Bölüm 5

Steganografi Alanındaki Araştırma Eğilimleri: Ulusal Literatür Üzerine Tematik Bir İnceleme

Mürsel Ozan İncetaş[1]

Murat Meriçelli[2]

Özet

Steganografi, dijital ortamlarda gizli verilerin metin, görüntü, ses, video gibi taşıyıcı nesneler içerisine gömülmesini temel alan bir bilgi gizleme yöntemidir. Kriptografiden farklı olarak, yalnızca mesajın içeriğini değil, iletişimin varlığını da gizlemeyi hedefler. Antik Yunan'dan günümüze uzanan köklü bir geçmişe sahip olan steganografi, dijital çağla birlikte siber güvenlik, adli bilişim ve telif hakkı koruma gibi alanlarda stratejik önem kazanmıştır. Bu çalışma, Türkiye'de steganografi alanında hazırlanmış lisansüstü tezlerin genel görünümünü, metodolojik eğilimlerini ve araştırma boşluklarını ortaya koymayı amaçlamaktadır. YÖK Ulusal Tez Merkezi'nde "steganografi" anahtar kelimesiyle taranan tezler PRISMA ilkeleri doğrultusunda değerlendirilmiş; tam metnine erişilen 111 tez (92 yüksek lisans, 19 doktora) betimsel analiz yöntemiyle incelenmiştir. Tezler; tür, yıl, üniversite, enstitü, anabilim dalı, danışman unvanı, sayfa sayısı, tablo-şekil kullanımı, taşıyıcı ortam, kullanılan yöntemler ve performans ölçütleri açısından analiz edilmiştir. Bulgular, tezlerin büyük çoğunluğunun Fen Bilimleri Enstitüleri bünyesinde ve bilgisayar mühendisliği ağırlıklı programlarda yürütüldüğünü göstermektedir. En çok tercih edilen yöntem LSB (45 tez) iken, kriptografik algoritmalardan AES (10 tez) öne çıkmaktadır. Performans değerlendirmesinde PSNR (35 tez) en sık kullanılan ölçüttür. Görüntü steganografisi baskın olmakla birlikte metin, ses, video ve ağ ortamlarında da çalışmalar mevcuttur. Steganaliz içeren tezlerin sınırlı sayıda kalması, alanın gizleme odaklı bir perspektifle şekillendiğini göstermektedir. Yapay zekâ tabanlı yöntemlerin (CNN, GAN) ise henüz yeterli düzeyde temsil edilmediği tespit edilmiştir. Sonuç olarak,

1 Doç. Dr., Alanya Alaaddin Keykubat Üniversitesi, ALTSO MYO, Bilgisayar Teknolojileri Bölümü, ozan.incetas@alanya.edu.tr, ORCID: 0000-0002-1016-1655

2 Dr. Öğr. Üyesi, Alanya Alaaddin Keykubat Üniversitesi, ALTSO MYO, Bilgisayar Teknolojileri Bölümü, murat.mericelli@alanya.edu.tr, ORCID: 0000-0003-0168-3221

https://doi.org/10.58830/ozgur.pub1230.c4966

Türkiye'de steganografi alanındaki lisansüstü tezler teknik ve uygulama odaklı bir çizgide ilerlemekte; ancak frekans alanı teknikleri, yapay zekâ uygulamaları ve steganaliz konularında metodolojik çeşitliliğin artırılması gerekmektedir. Bu çalışmanın, alanda çalışacak araştırmacılara yol gösterici bir kaynak olması beklenmektedir.

1. Giriş

Dijitalleşen dünyada bilginin stratejik bir öneminin olması, verinin güvenli bir şekilde iletilmesini ve depolanmasını zorunlu kılmıştır. Bilgi güvenliğinin temellerinden biri olan gizlilik kavramı, verinin yetkisiz kişilerin erişimine karşı korunmasını ifade eder (Stamp, 2011; Whitman & Mattord, 2009). Gizlilik, yalnızca verinin içeriğinin okunmasını engellemekle sınırlı değildir; bazı durumlarda iletişimin varlığının dahi gizli tutulması kritik bir gereksinim hâline gelmektedir.

Bilgi gizleme kavramı içerisinde yer alan kriptografi ve steganografi, benzer amaçlara hizmet etseler de yaklaşım ve yöntem bakımından birbirlerinden farklıdır. Kriptografi, mesajı matematiksel işlemlerle şifreleyerek üçüncü taraflar için anlamsız duruma getirirken, mesajın varlığını gizlememektedir (Buchmann & Buchamann, 2004). Steganografi ise mesajı bir taşıyıcı nesnenin içerisine gömerek, bizzat bilginin varlığını dahi gizlemeyi amaçlamaktadır (Kessler & Hosmer, 2011). Bu yönüyle steganografinin temelini oluşturan fark edilmezlik ilkesi, yöntemin tercih edilmesinde belirleyici olmaktadır (Mishra & Bhanodiya, 2015; Wang & Wang, 2004). Kriptografik bir veri potansiyel bir saldırgan için doğrudan bir hedef oluştururken, steganografik veri sıradan bir dijital içerik gibi algılandığından şüphe uyandırmamaktadır. Günümüzde siber güvenlik, istihbarat, dijital adli bilişim ve telif hakkı koruma uygulamaları gibi birçok alanda steganografinin önemi giderek artmaktadır (Dalal & Juneja, 2021).

Steganografinin kökenleri dijital çağdan çok önceye dayanmaktadır (Alabdali & Alzahrani, 2021; Kahn, 1996; Kessler & Hosmer, 2011). Antik Yunan'da Herodot'un aktardığı, mesajın bir kölenin kazınmış kafa derisine yazılarak gizlenmesi ya da balmumu tabletlerin altına kazınan metinler, bilginin fiziksel ortamlar aracılığıyla gizlenmesine yönelik erken dönem uygulamalar olarak kabul edilmektedir. Orta Çağ ve Rönesans dönemlerinde görünmez mürekkepler ve sanatsal eserler içerisine gizlenen semboller, steganografinin hem askeri hem de kültürel bağlamda kullanıldığını göstermektedir. II. Dünya Savaşı sırasında geliştirilen mikro nokta teknolojisi ise, bilginin fark edilmeden taşınması açısından steganografinin stratejik önemini ortaya koyan önemli bir dönüm noktası olmuştur.

Dijital çağın başlamasıyla birlikte steganografi, fiziksel ortamlardan dijital ortamlara taşınmış; taşıyıcı nesneler olarak metin, görüntü, ses, video ve ağ paketleri kullanılmaya başlanmıştır (Bhattacharyya, 2011; Kishor vd., 2016). Dijital görüntülerde piksellerin en az anlamlı bitleri, ses dosyalarındaki frekans bileşenleri veya ağ protokollerinin başlık alanları, veri gizleme amacıyla yaygın biçimde kullanılan ortamlar hâline gelmiştir. Bu çeşitlilik, steganografi çalışmalarında kullanılan yöntemlerin de uzamsal alan, frekans alanı ve adaptif yaklaşımlar gibi farklı teknik sınıflar altında ele alınmasını beraberinde getirmiştir (Dhawan & Gupta, 2021; Majeed vd., 2021).

