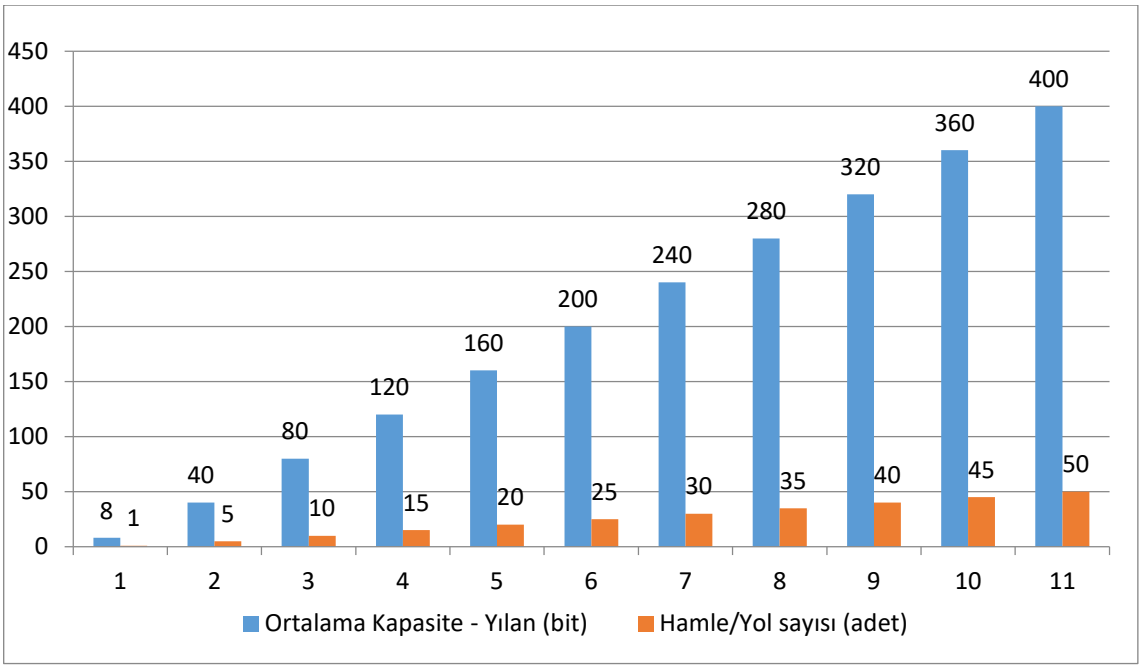
Öne sürülen planda vitaminin yeri gizli iletinin her bir karakterine göre hesaplanmıştır. Bir başka deyişle, oyuncunun hamlesi vitaminin yeri ile belirlenmektedir. Bu amaçla yapılan C dizisi aşağıdaki yapıya sahiptir:

$$C = ((x_0^{'}, y_0^{'}), (x_1^{'}, y_1^{'}), \dots, (x_n^{'}, y_n^{'})) \quad (4.1)$$

Burada, n in gizli mesajın uzunluğunu temsil ettiği belirtildi. Vitamini gizli mesaja gömmek için n koordinat (n harekete bağlı olarak) bulunmaktadır. Vitaminin her hareketine bir karakter (8 bit) saklanmıştır. Çizelge 4.1 kapasite ölçüm sonuçlarını göstermektedir.

Çizelge 4.1. Kapasite ölçüm detayları.

Gizli veri (bit)	8	40	80	120	160	200	240	280	320
Hamle sayısı (adet)	1	5	10	15	20	25	30	35	40
Oyun büyüklüğü (bit)	21504	21504	21504	21504	21504	21504	21504	21504	21504



Şekil 4.1.Yapılan hamlelere istinaden gizli bitleri gösteren kapasite grafiği.

