



T.C.
BURSA TEKNİK ÜNİVERSİTESİ
LİSANSÜSTÜ EĞİTİM ENSTİTÜSÜ

**Gradyan Analizi ve Kenar Genişletme ile Güçlendirilmiş
Uyarlama Çok Bitli LSB Steganografi Yöntemi**

DÖNEM PROJESİ

Danışman: Dr. Öğr. Üyesi Mustafa Özden

Öğrenci: Refga Mobarak Awadelkarim Mohamed

24434981221

Özet

Bu çalışma, dijital görüntü steganografisinde gömme kapasitesi, algısal fark edilemezlik ve istatistiksel güvenlik arasındaki dengeyi optimize etmek amacıyla uyarlamalı ayırt tabanlı çok bitli bir LSB yöntemi sunmaktadır. Geleneksel LSB yaklaşımının aksine önerilen yöntem, kapak görüntüsünün yerel karmaşıklığını analiz ederek veriyi yalnızca görsel bozulmaya karşı yüksek tolerans gösteren bölgelere gömmektedir. Canny ayırt dedektörü ve morfolojik genişletme ile belirlenen hassas bölge maskesi üzerinde, Sobel gradyan büyülüğüne dayalı olarak pikseller zayıf ve güçlü ayırtlar şeklinde sınıflandırılmaktadır. Zayıf ayırtlarda tek bit, güçlü ayırtlarda ise iki bitlik uyarlamalı bir strateji izlenirken; tüm gömme süreci deterministik çıkarım saldırısını önlemek amacıyla gizli bir anahtar üzerinden yürütülen sözde rastgele bir sıralama mekanizmasıyla (PRNG) güvence altına alınmaktadır. Deneysel sonuçlar, yöntemin yüksek veri yükleri altında dahi 59 dB'yi aşan PSNR değerleri ve 0,999 seviyesinde SSIM skorları üreterek üstün bir algısal kalite sunduğunu kanıtlamıştır. Histogram tabanlı L_1 , L_2 , ki-kare ve KL diverjansı analizleri, kapak ve stego görüntüleri arasındaki istatistiksel sapmanın minimum düzeyde olduğunu doğrulamıştır. Elde edilen bulgular, önerilen yöntemin hem görsel fark edilemezliği koruduğunu hem de modern güvenlik ihtiyaçları için yüksek kapasiteli ve dirençli bir çözüm sunduğunu göstermektedir.

Anahtar Kelimeler: Steganografi, LSB, Uyarlamalı Gömme, ayırt Tespiti, İstatistiksel Güvenlik.

1 Giriş

Dijital medya alışverişindeki artış, güvenli ve gizli iletişim tekniklerine olan talebi artırılmıştır. Görüntü steganografisi, bu ihtiyacı, görsel farkedilemezliği korurken gizli verileri görüntüler içine gömerek ele alır.

En Az Anlamlı Bit (LSB) tabanlı steganografi, basitliği ve yüksek kapasitesi nedeniyle yaygın olarak kullanılır; ancak, tek tip gömme genellikle istatistiksel tespit edilebilirliğe ve yüksek yüklerde görüntü kalitesinin bozulmasına yol açar (Chen vd., 2010; Luo vd., 2010). Bu sınırlamaların üstesinden gelmek için, ayırt tabanlı yöntemler piksel değişikliklerine daha toleranslı olan algısal olarak karmaşık bölgelerden yararlanarak, farkedilemezliği ve kapasiteyi iyileştirir (Wu & Tsai, 2003).

Son adaptif yaklaşımlar, yerel görüntü özelliklerine dayalı olarak gömme derinliğini ayarlayarak daha iyi kapasite-kalite dengeleri elde eder. Bununla birlikte, mevcut birçok yöntem sabit gömme kurallarına dayanmakta veya yeterli güvenlik mekanizmalarından yoksun olmakta, bu da onları deterministik çalışma karşı savunmasız bırakmaktadır (Tseng & Leng, 2014; Tripathy vd., 2025).

Bu çalışma, farkedilemezliği ve güvenliği artırmak için yerel karmaşıklık analizini anahtar tabanlı rastgelelik ile bütünlüğe adaptif bir ayırt tabanlı çok bitli LSB steganografi yöntemi önermektedir. Önerilen yaklaşım, algısal ve istatistiksel metrikler kullanılarak hem sabit hem de adaptif yük koşulları altında değerlendirilmiştir.

