Mühendislik Bilimleri ve Tasarım Dergisi
10(3), 816 – 830, 2022
e-ISSN: 1308-6693

Journal of Engineering Sciences and Design
DOI: 10.21923/jesd.960733

Araştırma Makalesi Research Article

GÖRÜNTÜ STEGANOGRAFİSİNDE YAYGIN KULLANILAN VERİ GİZLEME TEKNİKLERİNİN İNCELENMESİ

Murat UZUN[1], Serdar SOLAK[2]*

[1] Kocaeli Üniversitesi, Öğrenci İşleri Daire Başkanlığı, Rektörlük, Kocaeli, Türkiye
[2] Kocaeli Üniversitesi, Teknoloji Fakültesi, Bilişim Sistemleri Mühendisliği Bölümü, Kocaeli, Türkiye

Anahtar Kelimeler
Bilgi Güvenliği,
Görüntü Steganografisi,
GEMD,
PVD,
Veri Gizleme.

Öz

Sayısal veri iletiminde, veri güvenliğinin sağlanması için kullanılan yöntemlerden biri Steganografidir. Steganografinin amacı, verileri güvenli olmayan iletim kanalı üzerinden güvenli bir şekilde alıcıya iletmektir. Sayısal steganografinin bir alt dalı olan görüntü Steganografisi, özellikle veri gizleme kapasitesinin yüksekliği sebebiyle daha yaygın kullanılmaktadır. Makalede, uzaysal etki alanında yaygın kullanılan görüntü steganografisi tekniklerinden En Düşük Anlamlı Bit, Piksel Değeri Farkı, Değişim Yönünü Kullanma ve Genelleştirilmiş Değişim Yönünü Kullanma algoritmaları incelenmiştir. Bu yöntemler, bilgi taşıma kapasitesi, Tepe Sinyal Gürültü Oranı, Yapısal Benzerlik Endeksi gibi görüntü kalitesini ölçmek için kullanılan parametrelerin yanı sıra, histogram ve RS analizi ataklarına karşı dayanıklılık testleri incelenmiştir. Makale kapsamında gerçekleştirilen deneysel çalışmalara göre, kullanılan bu yöntemlerin birbirlerine göre üstün ve zayıf yönleri ortaya konularak, kullanım amacına göre uygun yöntem seçimiyle ilgili tavsiyelerde bulunulmaktadır. Özellikle yüksek kapasite gerektiren ve algılanamazlığın önemsenmediği durumlarda LSB-3 bit yöntemi, güvenliğin ve algılanamazlığın ön plana çıktığı daha düşük kapasitede veri gizleme işlemlerinde PVD, EMD ve GEMD yöntemlerinin kullanılması uygundur.

ANALYSIS OF COMMONLY USED IMAGE STEGANOGRAPHY DATA HIDING TECHNIQUES IN SPATIAL DOMAIN

Keywords
Information Security,
Image Steganography,
GEMD,
PVD,
Data Hiding.

Abstract

Steganography is one of the methods used to ensure data security in digital data transmission. The aim of the steganography technique is to transmit data securely over the unsecured transmission channel. The extensive use of social media and its ease of application make image steganography, a branch of digital steganography, popular. In this article, the examination of Least Significance Bit, Pixel Value Difference, Using the Change Direction and Using Generalized Change Direction techniques commonly used in image steganography and application methods with examples are explained. The results were interpreted by calculating the Load Capacity, Peak Signal-to-Noise Ratio, and Structural Similarity Indexes of these methods. The aim of our study is to determine the superior and weak aspects of these methods compared to each other according to the data obtained, and to make recommendations regarding the selection of the method suitable for the purpose. In particular, LSB-3 bit method is a high-capacity but insecure method, while PVD, EMD and GEMD data hiding techniques are low-capacity but security and undetectable methods by third parties.

Alıntı / Cite

Uzun, M., Solak, S., (2022). Görüntü Steganografisinde Yaygın Kullanılan Veri Gizleme Tekniklerinin İncelenmesi, Mühendislik Bilimleri ve Tasarım Dergisi, 10(3), 816-830.