Şekil 4.1, gizli bitlerin miktarına göre kapasite grafiğine karşılık yapılan hamle sayısının kapasite grafiğini belirtmektedir. Y ekseni gizli bit miktarını, x ekseni gerçekleştirilen deneylerin sayısını belirtir. Oyunun büyüklüğü Çizelge 4.1'de gösterildiği gibi sabittir. Oyundaki hamle sayısı arttıkça gizli bitlerin miktarının arttığı görülür. Yani, hamle başına 8 bit gömülmüştür.

4.2. ALGILANAMAZLIK ANALİZİ

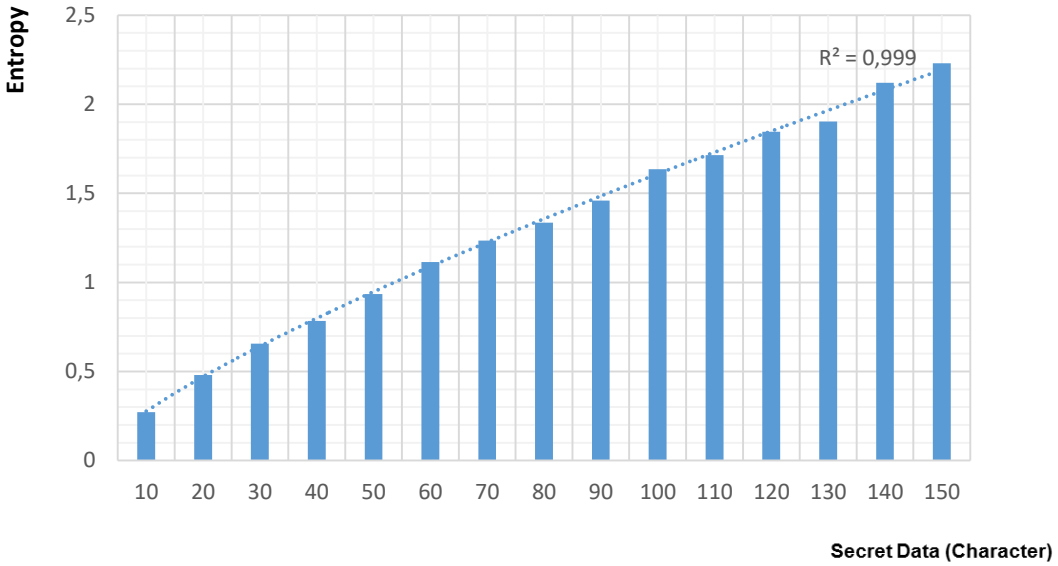
Shannon'un teorisine göre bilgi entropisi, bilgi ölçümünün temel rastlantısallıklarından biridir. Yüksek entropi değerleri yüksek rastlantısallık ifade eder ve m bit üzerine şifrelenen her mesaj için üst sınır m'dir. Entropinin formülü aşağıda gösterilmiştir [38]:

$$H = -\sum_{i=0}^{2m-1} p_i Log_2 p_i \tag{4.2}$$

[32]'de belirtildiği gibi, güvenli bir steganografi planı istatistiksel açıdan tespit edilemez olmalıdır. Bu alt bölümde, bir tarafsız değerlendirme için vitamin konumunun dağılımı incelenmiştir. Vitamin yerinin dağılımı gizli mesaj ve gizli mesajın uzunluğuyla hiçbir alakası yokmuş gibi gözükmelidir. Bu nedenle, Çizelge 4.2'de verilen gizli mesajların uzunluğu için entropi değerleri hesaplanır ve Şekil 4.3'te entropi eğilimi gösterilmiştir.

Çizelge 4.2**.** Hesaplanan entropi değerleri.

Karakter Uzunluk	10	30	50	70	90	110	130	150
Entropi	0.272	0.657	0.934	1.235	1.459	1.714	1.903	2.23



Şekil 4.2. Gizli veri boyutuna göre hesaplanan entropi değerlerini gösteren grafik.