2 İlgili Çalışmalar

Uyarlamalı görüntü steganografisi, gömme kapasitesi, farkedilemezlik ve güvenlik arasında denge kurmak için evrimleşmiştir. Erken çalışmalar, İnsan Görsel Sisteminin yüksek frekanslı bölgelerdeki değişikliklere daha az duyarlı olduğunu göstermiş, bu da ayırt tabanlı uyarlamalı gömme yöntemlerini motive etmiştir.

Piksel Değeri Farklılığı (PVD) gibi ilk içerik-uyarlamalı yöntemler, yük kapasitesini artırmak için yerel yoğunluk varyasyonlarından yararlanmıştır. Daha sonra, anahtar tabanlı işlemler yoluyla güvenliği artırmak için "LSB Eşleştirme Yeniden Değerlendirildi" kullanan ayırt-uyarlamalı şemalar önerilmiştir (Luo vd., 2010). Diğer yaklaşımlar, hibrit ayırt dedektörleri kullanmış ancak ayırt bilgisini depolamak için gösterge piksellerine dayanmış, bu da kullanabilir kapasiteyi azaltmış ve öngörelebilir bozulmalara yol açmıştır (Chen vd., 2010; Tseng & Leng, 2014).

Bu sınırlamaların üstesinden gelmek için, kör çıkarım teknikleri tanıtılmıştır. Bai vd. (2017), ayırt haritalarının yardımcı veri olmadan En Önemli Bitlerden (MSBs) yeniden oluşturulabileceğini göstermiştir. Yakın tarihli çalışmalar, derin öğrenme (Ray vd., 2021), DoG gibi gelişmiş filtreler (Patwari vd., 2023) ve blok tabanlı karmaşıklık analizi (Tripathy vd., 2025) kullanarak ayırt modellemesini daha da geliştirmiştir. Bu gelişmelere rağmen, ayırt dedektörlerinin gürültüye duyarlılığı, sabit bit tahsis stratejileri ve rastgelelik mekanizmalarının yokluğunda istatistiksel steganalize karşı savunmasızlık gibi zorluklar devam etmektedir.

3 Yöntem

3.1 Sistem Genel mimarisi

Bu bölüm, önerilen uyarlamalı ayırt tabanlı LSB steganografi sistemini açıklar. Genel işlem hattı iki ana aşamadan oluşur: veri gömme (Encoder) ve veri çıkarma (Decoder). Önerilen yöntemin blok diyagramı Şekil 1 ve Şekil 2 'de gösterilmektedir.

3.2 Kapak Görüntüsü Ön İşleme ve Bölge Seçimi

Bir RGB kapak görüntüsü (cover) göz önüne alındığında, öncelikle ayırt tespitini kolaylaştırmak için gri tonlamaya dönüştürülür. Sağlamlığı ve kesin yer belirlemesi nedeniyle ayırtlar, Canny ayırt dedektörü kullanılarak tespit edilir (Chen vd., 2010). Gömme kapasitesini artırmak için, tespit edilen ayırtlar, se_size boyutunda kare bir yapısal eleman kullanılarak morfolojik genişletme (dilation) ile genişletilir. Bu genişletme, bir ayırtın komşu piksellerinin - ki bunlar da yüksek doku karmaşıklığına sahiptir - gömme için kullanılmasını sağlar (Bai vd., 2017).

3.3 Uyarlamalı Gömme Kapasitesi Tahmini

Tüm ayırt pikselleri değişikliğe aynı toleransı göstermez. Bu nedenle, gri tonlamalı kapak görüntüsünün gradyan büyülüğü Sobel operatörü kullanılarak hesaplanır (Luo vd., 2010). Önceden tanımlanmış bir eşigi (T) aşan gradyan büyülüğüne sahip ayırt pikselleri güçlü ayırtlar olarak sınıflandırılırken, maskelenmiş piksellerin kalanı zayıf ayırtlar olarak ele alınır. Bu, sistemin yüksek ve orta karmaşıklıktaki alanları ayırt etmesine olanak tanır.