Steganografik yöntemlerin değerlendirilmesinde yalnızca gizleme işleminin başarıyla gerçekleştirilmesi yeterli görülmemekte; gizlenen verinin algılanabilirliği, taşıyıcı nesne üzerindeki bozulma düzeyi ve sistemin saldırılara karşı dayanıklılığı gibi ölçütler de önem kazanmaktadır. Bu bağlamda, literatürde PSNR, MSE, SSIM ve BER gibi performans ölçütleri yaygın olarak kullanılmaktadır (Beram, 2014; Malik vd., 2025; Setiadi, 2021). Bununla birlikte, steganografi sistemlerinin güvenlik düzeyinin bütüncül biçimde değerlendirilebilmesi için, gizleme yöntemlerinin steganaliz karşısındaki dirençlerinin de incelenmesi gerekmektedir. Steganaliz, gizli verinin varlığını tespit etmeyi amaçlayan yaklaşımları kapsamakta olup, steganografi ve steganaliz arasındaki ilişki alanın metodolojik olgunluğunu belirleyen temel unsurlardan biri olarak değerlendirilmektedir (Dalal & Juneja, 2021; Michaylov & Sarmah, 2025).

Bu çalışmada, steganografi alanında hazırlanmış lisansüstü tezler; kullanılan taşıyıcı ortamlar, tercih edilen yöntem ve teknikler, performans değerlendirme ölçütleri ve steganaliz uygulamalarının varlığı açısından sistematik biçimde incelenmiştir. Böylece alanın Türkiye özelindeki metodolojik eğilimlerinin ortaya konulması ve steganografi çalışmalarının hangi eksenler etrafında şekillendiğinin belirlenmesi amaçlanmıştır.

2. Yöntem

2.1 Araştırma Deseni

Bu çalışma, Türkiye'de steganografi alanında hazırlanmış lisansüstü tezlerin genel görünümünü ortaya koymayı amaçlayan, betimsel nitelikte bir doküman incelemesi olarak tasarlanmıştır. Araştırma kapsamında, farklı üniversite ve enstitülerde yürütülen yüksek lisans ve doktora tezleri sistematik bir yaklaşımla incelenmiş; alanın zamansal gelişimi, kurumsal dağılımı ve yapısal özellikleri bütüncül bir çerçevede ele alınmıştır. Çalışmada, incelenen tezlerden elde edilen nicel veriler betimsel istatistikler kullanılarak analiz edilmiş; tez türü, yayın yılı, üniversite, anabilim dalı ve danışman unvanı gibi değişkenler üzerinden

alanın genel görünümü ortaya konmuştur. Elde edilen bulgular, Türkiye'de steganografi alanındaki akademik üretimin mevcut durumunu betimlemenin yanı sıra, alandaki araştırma yoğunluklarını ve gelişim eğilimlerini görünür kılmayı amaçlamaktadır. Bu doğrultuda çalışma, hem alan yazına bütüncül bir bakış sunmayı hem de gelecekte yapılacak lisansüstü araştırmalar için yol gösterici bir kaynak oluşturmayı hedeflemektedir.

2.2 Veri Kaynağı

Araştırmanın veri kaynağını, Yükseköğretim Kurulu Ulusal Tez Merkezi'nde yer alan lisansüstü tezler oluşturmaktadır (YÖK, 2025). Tezlerin belirlenmesi sürecinde, özet bölümünde "steganografi" ifadesine yer verilen çalışmalar esas alınmış ve bu ölçüt doğrultusunda kapsamlı bir tarama gerçekleştirilmiştir. Bu yaklaşım, çalışmanın doğrudan steganografi alanına odaklanmasını sağlamak ve konu dışı tezlerin araştırma kapsamı dışında bırakılmasını temin etmek amacıyla tercih edilmiştir.

Gerçekleştirilen tarama sonucunda toplam 115 lisansüstü tez tespit edilmiştir. Tezlerin dâhil edilme ve hariç tutulma süreci, sistematik derleme çalışmalarında yaygın olarak kabul gören raporlama standartlarını belirleyen PRISMA ilkeleri çerçevesinde yürütülmüştür. Bu kapsamda, tam metnine erişim sağlanamayan 4 tez çalışma dışı bırakılmış; nihai analizler 111 tez üzerinden gerçekleştirilmiştir. Çalışmaya dâhil edilen tezler; tez türü, yayın yılı, üniversite, enstitü, anabilim dalı, danışman akademik unvanı, tezlerin toplam sayfa sayısı ile içerik yapısını yansıtan tablo ve şekil sayıları gibi ölçütler açısından ayrıntılı biçimde incelenmiştir. Elde edilen nicel veriler, alanın zamansal gelişimini, kurumsal dağılımını ve yapısal özelliklerini ortaya koymak amacıyla betimsel istatistikler kullanılarak analiz edilmiştir.

2.3. Veri Toplama Süreci

Araştırma kapsamında incelenen tezlere ilişkin bibliyografik ve yapısal veriler, Yükseköğretim Kurulu Ulusal Tez Merkezi üzerinden erişilen tezlerin tam metinleri ve özet bölümleri incelenerek manuel olarak toplanmıştır (YÖK, 2025). Veri toplama sürecinde, her bir tezin sistematik ve tutarlı biçimde değerlendirilmesini sağlamak amacıyla önceden belirlenmiş değişkenler esas alınmıştır. Bu doğrultuda; tez türü, yayın yılı, üniversite, enstitü, anabilim dalı, danışman akademik unvanı, toplam sayfa sayısı ile tezlerde yer alan tablo ve şekil sayıları gibi ölçütleri içeren bir veri kayıt formu hazırlanmıştır. İlgili bilgiler, her tez için ayrı ayrı olmak üzere doğrudan tez metinlerinden kontrol edilerek forma işlenmiştir. Veri girişleri sırasında olası hata ve tutarsızlıkların önüne geçmek amacıyla, eksik ya da belirsiz bilgiler tekrar gözden geçirilmiş ve gerekli durumlarda tezler çapraz olarak yeniden incelenmiştir. Tezlere

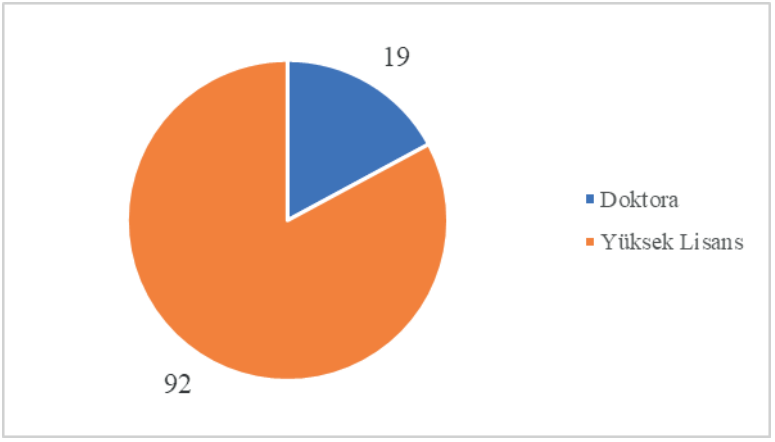
ait anabilim dalı ve bölüm bilgileri, orijinal haliylle kaydedilmiş ve analiz aşamasında karşılaştırılabilirlik sağlamak amacıyla yeniden sınıflandırılmak üzere korunmuştur. Toplanan veriler, analiz sürecine uygun biçimde tablolaştırılmış ve betimsel istatistiksel işlemlere hazır hâle getirilmiştir. Bu süreçte, verilerin araştırmanın amaçlarıyla uyumlu, karşılaştırılabilir ve tekrarlanabilir olmasına özen gösterilmiştir.

2.4. Veri Analizi

Araştırma kapsamında elde edilen nicel veriler, betimsel istatistik yöntemleri kullanılarak analiz edilmiştir. Bu doğrultuda; tez türü, yayın yılı, üniversite, enstitü, anabilim dalı ve danışman unvanı gibi değişkenlere ilişkin veriler frekans ve yüzde değerleri üzerinden değerlendirilmiştir. Nicel bulguların daha anlaşılır ve karşılaştırılabilir biçimde sunulabilmesi amacıyla, elde edilen sonuçlar tablolar ve grafikler aracılığıyla görselleştirilmiştir. Tezlerin anabilim dalı ve bölüm adlarının üniversiteler arasında farklılık göstermesi nedeniyle, bu değişkene ilişkin veriler analiz aşamasında yeniden sınıflandırılmıştır. Bu kapsamda, içerik benzerliği ve disipliner yakınlıktan yola çıkarak farklı adlandırmalara sahip ancak benzer akademik odağı paylaşan programlar ortak gruplar altında birleştirilmiştir.