Çizelge 4.2'de, deneyler sırasında her bir gizli mesajın karakter uzunluğundaki artış değeri 20'dir. Şekil 4.2'de, her gizli mesajın karakter uzunluğundaki artış değeri, deneyler sırasında hassas bir değerlendirme için 10'dur. Hem Çizelge 4.2'de hem de Şekil 4.2'de görüldüğü gibi, gizli veri boyutunun değerleri arttıkça 2'yi aştığı görülmüştür. Ayrıca Şekil 4.2'de grafikteki R eğrisinden görüldüğü gibi gizli mesaj boyutu arttıkça bu değerin 6'ya (gizli mesajı kodlamak için kullanılan bit sayısı) yakınsaması beklenmektedir. Bu sonuç önemlidir, çünkü gizli veriler, vitaminin hücre sayısını temsil eden 4 bit ile şifrelenir. Bu, vitamin yeri ile gizli veriler arasındaki ilişkinin baştan sona sonuna kadar azaldığı anlamına gelir. Başka bir deyişle, gizli veri uzunluğu arttıkça mevcut rastlantısallık artmaktadır. Verilen grafikteki sapma eğrisi önemli derecede R değerine sahip entropi eğilim dağıtımını gösterir.

4.3. GÜVENLİK ANALİZİ

Steganografide, sistemi kırmak için iki aşama vardır: Birincisi, bir saldırgan steganografik bir sistemde gizli mesajın varlığını saptamalıdır. İkincisi, saldırgan gömülü iletiyi çıkarmak zorundadır. Bu çalışmada başlangıçta bu iki konu üzerine durulmuştur. İlk madde için; gizli mesajın her karakteri oyun sırasında vitamin konumuna dönüştürülmüştür. Böylece, gizli mesajı vitamin için bir koordinat dizisi olarak temsil edilir; oyunun doğasına uygun bir bileşen (bkz. Bölüm 3.1. ve somut sonuç için Bölüm 3.4.). İkinci madde için gizli karakter ile vitamin yeri arasında DES S-kutuları ile doğrusal olmayan bir ilişki kurulmuştur (bkz. Bölüm 3.1. ve somut sonuç için Bölüm 3.4.).

Bununla birlikte, saldırganın gizli mesajı "kaba kuvvet" ile çıkarmaya çalışabileceğinin güçlü bir olasılığı vardır. Bu durumda, saldırgan, oyunu alıcı tarafta olduğu gibi kurmak için doğru bileşenleri (bkz. Bölüm 3.3.) ve gönderen ile alıcı arasında önceden paylaşılan genel anahtarı (bkz. Bölüm 3.1, adım 1) tahmin etmek zorundadır. Yani, saldırgan, tüm hareketleri incelemek yerine sadece gerekli vitamin hareketlerini incelemek için gizli mesajın uzunluğunu (n) tahmin etmelidir. Ayrıca saldırgan tanımlanmış hamleler üzerinde hatasız olarak çıkarma işlemi gerçekleştirebilmek için Bölge1, Bölge2, Bölge3, Bölge4 (Şekil 3.1) bölgelerindeki doğru S-kutusu düzenini ve son olarak genel anahtarı, yani, başlangıç matrisini tahmin etmelidir. Yani, saldırgan, oyun sırasında vitamin yeri aracılığıyla gizli mesajı çıkarmak için bu üç bileşenin tümünü doğru tahmin etmelidir.

Önerilen şemada, [1] 'de belirtildiği üzere, güvenlik seviyesini artırmak için kriptografi ve steganografi birleştirilmiştir. Gizli mesajı vitamin yeri yoluyla yerleştirmek için DES S-kutuları kullanılmıştır. Her bölgede, Bölüm 3.3'te belirtildiği gibi güvenliği arttırmak için bir oyun oturumunda 4 farklı S-kutusu kullanılmalıdır. Başlangıç matrisinin eklenmesiyle, bir saldırgan gizli mesajı çıkarmak için çok sayıda kombinasyon gerçekleştirmelidir. Buna göre, olası kombinasyon sayısı aşağıdaki gibi bulunur:

$$A = 36! \times 8^4 \times \binom{m}{n} \tag{4.3}$$

Burada A, kaba kuvvet saldırısının kombinasyon sayısını belirtir. m ise toplam vitamin hamle sayısını ve n gizli mesajın uzunluğunu belirtir (n ≤ m olduğuna dikkat ediniz). Yani, bir saldırgan, Denklem (3.2)'de belirten kombinasyon sayısını gerçekleştirmelidir.