3.4 Uyarlamalı Çok Bitli LSB Gömme Stratejisi

Her pikseldeki bit derinliğini kontrol etmek için uyarlamalı bir gömme haritası (bits_map) oluşturulur. Bölüm 3.3'teki sınıflandırmaya dayanarak (Patwari vd., 2023):

- Zayıf ayırtlar: 1 bit, 1. LSB'ye gömülüür.
- Güçlü ayırtlar: 2 bit, 1. ve 2. LSB'lere gömülüür.
- Düzgün bölgeler: 0 bit gömülüür (korunur).

Gömme işlemi, İnsan Görsel Sisteme (HVS) karşı en az duyarlı olduğu için yalnızca Mavi kanalda gerçekleştirilir (Wu & Tsai, 2003).

3.5 Gizli Veri Hazırlığı ve Kapasite Kontrolü

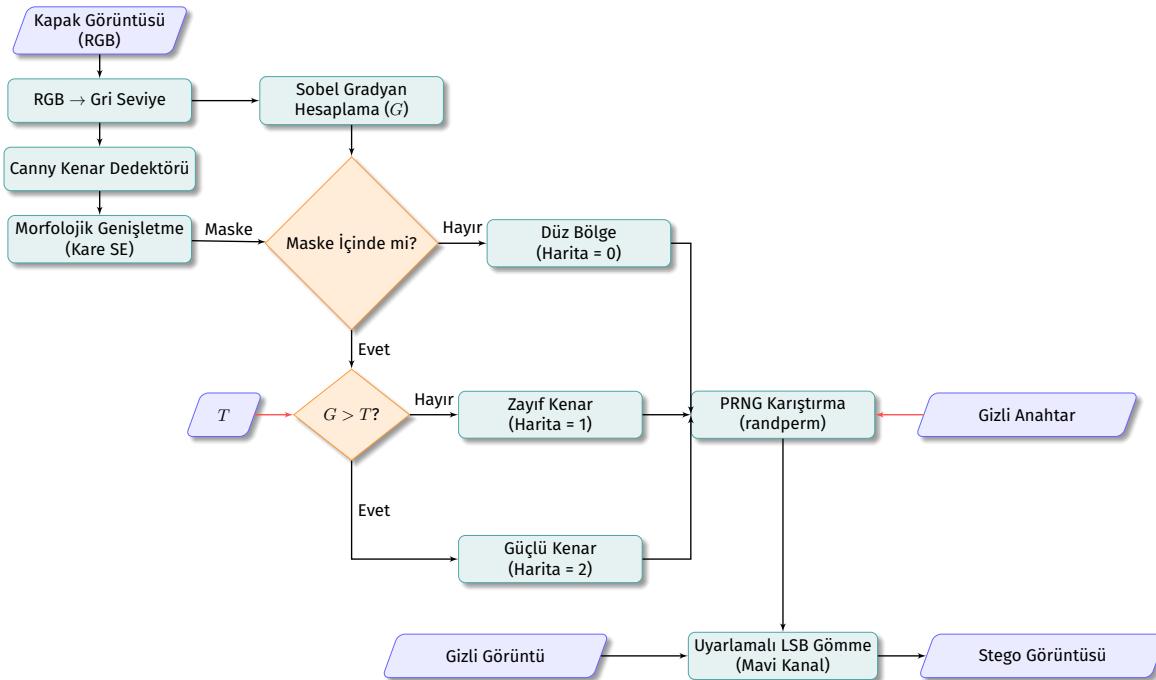
Gizli görüntü, her pikselin 8 bit ile temsil edildiği ikili bir bit akışına (bitstream) dönüştürülür. Gömmeden önce, sistem bits_map'i toplayarak toplam kullanılabılır kapasiteyi hesaplar (Ray vd., 2021). Gizli bit akışının boyutu bu kapasiteyi aşarsa, veri bütünlüğünü sağlamak ve kesmeyi önlemek için işlem sonlandırılır.