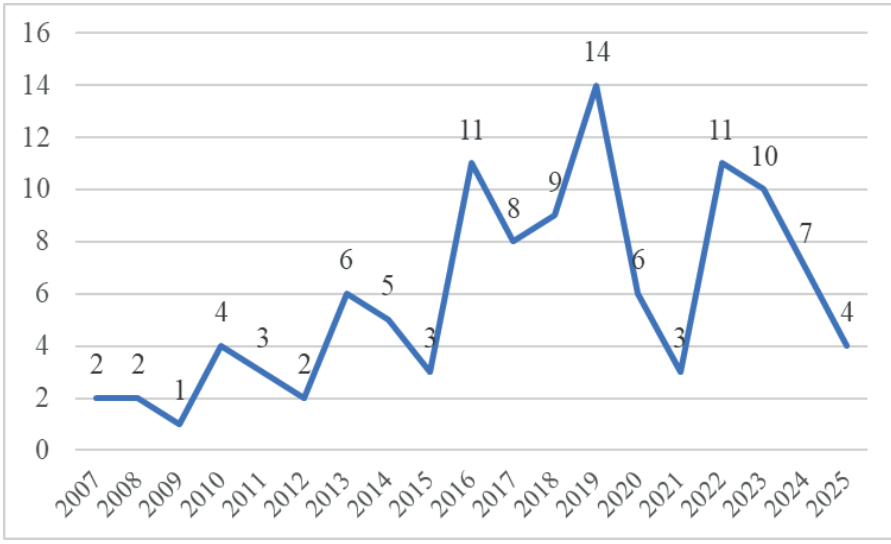
Nitel verilerin analizinde ise betimsel analiz yaklaşımı benimsenmiştir. Bu amaçla, tezlerin özet ve anahtar kelime bölümlerinde yer alan ifadeler incelenmiş; sık tekrar eden kavramlar belirlenerek kavramsal yoğunluklar ortaya konmuştur. Elde edilen kavramlar doğrultusunda oluşturulan anahtar kelime bulutu, steganografi alanındaki baskın temaların, yöntemsel eğilimlerin ve araştırma odaklarının görsel olarak yorumlanmasına imkân sağlamıştır. Analiz sürecinin son aşamasında, nicel ve nitel bulgular birlikte ele alınarak toplam bir değerlendirme yapılarak tartışılmıştır. Bu yaklaşım sayesinde, Türkiye'de steganografi alanında yürütülen lisansüstü çalışmaların mevcut durumu ve gelişim yönelimleri kapsamlı biçimde ortaya konmuştur.

3. Bulgular



Şekil 1 Tez türüne göre dağılımı

Şekil 1'de tez türlerine göre dağılım incelendiğinde, çalışmaya dâhil edilen lisansüstü tezlerin büyük çoğunluğunu yüksek lisans tezlerinin oluşturduğu görülmektedir. Toplam 111 tezin %82,9'u (n=92) yüksek lisans, %17,1'i (n=19) ise doktora tezlerinden oluşmaktadır. Bu dağılım, steganografi alanındaki akademik çalışmaların ağırlıklı olarak yüksek lisans düzeyinde yürütüldüğünü, doktora düzeyindeki çalışmaların ise daha sınırlı kaldığını göstermektedir. Doktora tezlerinin sayıca daha az olması, alanın henüz derinlemesine ve uzun soluklu araştırmalar açısından gelişim sürecinde olduğuna işaret edebileceği gibi, konunun çoğunlukla uygulama ve yöntem geliştirme odaklı ele alındığını da akla getirir. Şekil 2' de tezlerin yıllara göre dağılımı görülmektedir.



Şekil 2 Yıllara göre tez sayısı

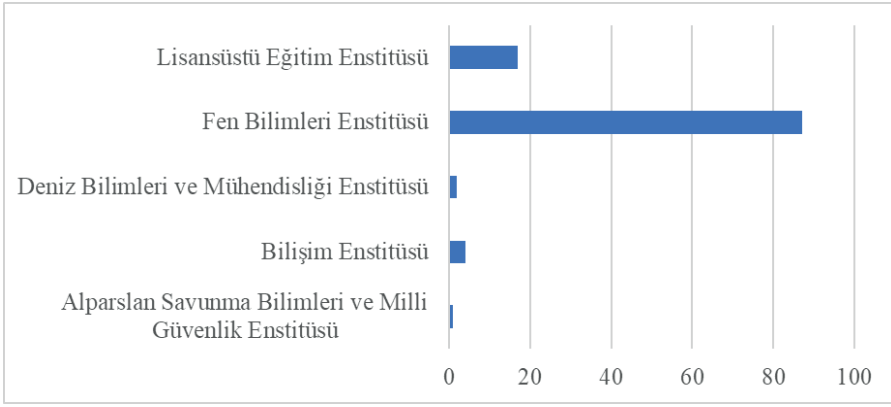
Şekil 2'de yer alan çizgi grafikten elde edilen bulgular, steganografi alanındaki lisansüstü çalışmaların zamansal gelişiminin üç temel evrede değerlendirilebileceğini göstermektedir. İlk evreyi oluşturan 2007–2012 yılları arasında tez sayılarının düşük seviyede seyretmesi, alanın Türkiye'de sınırlı sayıda araştırmacı tarafından ele alındığını ve henüz yaygınlaşmadığını düşündürmektedir. İkinci evre olarak değerlendirilebilecek 2013–2019 döneminde ise tez sayılarında belirgin bir artış eğilimi dikkat çekmektedir. Özellikle 2016 ve 2019 yıllarında gözlenen yükselişler, bilgi güvenliği, veri gizleme ve dijital medya teknolojilerindeki gelişmelerin steganografiye olan akademik ilgiyi artırmış olabileceğine işaret etmektedir. Üçüncü evrede (2020 ve sonrasında) tez sayılarında dalgalı bir yapı görülmekle birlikte, yıllık üretimin belirli bir seviyenin altına düşmemesi, alanın akademik gündemde kalmaya devam ettiğini göstermektedir. Bu dalgalanmanın, küresel ölçekte yaşanan pandemi süreci, araştırma önceliklerindeki değişimler, yapay zeka çalışmalarının ortaya çıkışı ve lisansüstü eğitim dinamikleriyle ilişkili olabileceği değerlendirilmektedir. Tablo 1'de üniversitelere göre tezlerin dağılımı yer almaktadır.