Dolayısıyla saldırı olasılığı şöyledir:

$$P = \frac{1}{36! \times 8^4 \times \binom{m}{n}} \tag{4.4}$$

m=n=1 olduğu durumları göz önünde bulundurulursa bu çok küçük bir sayıdır (aşağı yukarı 6×10^{-46}*).* Bu sonuçlara bakılacak olursa önerilen metot güvenlidir.

5. SONUÇLAR VE ÖNERİLER

Bu bölümde, önerilen metot literatürdeki diğer metotlar ile karşılaştırılmıştır. Karşılaştırma ölçütü olarak literatür esas alınarak kapasite seçilmiştir. Ayrıca saldırı olasılıkları da karşılaştırılmıştır. Sonrasında ise önerilen metoda ilişkin avantaj ve dezavantajlara değinilmiş ve genel bir yargıya ulaşılmıştır.

5.1. DEĞERLENDİRME SONUÇLARI

Bu bölümde, önerilen metot, literatürdeki diğer metotlar ile karşılaştırılmıştır. Önceki bölümde de anlatıldığı gibi önerilen metot kapasite, algılanamazlık ve güvenlik açısından analiz edilmiştir. Ancak literatürdeki en yaygın ölçüm parametresi olduğundan ötürü karşılaştırma amacıyla kapasite esas alınmıştır. Çizelge 5.1'de önerilen metot, literatürdeki diğer güncel metotlar ile kapasite açısından karşılaştırılmıştır. Karşılaştırma, hamle sayısına göre toplam kapasite (bit) olarak hesaplanmıştır.

Çizelge 5.1. Kapasite karşılaştırma sonuçları.

Hamle Sayısı (adet)	Yılan Oyununda kapasite (bit) (Satir ve Güner, 2017)	Labirent kapasite (bit) (Lee ve arkadaşları, 2010)	TicTacToe kapasite (bit) (Philip C. Ritchey ve Vernon J. Rego, 2012)	Satranç (A. Desoky ve M. Younis, 2009)
1	8	125	6	7
5	40	224	İlgili makalede formüle edilmemiş ve hesaplanmamış.	35
10	80	İlgili makalede formüle edilmemiş ve hesaplanmamış.	İlgili makalede formüle edilmemiş ve hesaplanmamış.	70

Çizelge 5.1 (devam). Kapasite karşılaştırma sonuçları.

30	240	İlgili makalede formüle edilmemiş ve hesaplanmamış.	İlgili makalede formüle edilmemiş ve hesaplanmamış.	210
40	320	İlgili makalede formüle edilmemiş ve hesaplanmamış.	İlgili makalede formüle edilmemiş ve hesaplanmamış.	280
Açıklama	Verilen örnek ile hesaplanmıştır.	İlgili makalede rapor edilmiştir.	İlgili makalede rapor edilmiştir.	İlgili makalelerdeki örneklerden sağlanmıştır.

Stego ortam olarak kullanılan labirent ve satranç oyunlarına ilişkin kapasite değerleri ilgili makalelerdeki örneklere dayanılarak verilmiştir. Tic Tac Toe oyunu stego ortamındaki kapasite değeri ilgili makaleden yararlanılarak verilmektedir. Yılan oyunu stego ortamındaki kapasite değeri de Tablo 4.1'de gösterilmiştir. Çizelge 5.1'de görüldüğü üzere, önerilen metodun kapasitesi hamle sayısı arttıkça artmıştır. Önerilen yöntemin literatürdeki diğer yöntemlere göre hamle sayısı arttıkça kapasitesinin daha fazla arttığı görülmüştür.