3.6 Anahtar Tabanlı Rastgele Gömme

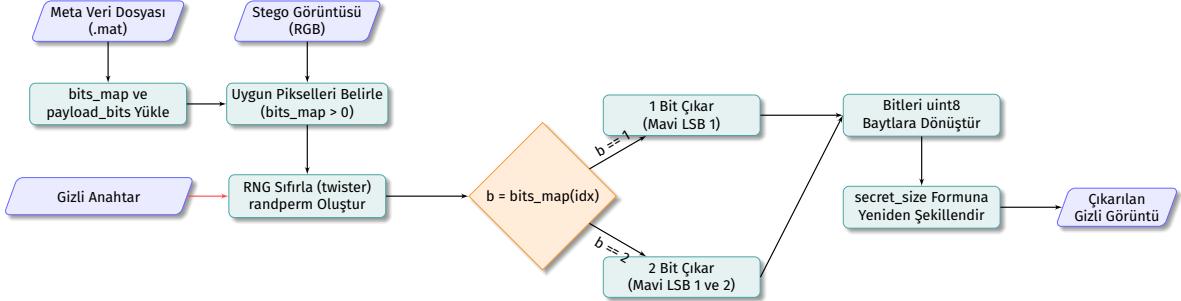
Güvenliği artırmak ve deterministik çıkarımı önlemek için, anahtar tabanlı bir rastgeleş tirme mekanizması kullanılır. Sıralı gömme yerine, piksel indeksleri, gizli bir anahtardan (key) oluşturulan bir sözde rastgele permütasyon kullanılarak karıştırılır (Luo vd., 2010). Bu, bir saldırgan ayırt maskesini tanımlasa bile, gizli bitlerin belirli anahtar olmadan doğru sırayla çıkarılamayacağını veya yeniden birleştirilemeyeceğini garanti eder.

3.7 Kod Çözme Süreci

Kod çözme süreci, gömme aşamasını yansıtır. Sağlanan meta verileri ve doğru gizli anahtarları kullanarak, alıcı tam olarak aynı sözde rastgele gömme sırasını yeniden oluşturur. Gerekli meta veriler arasında gömme haritası, yük uzunluğu ve gizli görüntü boyutları bulunur. Gömülü bitler daha sonra stego görüntünün mavi kanalının 1. ve 2. LSB'lerinden çıkarılır ve gösterge piksellerine gerek kalmadan orijinal gizli görüntüyü kurtarmak için yeniden şekillendirilir (Bai vd., 2017).



Şekil 1: Önerilen uyarlamalı ayırt tabanlı çok bitli LSB steganografi yönteminin gömme (encoder) aşamasının blok diyagramı



Şekil 2: Önerilen yöntemin gizli verinin çıkarımını gösteren kod çözme (decoder) aşamasının blok diyagramı.

4 Deneyler ve Sonuçlar

Bu bölümde, önerilen uyarlamalı ayırt tabanlı çok bitli LSB steganografi yönteminin performansı deneysel olarak değerlendirilmiştir. Deneyler, sabit yük ve kapasite-uyarlamalı yük olmak üzere iki farklı senaryo altında gerçekleştirilmiş ve sonuçlar nicek metrikler ve görsel analizler kullanılarak raporlanmıştır.

4.1 Deneysel Kurulum

Tüm deneyler MATLAB ortamında gerçekleştirilmiştir. Tekrarlanabilirliği sağlamak amacıyla tüm deneylerde aynı parametre ayarları kullanılmıştır. Yapısal eleman boyutu $se_size = 3$, ayırt gücü eşik değeri $T = 0.35$ olarak belirlenmiş ve tüm deneyler boyunca sabit bir gizli anahtar kullanılmıştır.

Deneylerde, farklı uzamsal çözünürlük ve içerik özelliklerine sahip üç adet RGB kapak görüntüsü kullanılmıştır. Tüm senaryolarda tek bir gri tonlamalı gizli görüntü (QR kodu) gömülüdür. Performans değerlendirmesi, gömme kapasitesi, algısal kalite ve istatistiksel güvenlik metrikleri üzerinden yapılmıştır.

4.2 Gömme Kapasitesi

Her bir kapak görüntüsü için gömme kapasitesi, ayırt tabanlı maske ve Sobel gradyanına dayalı uyarlamalı bit tahsis haritası kullanılarak hesaplanmıştır. Elde edilen kapasite değerleri Tablo 1 içerisinde sunulmaktadır.

Tablo 1: Kapak görüntülerine ait tahmini gömme kapasiteleri

Kapak Görüntü	Kapasite (bit)
cover_btu	917 630
cover_desert	5 045 854
cover_ebru	536 577

4.3 Deney A: Sabit Yük Değerlendirmesi

Bu deneyde, tüm kapak görüntülerine minimum kapasitenin %80'ine karşılık gelen 429 261 bitlik sabit bir yük gömülüdür. Bu senaryo, farklı görüntü içerikleri altında yöntemin

algısal kalite ve istatistiksel özellikler bakımından tutarlığını değerlendirmeyi amaçlamaktadır.