Tablo 1 Üniversitelere Göre Tezlerin Dağılımı

Üniversite	Program sayısı
Altınbaş Üniversitesi	11
Gazi Üniversitesi	10
Fırat Üniversitesi	8
Selçuk Üniversitesi	8
İstanbul Aydın Üniversitesi	6
Düzce Üniversitesi	5
Ankara Üniversitesi	4
İstanbul Ticaret Üniversitesi	4
Kocaeli Üniversitesi	4
Sakarya Üniversitesi	4
Trakya Üniversitesi	4
Çankaya Üniversitesi	3
Ankara Yıldırım Beyazıt Üniversitesi	2
Atılım Üniversitesi	2
Başkent Üniversitesi	2
Deniz Harp Okulu Komutanlığı	2
Gaziantep Üniversitesi	2
İstanbul Teknik Üniversitesi	2
Kadir Has Üniversitesi	2
Karadeniz Teknik Üniversitesi	2
Üsküdar Üniversitesi	2

Tablo 1'de, çalışmaların belirli üniversitelerde yoğunlaştığı görülmektedir. En yüksek tez sayısına sahip olan Altınbaş Üniversitesi (n=11) ve Gazi Üniversitesi (n=10), alanın kurumsal düzeyde en aktif üretim merkezleri olarak öne çıkmaktadır. Bu üniversiteleri Fırat Üniversitesi ve Selçuk Üniversitesi (n=8) takip etmektedir. Bu dağılım, steganografi alanındaki akademik üretimin hem devlet hem de vakıf üniversitelerinde var olduğunu göstermektedir. Ayrıca, tezlerin farklı üniversitelere dağılmış olması, alanın belirli merkezlerle sınırlı kalmadığını; Türkiye genelinde farklı akademik birimlerde çalışıldığını ortaya koymaktadır. Çok sayıda tezin ise belirli üniversitelerde kümelenmesi, bu kurumlarda konuya ilişkin akademik kadro birikimi, danışman uzmanlaşması veya lisansüstü programların teknik altyapı yeterlilikleriyle ilişkili olabilir. Ek olarak, dağılımın homojen olmaması, steganografi alanında kurumsal uzmanlaşmanın henüz sınırlı sayıda üniversitede yoğunlaştığını göstermektedir.

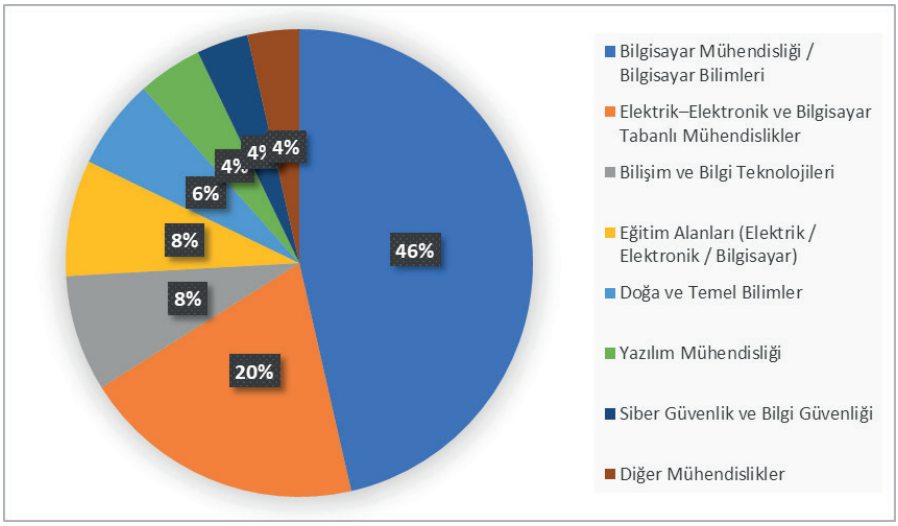
Bu durum, alanın Türkiye'de gelişmekte olan ancak belirli araştırma merkezlerinde derinleşen bir yapıya sahip olduğunu düşündürmektedir. Şekil 3'te üniversitelere göre tezlerin dağılımı gösterilmektedir.



Şekil 3 Enstitülere göre tezlerin dağılımı

Şekil 3 incelendiğinde, steganografi alanındaki lisansüstü tezlerin çok büyük bir bölümünün fen bilimleri enstitüsü bünyesinde hazırlandığı görülmektedir (n=87). Bu sayı, toplam tezlerin açık ara çoğunluğunu oluşturmakta olup, alanın teknik ve mühendislik temelli bir disiplin olarak konumlandığını açık biçimde ortaya koymaktadır. Bunu, 17 tez ile lisansüstü eğitim enstitüsü izlemektedir. Lisansüstü Eğitim Enstitülerinin son yıllarda birçok üniversitede farklı enstitülerin birleştirilmesiyle oluşturulduğu dikkate alındığında, bu sayı yapısal dönüşümün bir yansıması olarak değerlendirilebilir.

Bilişim Enstitüsü (n=4) ve Deniz Bilimleri ve Mühendisliği Enstitüsü (n=2) bünyesinde hazırlanan tezler ise alanın belirli alt uzmanlık alanlarında da çalışıldığını göstermektedir. En düşük tez sayısının Alparslan Savunma Bilimleri ve Milli Güvenlik Enstitüsü bünyesinde görülmesi (n=1) ise daha sınırlı kaldığını göstermektedir. Bu durum, gelecekte disiplinler arası çalışmalar için potansiyel bir gelişim alanı olarak değerlendirilebilir. Şekil 4'te alanlara göre tezlerin dağılımı yer almaktadır.

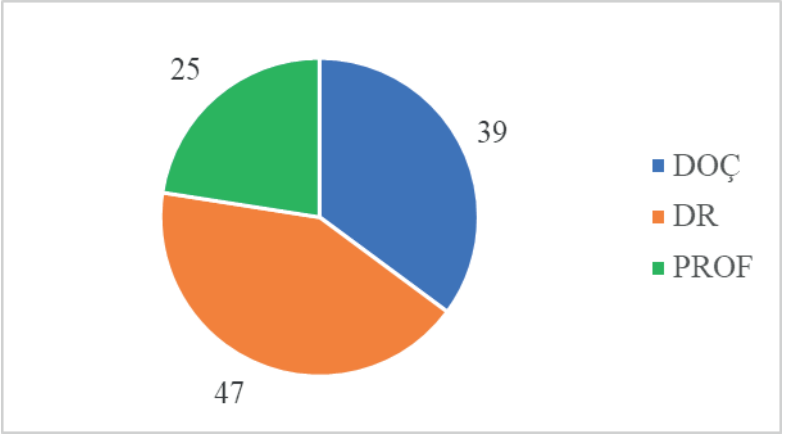


Şekil 4 Alanlara göre tezlerin dağılımı

Şekil 4 ele alındığında, tezlerin büyük ölçüde bilgisayar temelli mühendislik disiplinlerinde yoğunlaştığı anlaşılmaktadır. Toplam 111 tezin 52'si (%46,8) Bilgisayar Mühendisliği / Bilgisayar Bilimleri grubunda yer almaktadır. Bu oran, alanın neredeyse yarısının doğrudan bilgisayar bilimi paradigması içinde üretildiğini göstermektedir. Bunu 22 tez (%19,8) ile Elektrik-Elektronik ve Bilgisayar Tabanlı Mühendislikler grubu takip etmektedir. Bu bulgu, steganografinin yalnızca yazılım veya algoritma düzeyinde değil; sinyal işleme, gömülü sistemler ve haberleşme temelli mühendislik alanlarıyla da güçlü bir ilişki içinde olduğunu göstermektedir. Bu iki grup birlikte değerlendirildiğinde, toplam tezlerin yaklaşık %66'sının doğrudan mühendislik ve teknik altyapı odaklı disiplinlerde üretildiği anlaşılmaktadır. Bu durum, steganografinin Türkiye'de ağırlıklı olarak teknik, algoritmik ve uygulama temelli bir araştırma alanı olarak konumlandığını ortaya koymaktadır.