Çizelge 5.2. Güvenlik analizi karşılaştırma sonuçları.

Hamle Sayısı (adet)	Gizli Mesaj Uzunluğu (karakter)	Labirent saldırı olasılığı (Lee ve arkadaşları, 2010)	Yılan Oyununda saldırı olasılığı (Satir ve Güner, 2017)
10	4	10^{-10}	$3x10^{-48}$
20	8	20^{-18}	$4x10^{-52}$
30	12	30^{-26}	$7x10^{-54}$
40	16	40^{-34}	$10x10^{-56}$
Açıklama		İlgili makaledeki formüle göre hesaplanmıştır.	Önerilen metot için oluşturulan formüle göre hesaplanmıştır.

Güvenlik yönünden karşılaştırma sonuçları da Çizelge 5.2'de verilmiştir. Stego ortam olarak kullanılan labirent oyununa ilişkin saldırı olasılığı değerleri, ilgili makaledeki formüle dayanılarak hesaplanmıştır. Yılan oyunu saldırı olasılığı da önerilen yöntemde verilen formüle göre hesaplanmıştır. Çizelge 5.2'de görüldüğü üzere, önerilen yöntemin hamle sayısı ve gizli mesaj uzunluğu arttıkça saldırı olasılığı da azalmıştır. Literatürdeki diğer metot olan labirent yöntemine göre de daha güvenli olduğu görülmüştür.

5.2. ÖNERİLER

Bu çalışmada, örtme aracı olarak yılan oyunu kullanan bir oyun steganografi yöntemi önerilmiştir. Oynanan her bir oyun için vitaminin her hamlesi gizli birer karakter simgelemektedir. Ancak bu gizleme işlemini doğrudan yaparak güvenlik ve algılanamazlık sağlanamamaktadır. Bu sebeple DES S-kutularını kullanarak gizli veri ve vitaminin yeri arasında doğrusal olmayan bir ilişki kurulmuştur. Bu sayede, güvenlik ve algılanamazlık sağlanmış ve 8 bit her bir hamlenin içine gizlenmiştir. Ayrıca, eğer farklı bir S-kutu sırası kullanılırsa, aynı gizli iletinin saklanması halinde farklı çıktılar elde edilmiştir. Bir anlamda vitamin oyun tahtasında farklı yerlerde olacaktır. Önerilen yöntemin literatürdeki diğer yöntemlere göre hamle sayısı arttıkça kapasite yönünden daha fazla olduğu görülmüştür. Saldırı olasılığı da hamle sayısı ve gizli mesaj uzunluğu arttıkça çok düşmüştür. Bu nedenle önerilen metodun güvenilir olduğu söylenebilir.

Bununla birlikte eleştiri olarak, bu çalışmada 6×4 bitlik S-kutuları kullanılmıştır. Önerilen şemayı, algılanamazlık ve güvenlik açısından daha esnek hale getirmek için çok avantajlı bir fırsat vardır. Oyun tahtasındaki hücrelerin sayısı ve çeşitli gizli semboller, AES gibi daha karmaşık S-kutuları kullanılarak arttırılabilir. Bu, daha sonraki çalışmalarda ele alınacak ana konudur.

6. KAYNAKLAR

[1] M.M. Sadek, A.S. Khalifa, Mostafa, "Video steganography: a comprehensive review," *Multimed Tool Appications*, vol. 74, no. 17, pp. 7063-7094, 2015.

[2] Zaker, N. & Hamzeh, "A novel steganalysis for TPVD steganographic method based on differences of pixel difference histogram," *Multimed Tool Appications*, vol. 58, no. 1, pp. 147-1666, 2012.

[3] Gutub, Fattani,"A novel Arabic text steganography method using letter points and extensions", *WASET International Conference on Computer, Information and Systems Science and Engineering (ICCISSE)*, vol. 1, no. 3, pp. 107-118, 2007.