Elde edilen kalite ve istatistiksel güvenlik metrikleri Tablo 2'de sunulmaktadır.

Tablo 2: Deney A: Sabit yük (429 261 bit) altında kalite ve istatistiksel metrikler

Görüntü	PSNR (dB)	SSIM	L1	L2	χ^2	KL
cover_btu	69.45	0.99997	0.00988	0.00097	0.00033	0.00015
cover_desert	69.12	1.00000	0.00874	0.00068	0.00013	0.00007
cover_ebru	59.28	0.99987	0.09196	0.00955	6311.2	0.00518

4.4 Deney B: Kapasite-Uyarlamalı Yük Değerlendirmesi

Bu deneyde, her bir kapak görüntüsüne kendi maksimum mevcut kapasitesinin %80'ine karşılık gelen uyarlamalı bir yük gömülümüştür. Bu senaryo, yöntemin yüksek gömme oranları altındaki davranışını değerlendirmeyi amaçlamaktadır.

Elde edilen sonuçlar Tablo 3'de sunulmaktadır.

Tablo 3: Deney B: Kapasite-uyarlamalı yük altında kalite metrikleri

Görüntü	Kapasite (bit)	Yük (bit)	PSNR (dB)	SSIM
cover_btu	917 630	734 104	67.21	0.99995
cover_desert	5 045 854	4 036 683	59.37	0.99997
cover_ebru	536 577	429 261	59.28	0.99987



Şekil 3: Örnek bir kapak görüntüsü için kapak görüntüsü (sol), stego görüntüsü (orta) ve ayrıt tabanlı gömme maskesi (sağ)

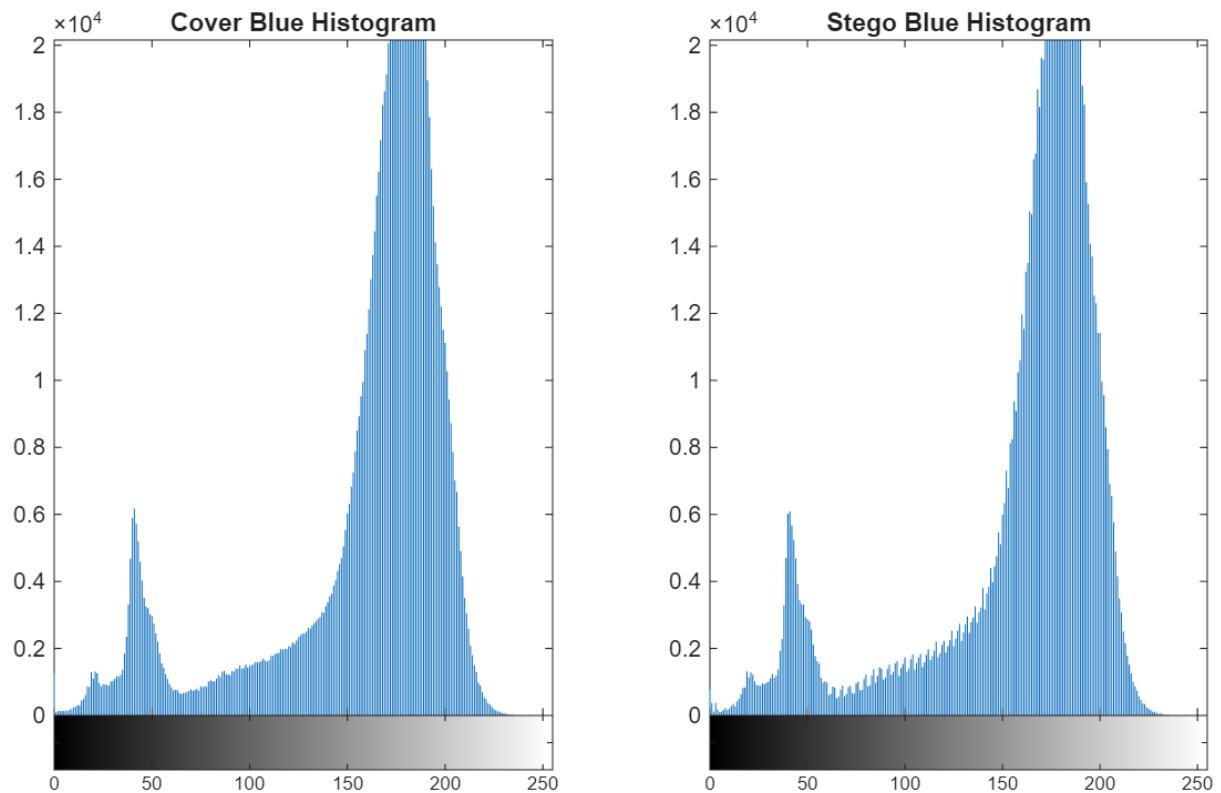
4.5 Histogram ve Frekans Alanı Güvenlik Analizi