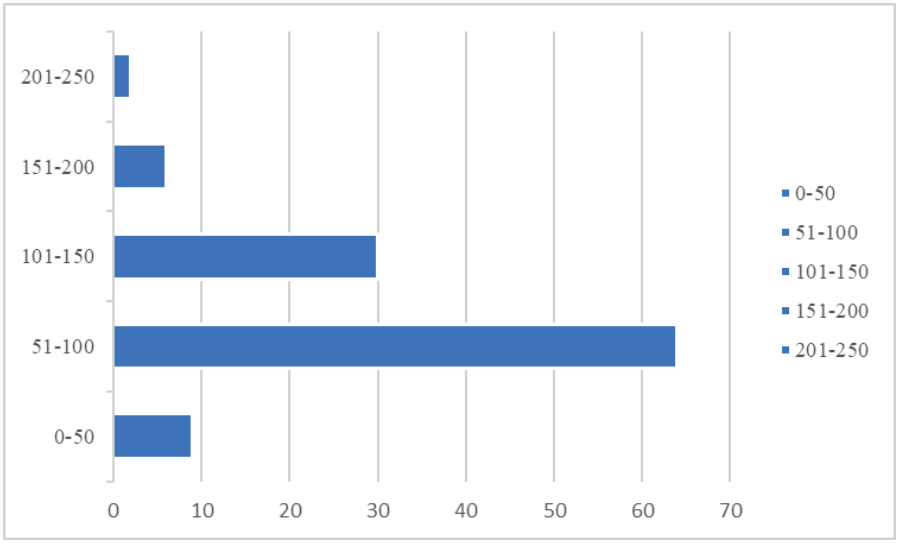
Bilişim ve Bilgi Teknolojileri (%8,1) ile Eğitim Alanları (Elektrik / Elektronik / Bilgisayar) (%8,1) gruplarının benzer oranlara sahip olması dikkat çekicidir. Özellikle eğitim temelli programlarda üretilen tezler, alanın pedagojik veya uygulamalı öğretim boyutunun da ele alındığını göstermektedir. Buna karşılık, doğrudan Siber Güvenlik ve Bilgi Güvenliği grubunda yer alan tezlerin oranının %3,6 gibi görece düşük bir seviyede kalması önemli bir bulgudur. Steganografi doğası gereği bilgi gizleme ve güvenli iletişimle doğrudan ilişkili olmasına rağmen, çalışmaların çoğunun "siber güvenlik" etiketi altında değil, daha çok bilgisayar mühendisliği şemsiyesi altında yürütülmesi dikkat çekmektedir. Alanın kurumsal olarak güvenlik disiplininden ziyade

teknik mühendislik disiplinleri içinde konumlandığı düşünülebilir. Doğa ve Temel Bilimler (%6,3) ile Diğer Mühendislikler (%3,6) gruplarındaki tez sayılarının sınırlı olması, steganografinin matematiksel kuramsal çerçevede veya disiplinlerarası modelleme bağlamında henüz güçlü bir temsil alanı bulamadığını işaret eder. Özellikle matematik ve hesaplamalı bilimler temelli çalışmaların düşük oranı, alanın teorik derinleşmeden ziyade uygulama geliştirme odaklı ilerlediğini ortaya koyar. Şekil 5'te danışman unvanına göre tezlerin dağılımı gösterilmektedir.



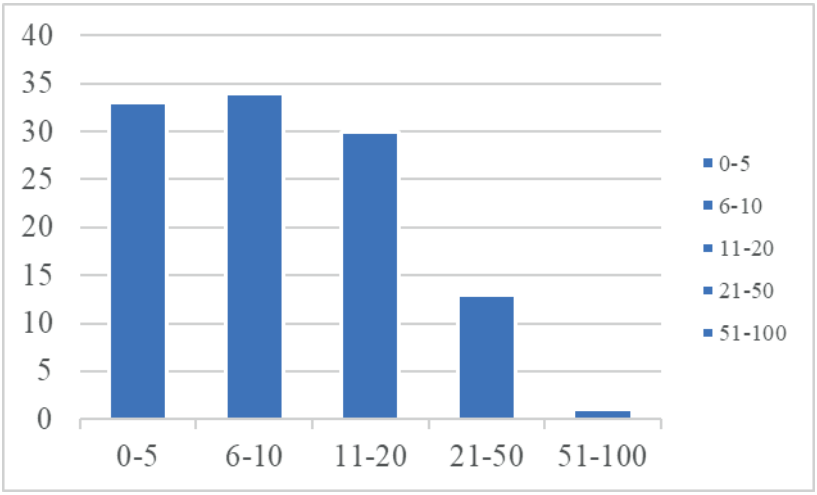
Şekil 5 Danışman unvanına göre tezlerin dağılımı

Şekil 5'e bakıldığında, 47 tezin doktor, 39 tezin doçent ve 25 tezin profesör unvanına sahip akademisyenler tarafından yürütüldüğü görülmektedir. Bilişim ve mühendislik temelli araştırma alanlarında, aktif proje üretimi ve uygulama geliştirme süreçlerinde daha yoğun rol alan Dr. ve Doç. unvanlarının tez danışmanlığında daha yüksek sayılara ulaşması yapısal bir durum olarak değerlendirilebilir. En yüksek sayının 47 tez ile Dr. grubunda yer alması, alanın uygulama ve teknik geliştirme odaklı niteliğiyle uyumludur. Profesör danışman sayısının 25 olması ise steganografinin görece yeni ve dinamik bir araştırma alanı olması nedeniyle orta kuşak akademisyenler tarafından daha yoğun sahiplenildiği şeklinde yorumlanabilir. Genel dağılım, alanın yalnızca belirli bir akademik unvan grubunun tekelinde olmadığını; farklı kıdem düzeylerinden akademisyenlerin katkısıyla sürdürüldüğünü göstermektedir. Şekil 6'da sayfa sayılarına göre tezlerin dağılımı yer almaktadır.



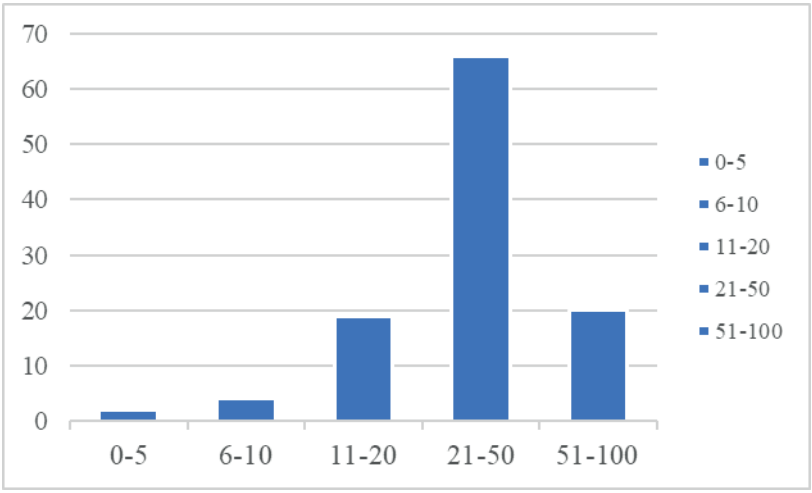
Şekil 6 Sayfa sayılarına göre tezlerin dağılımı

Şekil 6 incelendiğinde, çalışmaların büyük bölümünün 51–100 sayfa aralığında yoğunlaştığı görülmektedir (n=64). Bu aralığı 101–150 sayfa aralığında yer alan 30 tez izlemektedir. Buna karşılık 0–50 sayfa aralığında 9, 151–200 sayfa aralığında 6 ve 201–250 sayfa aralığında yalnızca 2 tez bulunmaktadır. Bu dağılım, tezlerin ağırlıklı olarak orta hacimli çalışmalar şeklinde hazırlandığını göstermektedir. 51–100 sayfa aralığındaki belirgin yoğunluk, çalışmaların büyük bölümünün belirli bir yöntem, veri seti ve performans analizi çerçevesinde yapılandırıldığını düşündürmektedir. 101–150 sayfa aralığında yer alan tezler ise görece daha kapsamlı literatür taraması ve deneysel karşılaştırmalar içeren araştırmalara işaret etmektedir. 151 sayfa ve üzerindeki tezlerin sınırlı sayıda olması, alan çalışmalarının çoğunlukla belirli bir teknik yaklaşım veya uygulama problemi etrafında kurgulandığını göstermektedir. 201–250 sayfa aralığındaki düşük frekans ise oldukça geniş kapsamlı ve derinlemesine yapılandırılmış çalışmaların nispeten daha az üretildiğini ortaya koymaktadır. Şekil 7'de Tablo sayısına göre tezlerin dağılımı gösterilmektedir.