[4] J.C. Hernandez-Castro, I. Blasco-Lopez, J.M. Estevez-Tapiador, A. Ribagorda-Garnacho, "Steganography in games: A general methodology and its application to the game of Go," *Computers & Security*, vol. 25, no. 1, pp. 64-71, 2006.

[5] W. Luo, F. Huang, J. Huang, "A more secure steganography based on adaptive pixel-value differencing scheme," *Multimed Tool Appications,* vol. 52, no. 2-3, pp. 407-430, 2011.

[6] H. Sajedi, M. Jamzad, "Secure steganography based on embedding capacity," *International Journal of Information Security*, vol. 8, no. 6, pp. 433-445, 2009.

[7] K. Bailey, K. Curran, "An evaluation of image based steganography methods using visual inspection and automated detection techniques," *Multimed Tool Appications*, vol. 31, no. 3, pp. 327-327, 2006.

[8] Betül Dolay, (2017, 12 Nisan), *Veri Gizleme Bilimi*, [Online]. Erişim: http://e-bergi.com/y/Veri-Gizleme-Bilimi.

[9] Erkin Z., Örencik B., "Steganografik Kütüphane", *Ağ ve Bilgi Güvenliği Ulusal Sempozyumu Bildirileri,* İstanbul, Türkiye, 2005, ss. 672–680.

[10] Cheddad A., Condell J., Curran K., McKevitt P., "Digital image steganography: Survey and analysis of current methods," *Signal Processing,* vol. 90, no. 3, pp. 727-752, 2010.

[11] E. Satir, H. Isik, "A compression-based text steganography method," *Journal of Systems and Software,* vol.85, no. 10, pp. 2385–2394, 2012.

[12] V. Sabeti, S. Samavi, S. Shirani, "An adaptive LSB matching steganography based on octonary complexity measure," *Multimed Tool Appications*, vol. 64, no. 3, pp. 777-793, 2013.

[13] L.H. Lee, C.F. Lee, L.H. Chen, "A perfect maze based steganographic method," *The Journal of Systems and Software*, vol. 83, no. 12, pp. 2528-2535, 2010.

[14] Wen-Chao Yang, Ling-Hwei Chen, "A steganographic method via various animations in PowerPoint files," *Multimed Tool Appications*, vol.74, no. 3, pp. 1003-1019, 2013.

[15] Hussain, M. ve Hussain, M., "A survey of image steganography techniques," *International Journal of Advanced Science and Technology,* vol. 54, no. 18, pp. 975-8887, 2013.

[16]Sui, X.G., Luo, H., "A new steganography method based on hypertext", *Radio Science Conference*, Qingdao, China , 2004, pp. 24- 27.

[17] Castiglione A, De Santis A, Fiore U, Palmieri F, "An asynchronous covert channel using spam," *Computer & Mathematics with Appications,* vol. 63, no. 2, pp. 437-447, 2012.

[18] Zhi-Hui Wang, Chin-Chen Chang, "Emotion-based text steganography in chat," *Asia-Pacific Conference*, Wuhan, China, 2009, pp. 54-65.

[19] Natthawut Samphaiboon and Matthew N. Dailey, "Steganography in Thai Text", *In Proceedings of ECTI-CON*, Krabi, Thailand, 2008, pp. 133-136.

[20] D. Yan, R. Wang, "Huffman table swapping-based steganograpy for MP3 audio,"*Multimedia Tools Appications,* vol. 52, no. 2-3, pp. 291-305, 2011.

[21] A. Desoky, "Listega: list-based steganography methodology," *International Journal of Information Security*, vol. 8, no. 4, pp. 247-261, 2009.

[22] Yeh, W. H.,Hwang, J.J., "Hiding Digital Information Using a Novel System Scheme,"*Computers & Security*, vol. 20, no. 6, pp. 533-538, 2001.

[23] E. Satir, H. Isik, "A Huffman compression based text steganography method," *Multimed. Tools Appications,* vol. 70, no. 3, pp. 2085-2110, 2014.