Histogram tabanlı güvenlik metrikleri, örnek bir stego görüntüsü için hesaplanmış ve Tablo 4'de sunulmuştur.

Tablo 4: Örnek bir stego görüntüsü için histogram tabanlı güvenlik metrikleri

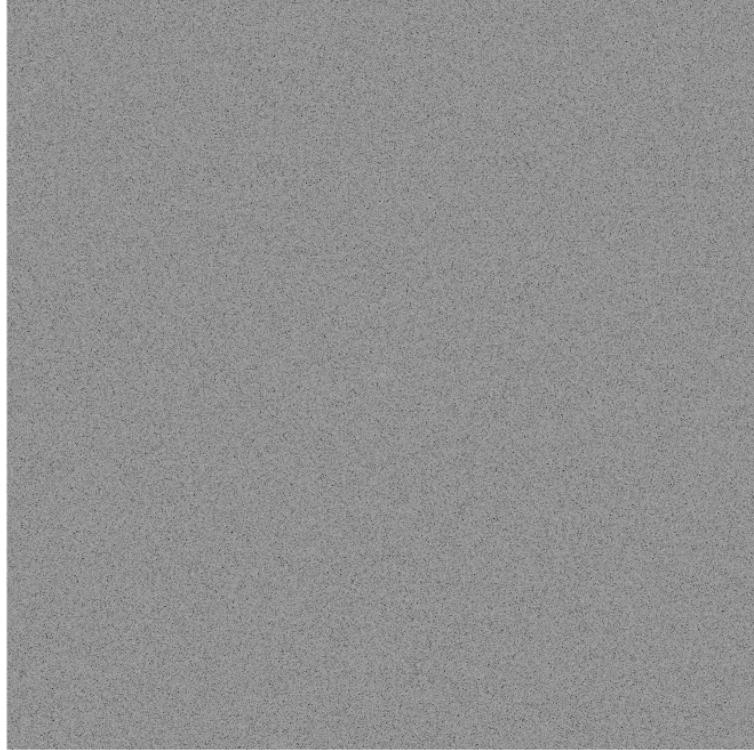
Metik	Değer
L1 mesafesi	0.04890
L2 mesafesi	0.00524
Ki-kare mesafesi	487.95
KL diverjansı	0.00268

Frekans alanında yapılan analizler, stego ve kapak görüntülerini farkının yapısal artefaktlar içermeyen gürültü-benzeri bir spektrum sergilediğini şekil 5’de göstermektedir. Şekil 4’te sunulan histogram karşılaştırması, kapak ve stego görüntülerinin mavi kanal dağılımlarının büyük ölçüde örtüşüğünü göstermektedir. Histogram eğrileri arasında belirgin bir kayma veya düzensiz yoğunluk artışı gözlemlenmemiştir. Dolayısıyla, yöntem histogram tabanlı istatistiksel steganaliz tekniklerine karşı güçlü bir direnç sergilemektedir.



Şekil 4: Kapak ve stego görüntülerinin mavi kanal histogramlarının karşılaştırılması.

Log Spectrum of (Stego - Cover) in Blue Channel



Şekil 5: Stego ve kapak görüntüleri farkının frekans alanı gösterimi.

5 Tartışma

Deneysel sonuçlar, önerilen uyarlamalı ayırt tabanlı çok bitli LSB steganografi yönteminin yüksek gömme kapasitesine rağmen algısal kaliteyi etkili bir şekilde koruduğunu göstermektedir. Sabit yük koşulları altında elde edilen sonuçlar, yöntemin farklı görüntü içeriklerine karşı tutarlı bir performans sergilediğini ortaya koymaktadır.