Şekil 7 Tablo sayısına göre tezlerin dağılımı

Şekil 7'ye bakıldığında, çalışmaların büyük bölümünün 0–10 tablo aralığında yoğunlaştığı görülmektedir. 6–10 tablo aralığında 34 tez, 0–5 tablo aralığında ise 33 tez bulunmaktadır. Bu durum, araştırmaların önemli bir kısmında tablo kullanımının sınırlı düzeyde tutulduğunu göstermektedir. 11–20 tablo aralığında yer alan 30 tez, orta yoğunlukta tablo kullanımına sahip çalışmaların da önemli bir yer tuttuğunu ortaya koymaktadır. Buna karşılık 21–50 tablo aralığında yalnızca 13 tez bulunması, yüksek yoğunluklu tablo kullanımının daha sınırlı olduğunu göstermektedir. 51–100 tablo aralığında sadece 1 tez yer alması ise aşırı yoğun tablo temelli raporlamanın istisnai olduğunu ortaya koymaktadır. Buna göre, steganografi alanındaki lisansüstü tezlerin çoğunlukla görsel veri sunumunu dengeli ve sınırlı bir çerçevede kullandığı; aşırı tablo yoğunluğuna dayalı büyük ölçekli veri analizlerinin ise oldukça nadir olduğu söylenebilir. Şekil 8'de şekil sayısına göre tezlerin dağılımı yer almaktadır.



Şekil 8 Şekil sayısına göre tezlerin dağılımı

Şekil 8 ele alındığında, çalışmaların büyük bölümünün 21–50 şekil aralığında yoğunlaştığı görülmektedir (n=66). Bu aralık açık ara en yüksek frekansa sahiptir ve toplam tezlerin yarısından fazlasını oluşturmaktadır. 51–100 şekil aralığında yer alan 20 tez ise görsel yoğunluğu yüksek çalışmaların da önemli bir yer tuttuğunu göstermektedir.11–20 şekil aralığında 19 tez bulunması, orta düzeyde görsel kullanımının da yaygın olduğunu ortaya koymaktadır. Buna karşılık 0–5 (n=2) ve 6–10 (n=4) aralıklarında yer alan tezlerin oldukça sınırlı sayıda olması, düşük görsel içerikli çalışmaların istisnai kaldığını göstermektedir. Bu dağılım, steganografi alanındaki lisansüstü tezlerin tablo kullanımındaki sınırlılığa karşın büyük ölçüde görsel temelli raporlamaya dayandığını ortaya koymaktadır. Tablo 2'de görüntü dışı steganografi ortamlarına göre tezlerin dağılımı yer almaktadır.

Tablo 2 Görüntü Dışı Steganografi Ortamlarına Göre Tez Dağılımı

Steganografi Ortamı	Tez Sayısı
Metin	8
Ses	8
Video	7
Ağ	8

Tablo 2 incelendiğinde, görüntü dışı steganografi ortamları arasında tez dağılımının oldukça dengeli olduğu görülmektedir. Metin (n=8), ses (n=8) ve ağ (n=8) ortamları eşit sayıda çalışmaya konu olurken, video

ortamında 7 tez bulunmaktadır. Buradan anlaşılacağı üzere, araştırmacıların görüntü temelli steganografi dışında farklı veri taşıyıcı ortamlarına da benzer düzeyde ilgi gösterdiği görülmektedir. Özellikle metin, ses ve ağ tabanlı steganografi çalışmalarının eşit sayıda olması, bu alanların metodolojik ve uygulama açısından birbirine yakın araştırma potansiyeline sahip olduğunu düşündürmektedir. Video ortamındaki tez sayısının bir miktar daha düşük olması (n=7) ise bu alandaki teknik karmaşıklık, yüksek veri boyutu ve işlem maliyetleri gibi faktörlerle ilişkili olabilir; ancak dağılım genel olarak değerlendirildiğinde "ortamlar arasında belirgin bir fark yoktur. Tablo 3'te steganografi çalışmalarında kullanılan yöntemler ifade edilmektedir.

Tablo 3 Steganografi Çalışmalarında Kullanılan Yöntemler

Kategori	Yöntem	Tez Sayısı
Kriptografi	AES	10
	DES	4
	RSA	5
Steganografi Tekniği	LSB	45
	DCT	5
Yapay Zeka	CNN	2

Tablo 3 değerlendirildiğinde, steganografi çalışmalarının ağırlıklı olarak geleneksel gizleme teknikleri üzerine yoğunlaştığı görülmektedir. Özellikle LSB (Least Significant Bit) yönteminin açık ara en sık tercih edilen teknik olması, alanın önemli ölçüde uzamsal alan (spatial domain) temelli yaklaşımlar etrafında şekillendiğini göstermektedir. LSB'nin uygulama kolaylığı, düşük hesaplama maliyeti ve hızlı sonuç üretmesi, lisansüstü tez çalışmalarında tercih edilmesinde belirleyici faktörler olarak değerlendirilebilir. Bununla birlikte, bu durum aynı zamanda literatürde yöntemsel çeşitliliğin sınırlı kaldığına da işaret etmektedir. Frekans alanına dayalı tekniklerden DCT'nin daha sınırlı sayıda tezde yer alması, transform domain yaklaşımlarının görece daha teknik ve karmaşık yapısı ile ilişkilendirilebilir. Ancak literatürde DCT tabanlı yöntemlerin dayanıklılık açısından avantajlı olduğu bilinmesine rağmen tezlerde sınırlı temsil edilmesi, araştırmaların daha çok uygulama odaklı ve temel düzeyde kaldığını düşündürmektedir.

Kriptografik algoritmaların (AES, DES, RSA) belirli sayıda tezde kullanılmış olması, steganografinin tek başına yeterli görülmediği ve çoğu çalışmada veri gizleme öncesinde ek bir güvenlik katmanı oluşturma eğiliminin bulunduğunu göstermektedir. Özellikle AES'in diğer kriptografik yöntemlere kıyasla daha fazla tercih edilmesi, güncel güvenlik standartlarıyla uyumlu ve

daha güçlü kabul edilen algoritmaların akademik çalışmalara yansıdığını ortaya koymaktadır. DES'in daha sınırlı kullanımı ise, algoritmanın güncel güvenlik gereksinimlerini karşılamada zayıf kalmasıyla açıklanabilir.

Yapay zekâ tabanlı yöntemlerin, özellikle CNN temelli yaklaşımların, sınırlı sayıda tezde yer alması ise alanın henüz dönüşüm sürecinde olduğunu göstermektedir. Derin öğrenme tekniklerinin hem gizleme hem de steganaliz süreçlerinde artan önemi dikkate alındığında, mevcut dağılım geleneksel yöntemlerin hâlen baskın olduğunu, ancak yeni nesil yaklaşımların akademik literatüre giriş yapmaya başladığını ortaya koymaktadır. Tablo 4'te steganografi çalışmalarında kullanılan performans ölçütleri yer almaktadır.