[24] W. Mazurczyk, K. Szczypiorski, "Evaluation of steganographic methods for oversized IP packets," *Telecommunication Systems,* vol. 49, no. 2, pp. 207–217, 2012.

[25] B. Jankowski, W. Mazurczyk, K. Szczypiorski, "PadSteg: introducing inter-protocol steganography," *Telecommunication Systems,* vol. 52, no. 2, pp. 1101–1111, 2013.

[26] W.C. Yang, L.H. Chen, "A steganographic method via various animations in PowerPoint files," *Multimed. Tools Applications,* vol. 74, no. 3, pp. 1003–1019, 2015.

[27] D. Uljarevic´, M. Veinovic´, G. Kunjadic´, D. Tepšic´, "A new way of covert communication by steganography via JPEG images within a Microsoft Word document," *Multimedia Systems*, vol. 23, no. 3, pp. 333-341, 2015.

[28]Julio C. Hernandez-Castro, Ignacio Blasco-Lopez, Juan M.Estevez-Tapiador, Arturo Ribagorda-Garnacho, "Steganography in games: A general methodology and its application to the game of Go," *Computer & Security*, vol. 25, no. 1, pp. 64-71, 2006.

[29] A. Desoky, M. Younis, "Chestega: chess steganography methodology," *Security and Communication Networks*, vol. 2, no. 6,pp.555–566, 2009.

[30] L.H. Lee, C.F. Lee, L.H. Chen, "A perfect maze based steganographic method," *The Journal of Systems and Software*, vol. 83, no. 12, pp. 2528–2535, 2010.

[31] Philip C. Ritchey, Vernon J. Rego,"Covert Channels in Combinatorial Games," *In: 5th International ICST Conference on Simulation Tools and Techniques*, Rome, Italy, 2012, pp. 234-241.

[32] Z.H. Ou, L.H. Chen, "A steganographic method based on tetris games," *Information Sciences*, vol. 276, pp. 343–353, 2014.

[33] M. Virvou, S. Papadimitriou, "Simple arithmetic lessons through an adaptive snake game," *International Conference on Computer*, Piraeus-Athens, Greece, 2013, pp. 71-75.

[34] V. Di Iorio, R.S. Bigonha, M.A.S. Bigonha, A. Oliveira, E. Miguel, "What's the Name of the Game? Formal specification of artificial intelligence games," *Electronic Notes Theoretical Computer Science*, vol. 130, pp. 129-150, 2005.

[35] M. Temmerman, E.G. Daylight, F. Catthoor, S. Demeyer, T. Dhaene, "Optimizing data structures at the modeling level in embedded multimedia," *Journal of Systems Architecture,* vol. 53, no. 8, pp. 539-549, 2007.

[36] P. Roelse, "The design of composite permutations with applications to DES-like Sboxes," *Designs, Codes and Crytography,* vol. 42, no. 1,pp. 21–42, 2007.

[37] K. Winstein, (2016, April 01). *Lexical steganography,* [Online]. Available:http://alumni.imsa.edu/~keithw/tlex.

[38] F.K. Mohamed, "A parallel block-based encryption schema for digital images using reversible cellular automata," *Engineering Science and Technology, an International Journal,* vol. 17, no. 2, pp. 85-94, 2014.

ÖZGEÇMİŞ

KİŞİSEL BİLGİLER

Adı Soyadı : Kubilay GÜNER

Doğum Tarihi ve Yeri : 06.01.1991 - Bolu

Yabancı Dili : İngilizce

E-posta : kubilay.guner@hotmail.com

ÖĞRENİM DURUMU

Derece	**Alan**	**Okul/Üniversite**	**Mezuniyet Yılı**
Yüksek Lisans	Bilgisayar Müh.	Düzce Üniversitesi	2017
Lisans	Bilgisayar Müh.	Sakarya Üniversitesi	2013
Lise	Fen Bilimleri	Bolu Anadolu Öğretmen Lisesi	2009