Kapasite-uyarlamalı deney sonuçları, yöntemin her bir kapak görüntüsünün mevcut kapasitesine göre yükü verimli bir şekilde ölçeklendirebildiğini göstermektedir. Yük miktarının artmasına rağmen SSIM değerlerinin bire yakın kalması, yapısal benzerliğin büyük ölçüde korunduğunu göstermektedir.

Histogram tabanlı metrikler, kapak ve stego görüntüleri arasında güclü bir istatistiksel benzerlik olduğunu doğrulamaktadır. Ki-kare metriğinin daha küçük görüntüler için daha hassas davranışını beklenen bir durumdur; buna karşın L1, L2 ve KL metriklerinin düşük seviyelerde kalması, genel istatistiksel görünmezliği desteklemektedir.

Anahtar tabanlı rastgeleleştirme mekanizması, deterministik gömme yollarını ortadan kaldırarak güvenliği artırmaktadır. Frekans alanında gözlemlenen gürültü-benzeri spektrumlar, belirgin gömme desenlerinin oluşmadığını ve önerilen yöntemin yetkisiz çıkarımı karşı daha dirençli olduğunu göstermektedir.

Klasik tek-bitli LSB steganografi yöntemleriyle karşılaşıldığında, önerilen yaklaşım yalnızca algısal olarak toleranslı ayırt bölgelerinde gömme yaparak hem görsel bozulmayı azaltmakta hem de istatistiksel tespit edilebilirliği düşürmektedir. Ayrıca, anahtar tabanlı rastgele gömme sırası sayesinde, deterministik ve sıralı LSB yöntemlerine kıyasla yetkisiz çıkarımı karşı daha yüksek bir güvenlik seviyesi sunmaktadır.

6 Sonuç

Bu çalışma, gömme kapasitesi, farkedilemezlik ve güvenlik arasında denge kurmak üzere tasarlanmış uyarlamalı bir ayırt tabanlı çok bitli LSB steganografi yöntemi sunmuştur. Veri gömme işlemini ayırt bölgeleriyle sınırlandırarak ve yerel görüntü karmaşıklığına dayalı olarak gömülüen bit sayısını uyarlamalı bir şekilde tahsis ederek, önerilen yaklaşım algısal olarak toleranslı alanları etkili bir şekilde kullanırken görünür bozulmayı en aza indirmektedir.

Deneysel sonuçlar, yöntemin tüm test edilen senaryolarda PSNR değerlerinin 59 dB'yi aşması ve SSIM değerlerinin bire yakın olmasıyla çok yüksek görsel kalite sağladığını göstermiştir. Sabit yük deneyi, eşit yük koşulları altında tutarlı farkedilemezliği doğrularken, kapasite-uyarlamalı deney ise yöntemin her bir kapak görüntüsünün mevcut kapasitesiyle orantılı olarak yükü ölçeklendirme yeteneğini vurgulamıştır.

L1 mesafesi, L2 mesafesi, Ki-kare mesafesi ve KL diverjansı dahil olmak üzere çoklu histogram tabanlı benzerlik metrikleri kullanılarak yapılan güvenlik değerlendirmesi, kapak ve stego görüntüleri arasında minimum istatistiksel sapma olduğunu göstermiştir. Ki-kare metriği daha küçük görüntüler için daha yüksek hassasiyet sergilemiş olsa da, tamamlayıcı metrikler genel olarak güçlü istatistiksel görünmezliği doğrulamıştır. Ek olarak, anahtar tabanlı rastgeleleştirme, deterministik gömme modellerini ortadan kaldırarak yetkisiz çıkarmaya karşı direnci artırmıştır.

Genel olarak, sonuçlar, önerilen yöntemin farklı görüntü özelliklerine zarif bir şekilde uyum sağlayan performansıyla, yüksek kapasiteli ve güvenli görüntü steganografisi için etkili ve pratik bir çözüm sunduğunu doğrulamaktadır.

7 Sınırlamalar ve Gelecek Çalışmalar

Etkililiğine rağmen, önerilen yöntemin gelecekte iyileştirme fırsatları sunan çeşitli sınırlamaları bulunmaktadır.

İlk olarak, mevcut uygulama tamamen uzamsal alanda çalışmakta ve JPEG sıkıştırma, yeniden boyutlandırma veya gürültü ekleme gibi yaygın görüntü işleme operasyonlarına karşı sağlamlığı açıkça dikkate almamaktadır. Gelecekteki çalışmalar, bu tür saldırılardan altında sağlamlığı artırmak için yöntemi hibrit uzamsal-frekans alanı gömme yöntemine genişletebilir.