Tablo 4 Steganografi Çalışmalarında Kullanılan Performans Ölçütleri

Performans Ölçütü	Tez Sayısı (n)
PSNR	35
MSE	18
SSIM	15
BER	11

Tablo 4 incelendiğinde, tezlerde en sık kullanılan performans ölçütünün PSNR olduğu görülmektedir (n=35). Bu metriği MSE (n=18) ve SSIM (n=15) izlemektedir. BER ise 11 tezde kullanılmıştır. Bu durum, çalışmaların ağırlıklı olarak görüntü kalitesini ölçmeye odaklandığını göstermektedir. PSNR'nin açık ara önde olması, özellikle görüntü steganografisi çalışmalarında gizleme sonrasında oluşan kalite kaybını sayısal olarak ifade etme ihtiyacının belirleyici olduğunu düşündürmektedir. MSE'nin de görece yüksek bir kullanım oranına sahip olması, piksel düzeyindeki hata analizinin hâlâ temel değerlendirme araçlarından biri olduğunu göstermektedir. SSIM'in daha sınırlı sayıda çalışmada yer alması ise algısal benzerliği dikkate alan ölçütlerin klasik hata temelli metriklere kıyasla daha az tercih edildiğini ortaya koymaktadır. Bu durum, performans değerlendirmesinde geleneksel kalite metriklerinin hâlen baskın olduğunu göstermektedir. BER'in 11 tezde kullanılmış olması, dayanıklılık ve hata oranı analizlerinin tamamen ihmal edilmediğini; ancak kalite temelli ölçütlere kıyasla daha geri planda kaldığını düşündürmektedir. Özellikle saldırı, sıkıştırma veya iletim hataları gibi senaryolara karşı sistem performansını ölçen çalışmaların sayısının görece sınırlı olduğu söylenebilir. Şekil 8'de anahtar kelime bulutu görünümü yer almaktadır. Şekil 9'da anahtar kelime bulutu görülmektedir.

Şekil 9 Anahtar kelime bulutu

Şekil 9'da yer alan kelime bulutu, bilgi gizleme ve steganografi alanının Türkiye'de nasıl kavramsallaştırıldığını, hangi teknik ve kuramsal eksenler etrafında yoğunlaştığını açık biçimde yansıtan, çok katmanlı bir görsel özet sunmaktadır. Görselin yorumlanmasında yalnızca en büyük ve baskın kavramlara odaklanmak yeterli değildir; aynı zamanda kavramların birlikte görünme biçimleri, oluşturdukları kümeler ve aralarındaki örtük ilişkiler dikkate alınmalıdır.

Öncelikle "Steganografi", "Bilgi Gizleme" ve "Veri Gizleme" kavramlarının merkezî ve baskın biçimde yer alması, alanın çekirdeğinin gizli bilginin fark edilmeden saklanması ve iletilmesi problematiği etrafında şekillendiğini göstermektedir. Bu durum, çalışmaların büyük ölçüde steganografiyi bağımsız bir teknik alan olarak değil; bilgi güvenliği ve gizli iletişim bağlamının temel bir bileşeni olarak ele aldığını düşündürmektedir. "Veri gizleme" kavramının öne çıkması, steganografinin yalnızca teorik bir gizleme problemi olarak değil, uygulanabilir ve sistematik bir veri koruma yaklaşımı olarak konumlandırıldığını göstermektedir.

İkinci belirgin kavramsal küme, "LSB", "DCT", "JPEG", "MSE", "PSNR" ve "Histogram" gibi terimler etrafında oluşmaktadır. Bu kümelenme, çalışmaların ağırlıklı olarak sayısal görüntü işleme temelli, ölçülebilir performans kriterlerine dayanan ve deneysel doğrulamayı önceleyen bir yaklaşımı benimsediğini ortaya koymaktadır. Özellikle LSB'nin belirgin biçimde öne çıkması, literatürde klasik ve kolay uygulanabilir yöntemlerin hâlen yaygın biçimde kullanıldığını;

PSNR ve MSE gibi metriklerin görünürlüğü ise çalışmaların algılanamazlık ve bozulma düzeyini nicel olarak kanıtlama kaygısını yansıttığını göstermektedir.

Üçüncü önemli katman, "Kriptografi", "Şifreleme", "AES", "DES" ve "RSA" gibi kavramlarla temsil edilen güvenlik merkezli yaklaşımlardır. Bu küme, steganografinin çoğu zaman kriptografik yöntemlerle birlikte veya hibrit yapılar içinde ele alındığını göstermektedir. Gizli bilginin yalnızca saklanması değil, aynı zamanda içeriğinin de korunması hedeflenmekte; bu durum steganografi–kriptografi bütünleşmesinin güçlü bir araştırma yönelimi olduğunu ortaya koymaktadır.

Ayrıca "Ses Steganografisi", "Görüntü Steganografisi" ve "Video Steganografisi" kavramlarının birlikte görünmesi, çalışmaların tek bir medya türüyle sınırlı kalmadığını; farklı taşıyıcı ortamlar üzerinden gizleme tekniklerinin karşılaştırmalı veya paralel biçimde ele alındığını göstermektedir. Ancak bu kümelenme içinde görüntü steganografisinin daha baskın olması, pratikte görsel verilerin hâlen en yaygın ve tercih edilen kapak ortamı olduğunu düşündürmektedir.

4. Tartışma ve Sonuç

Bu çalışmada, Türkiye'de steganografi alanında hazırlanmış lisansüstü tezler; tür, yıl, üniversite, enstitü, çalışma alanı, danışman unvanı, sayfa sayısı, tablo-şekil kullanımı, kullanılan yöntemler, taşıyıcı ortamlar ve performans ölçütleri açısından sistematik olarak incelenmiştir. Sonuçlar, alanın genel görünümünü ortaya koymanın yanı sıra metodolojik eğilimler ve araştırma boşlukları hakkında da önemli ipuçları sunmaktadır.

Ulaşılan sonuçlar, alanın metodolojik bir olgunluğa eriştiğini ancak belirli teknik kalıpların dışına çıkmakta henüz direnç gösterdiğini ortaya koymaktadır. Tezlerin büyük çoğunluğunun yüksek lisans düzeyinde olması (%82,9), steganografinin Türkiye'de doktora düzeyinde henüz yeterli derinliğe ulaşmadığını göstermektedir. Doktora düzeyindeki çalışmaların %17,1 gibi sınırlı bir oranda kalması, alanın kuramsal derinleşme ve uzun soluklu araştırma projeleri üretme kapasitesinin henüz gelişim aşamasında olduğuna işaret etmektedir. Yıllara göre dağılım, 2013 sonrasında belirgin bir artış olduğunu, ancak 2020'den itibaren dalgalı bir seyir izlendiğini ortaya koymaktadır. Bu durum, küresel ölçekte yaşanan pandemi süreci, araştırma önceliklerindeki değişimler ve yapay zekâ çalışmalarının yükselişiyle ilişkili olabilir (Invernici vd., 2024; Singh, 2025).

Üniversite bazlı dağılım, Altınbaş ve Gazi üniversitelerinin öne çıktığını, ancak üretimin tekelleşmediğini göstermektedir. Fen Bilimleri Enstitüleri'nin açık ara önde olması, steganografinin Türkiye'de ağırlıklı olarak mühendislik

temelli bir disiplin olarak konumlandığını doğrulamaktadır. Buna karşın, sosyal bilimler veya disiplinler arası programlarda yürütülen tezlerin yok denecek kadar az olması, alanın teknik yönünün baskınlığını pekiştirmektedir.

Steganografinin kurumsal olarak "Siber Güvenlik" programlarından ziyade (%3,6), doğrudan "Bilgisayar Mühendisliği" (%46,8) çalışma alanı altında ele alınmaktadır. Bu durum, steganografinin Türkiye'deki akademik algıda bir savunma ya da güvenlik disiplininden çok, algoritmik bir veri işleme problemi olarak konumlandırıldığını ortaya koymaktadır. Doğa ve Temel Bilimler programlarındaki düşük temsil oranı ise, alanın matematiksel ve teorik modelleme boyutunun uygulama odaklı yaklaşımların gölgesinde kaldığını desteklemektedir.

Yöntemsel eğilimler açısından LSB tekniğinin (%40,5 ile 45 tez) ve PSNR (%31,5) ölçütünün baskınlığı, ulusal literatürün uygulama kolaylığı ve düşük maliyetli çözümlere yöneldiğini kanıtlamaktadır. LSB'nin kullanım avantajına rağmen, modern güvenlik ihtiyaçları karşısındaki zayıflığı bilinmektedir (Abdulhameed Alher vd., 2024; Tran vd., 2022). Buna karşın, uluslararası literatürde derin öğrenme tabanlı (CNN, GAN) steganografi ve steganaliz çalışmaları hızla artarken (Malik vd., 2025; Michaylov & Sarmah, 2025) Türkiye'deki tezlerde bu yöntemlerin oldukça sınırlı kalması, küresel akıllı steganografi eğilimlerinin ulusal literatüre entegrasyonunda kısmi bir gecikme yaşandığını göstermektedir. Öte yandan, steganografinin AES gibi algoritmalarla hibritlenmesi, verinin hem varlığını hem içeriğini korumaya yönelik güçlü bir güvenlik farkındalığının geliştiğine işaret etmektedir (Badhan & Malhi, 2024; Banoori vd., 2025). Taşıyıcı ortam çeşitliliği açısından metin, ses, video ve ağ steganografisi üzerine yapılan çalışmaların sayıca dengeli olması olumludur. Buna karşın, görüntü steganografisinin hâlâ baskın olması, araştırmacıların geleneksel medya türlerine yöneldiğini, güncel taşıyıcılar konusunda ise henüz yeterli çalışma yapılmadığını ortaya koymaktadır.

Çalışmanın en dikkat çekici sonuçlarından biri, gizleme tekniklerine odaklanan (Das vd., 2011), yoğun literatüre kıyasla steganaliz çalışmalarının geri planda kalmış olmasıdır. Literatürün sağlıklı bir dönüşüm sürecine girebilmesi için gizleme yöntemleri kadar, bu yöntemleri deşifre edecek savunma mekanizmalarının da akademik gündeme taşınması kritik bir gerekliliktir.

Sonuç olarak, Türkiye'de steganografi alanındaki lisansüstü tezler; teknik, deneysel ve performans odaklı bir çizgide ilerlemekte klasik yöntemler hâlâ baskınlığını korurken kriptografi ile bütünleşik yaklaşımlar da önemli bir yer tutmaktadır. Bununla birlikte, yapay zekâ tabanlı yöntemler, frekans alanı teknikleri, steganaliz odaklı çalışmalar ve disiplinler arası yaklaşımlar açısından önemli boşluklar bulunmaktadır (Alhomoud, 2021; Laishram & Tuithung,

2018). Gelecek araştırmaların bu alanlara yönelmesi hem ulusal alanyazının zenginleşmesine hem de uluslararası düzeyde rekabet edebilirliğin artmasına katkı sağlayacaktır.

Kaynaklar

Abdulhameed Alher, Z., M Al Imran, B., & Al Ali, I. (2024). LSB as a steganography tool in information security. *5th International Conference on Communication Engineering and Computer Science (CIC-COCOS'24)*, 348-355.

Alabdali, N., & Alzahrani, S. (2021). An overview of steganography through history. *Int. J. Sci. Eng. Sci*, *5*, 41-44.

Alhomoud, A. M. (2021). Image steganography in spatial domain: Current status, techniques, and trends. *Intelligent Automation & Soft Computing*, *27*(1).

Badhan, A., & Malhi, S. S. (2024). A Review on Hybrid Cryptography approach with Steganography. *2024 12th International Conference on Internet of Everything, Microwave, Embedded, Communication and Networks (IEMECON)*, 1-7.

Banoori, S. Z., Khan, W., Rahman, S., Masood, F., Salam, A., Amin, F., De La Torre, I., Villar, M. G., Garay, H., & Choi, G. S. (2025). An improved hybrid image steganography method using AES algorithm. *Scientific Reports*.

Beram, F. G. (2014). Effective parameters of image steganography techniques. *International Journal of Computer Applications Technology and Research*, *3*(6), 361-363.

Bhattacharyya, S. (2011). A survey of steganography and steganalysis technique in image, text, audio and video as cover carrier. *Journal of global research in computer science*, *2*(4).

Buchmann, J., & Buchamann, J. (2004). *Introduction to cryptography* (C. 335). Springer.

Dalal, M., & Juneja, M. (2021). Steganography and Steganalysis (in digital forensics): a Cybersecurity guide. *Multimedia Tools and Applications*, *80*(4), 5723-5771.

Das, S., Das, S., Bandyopadhyay, B., & Sanyal, S. (2011). Steganography and Steganalysis: different approaches. *arXiv preprint arXiv:1111.3758*.

Dhawan, S., & Gupta, R. (2021). Analysis of various data security techniques of steganography: A survey. *Information Security Journal: A Global Perspective*, *30*(2), 63-87.

Invernici, F., Bernasconi, A., & Ceri, S. (2024). Exploring the evolution of research topics during the COVID-19 pandemic. *Expert Systems with Applications*, *252*, 124028.

Kahn, D. (1996). The history of steganography. *International workshop on information hiding*, 1-5.

Kessler, G. C., & Hosmer, C. (2011). An overview of steganography. *Advances in Computers*, *83*, 51-107.

Kishor, S. N., Ramaiah, G. N. K., & Jilani, S. A. K. (2016). A review on steganography through multimedia. *2016 International conference on research advances in integrated navigation systems (RAINS)*, 1-6.

Laishram, D., & Tuithung, T. (2018). A survey on digital image steganography: current trends and challenges. *proceedings of 3rd international conference on internet of things and connected technologies (ICIoTCT)*, 26-27.

Majeed, M. A., Sulaiman, R., Shukur, Z., & Hasan, M. K. (2021). A review on text steganography techniques. *Mathematics*, *9*(21), 2829.

Malik, K. R., Sajid, M., Almogren, A., Malik, T. S., Khan, A. H., Altameem, A., Rehman, A. U., & Hussen, S. (2025). A hybrid steganography framework using DCT and GAN for secure data communication in the big data era. *Scientific Reports*, *15*(1), 19630.

Michaylov, K. D., & Sarmah, D. K. (2025). Steganography and steganalysis for digital image enhanced Forensic analysis and recommendations. *Journal of Cyber Security Technology*, *9*(1), 1-27.

Mishra, R., & Bhanodiya, P. (2015). A review on steganography and cryptography. *2015 International Conference on Advances in Computer Engineering and Applications*, 119-122.

Setiadi, D. R. I. M. (2021). PSNR vs SSIM: imperceptibility quality assessment for image steganography. *Multimedia tools and applications*, *80*(6), 8423-8444.

Singh, A. (2025). From Algorithms to AI: A Comprehensive Review of Core Concepts in Computer Science. *Global Research Repo*, *1*(2), 129-153.

Stamp, M. (2011). *Information security: principles and practice*. John Wiley & Sons.

Tran, D. N., Zepernick, H.-J., & Chu, T. M. C. (2022). LSB data hiding in digital media: A survey. *EAI Endorsed Transactions on Industrial Networks and Intelligent Systems*, 1-50.

Wang, H., & Wang, S. (2004). Cyber warfare: steganography vs. steganalysis. *Communications of the ACM*, *47*(10), 76-82.

Whitman, M. E., & Mattord, H. J. (2009). *Principles of information security*. Thomson Course Technology Boston, MA.

YÖK. (2025). *YÖK Ulusal Tez Merkezi*. https://tez.yok.gov.tr/UlusalTezMerkezi/