İkinci olarak, gömme stratejisi, ampirik olarak seçilen sabit eşikler ve parametrelere (örneğin, ayırt gücü eşiği ve yapısal eleman boyutu) dayanmaktadır. Uyarlamalı veya öğrenme tabanlı parametre seçimi, daha geniş bir görüntü yelpazesinde performansı daha da optimize edebilir.

Üçüncü olarak, anahtar tabanlı rastgeleleştirme güvenliği artırırsa da, sistem yükün kendisinin kriptografik şifrelemesini içermemektedir. Gömmeden önce hafif şifrelemenin entegre edilmesi ek bir koruma katmanı sağlayabilir.

Son olarak, makine öğrenimi tabanlı dedektörler de dahil olmak üzere daha gelişmiş steganaliz teknikleri bu çalışmada değerlendirilmemiştir. Gelecekteki çalışmalar, modern derin öğrenme steganaliz modellerine karşı direnci değerlendirebilir ve adversaryal (düşmanca) gömme stratejilerini araştırabilir.

Bu çalışmada, ayırt-tabanlı adaptif çok-bitli ve anahtar-rastgeleştirmeli bir görüntü steganografi yöntemi önerilmiştir. Yöntem, yüksek kapasite, yüksek algısal kalite ve geliştirilmiş güvenlik özelliklerini birlikte sunmaktadır.

Gelecek çalışmalarında, yöntemin farklı renk uzaylarında uygulanması, derin öğrenme tabanlı steganaliz yöntemlerine karşı dayanıklılığının incelenmesi ve gerçek zamanlı uygulamalar için optimizasyonu planlanmaktadır.

Kaynakça

- Al-Rawashdeh, R., Rahman, M. M., & Niazi, M. (2025). Robust image steganography approach based on edge detection combined with CNN algorithm. *IEEE Access*, 13, 109099–109115. <https://doi.org/10.1109/access.2025.3582159>
- Bai, J., Chang, C.-C., Nguyen, T.-S., Zhu, C., & Liu, Y. (2017). A high payload steganographic algorithm based on edge detection. *Displays*, 46, 42–51. <https://doi.org/10.1016/j.displa.2016.12.004>
- Chen, W.-J., Chang, C.-C., & Le, T. (2010). High payload steganography mechanism using hybrid edge detector. *Expert Systems with Applications*, 37(4), 3292–3301. <https://doi.org/10.1016/j.eswa.2009.09.050>
- Luo, W., Huang, F., & Huang, J. (2010). Edge adaptive image steganography based on LSB matching revisited. *IEEE Transactions on Information Forensics and Security*, 5(2), 201–214. <https://doi.org/10.1109/TIFS.2010.2041812>
- Patwari, B., Nandi, U., & Ghosal, S. K. (2023). Image steganography based on difference of Gaussians edge detection. *Multimedia Tools and Applications*, 82(28), 43759–43779. <https://doi.org/10.1007/s11042-023-15360-7>
- Ray, B., Mukhopadhyay, S., Hossain, S., Ghosal, S. K., & Sarkar, R. (2021). Image steganography using deep learning based edge detection. *Multimedia Tools and Applications*, 80(21), 33475–33503. <https://doi.org/10.1007/s11042-021-11177-4>
- Tripathy, B. K., Rampal, S., Shah, M. D., Maddikayala, V. N., Gopinath, S., & Nanda, S. (2025). Edge-adaptive steganography scheme with minimal distortion using local complexity and adaptive second-order statistics. In *2025 World Skills Conference on Universal Data Analytics and Sciences (WorldSUAS)* (pp. 1–6). <https://doi.org/10.1109/worldsuas66815.2025.11199261>
- Tseng, H., & Leng, H. (2014). High-payload block-based data hiding scheme using hybrid edge detector with minimal distortion. *IET Image Processing*, 8(11), 647–654. <https://doi.org/10.1049/iet-ipr.2013.0584>
- Wu, D.-C., & Tsai, W.-H. (2003). A steganographic method for images by pixel-value differencing. *Pattern Recognition Letters*, 24(9–10), 1613–1626. [https://doi.org/10.1016/S0167-8655\(02\)00402-6](https://doi.org/10.1016/S0167-8655(02)00402-6)