* İlgili yazar / Corresponding author: serdars@kocaeli.edu.tr, +90-262-303-2269

Yazar Kimliği / Author ID (ORCID Number)	Makale Süreci / Article Process	
M. Uzun, 0000-0002-5255-8247	**Başvuru Tarihi / Submission Date**	01.07.2021
S. Solak, 0000-0003-1081-1598	**Revizyon Tarihi / Revision Date**	25.03.2022
	Kabul Tarihi / Accepted Date	20.04.2022
	Yayım Tarihi / Published Date	30.09.2022

1. Giriş (Introduction)

İnternet aracılığıyla günlük olarak gönderilen epostalar, sosyal medyada yapılan paylaşımlar ve yorumlar, atılan mesajlar, görüntülenen fotoğraf ve videoların sayısını tahmin etmek neredeyse imkansızdır. Günaşırı ortaya çıkan yeni uygulamalarla da bu sayı üstel olarak artmaktadır. Böylesine devasa bir veri trafiğinde, veri güvenliğinin sağlanması büyük önem taşımaktadır. Veri güvenliği özetle, verilerin yetkisiz erişime karşı korunması olarak tanımlanabilir. Veri güvenliğinde en önemli nokta, kişisel veya kurumsal verileri korurken verilerin gizliliğini sağlamak ve bütünlüğünü doğrulamaktır.

Veri güvenliğinin sağlanması, verinin şifrelenmesi veya verinin gizlenmesi yoluyla yapılabilir. Verinin şifrelenmesi, Kriptografi (Thambiraja vd., 2012) olarak adlandırılır. Güvenli bir yöntem olmakla birlikte, şifrelenmiş veri dikkatleri üzerine çekebilmektedir. Ancak, açık bir ağ üzerinden dikkat çekmeyecek, adeta görünmez bir şekilde gizli verinin gönderilmesi gerekebilir. Burada, veri gizleme işlemi gerçekleştirilmektedir. Veri gizleme, Steganografi (Kadhim vd., 2019) ve Filigran (Petitokolas vd., 1999, Wan vd., 2022) olmak üzere ikiye ayrılır. İkisi de mesajı gizlemek için kullanılır ancak amaçları farklıdır. Genel olarak steganografi, verinin gizli ve tespit edilemez şekilde iletilmesini hedeflerken filigranlama, içeriklerin fikri mülkiyetini korumayı hedeflemektedir (Wan vd., 2022).

Steganografi, görüntü, metin, ses, video vb. dijital ortamlara veri gizleme tekniklerini içeren bilimdir (Hussain vd., 2018). Gizlenmek istenen veri, masum görünüşlü bir ortamda saklanır. Steganografi teknikleri, yapısal olarak Tersine Çevrilemez (Irreversible) ve Tersine Çevrilebilir (Reversible) teknikler olmak üzere ikiye ayrılır (Lu ve Vo., 2020; Puteaux vd., 2021). Tersine çevrilemez tekniklerde, orijinal görüntüye gizli veri gömüldükten sonra oluşan stego görüntüden gizli veri çıkartıldığında, orijinal görüntü elde edilemez. Tersine çevrilebilir tekniklerde ise veri çıkarma işleminden sonra görüntünün orijinali tekrar elde edilir. Orijinal görüntünün gizli mesaj kadar önemli olduğu tıbbi alanlar, iletim sırasında orijinal görüntüdeki herhangi bir belirsizliğin iletilen istihbaratı ve genel sonuçları etkileyebileceği askeri vb. alanlarda tersine çevrilebilir teknikler tercih edilmektedir. Steganografik teknikler, uygulandığı etki alanına göre Uzaysal (Spatial) ve Frekans (Frequency) domain olmak üzere ikiye ayrılır. Makale kapsamında uzaysal domainde yaygın olarak kullanılan veri gizleme teknikleri, güçlü ve zayıf yanları, birbirleriyle kıyaslamaları sunulmaktadır.

En düşük anlamlı bit (Least Significant Bit - LSB) (Chan ve Cheng, 2004; Solak ve Altınışık, 2019; Solak ve Altınışık, 2021), en yaygın kullanılan ilk uzaysal domain steganografi tekniğidir. LSB steganografisi, bir örtü görüntüsünde, göze çarpan görsel bozulmalar olmaksızın büyük gizli bilgileri gizleyebilen temel ve geleneksel yöntemlerden biridir (Li vd., 2011). Temel olarak, örtü görüntüsündeki rastgele veya seçilen piksellerin en düşük anlamlı bitlerini gizli mesaj bitleriyle değiştirerek çalışmaktadır. Zamanla, steganografik yöntemlerde, LSB'nin piksel veya bit düzlemlerinin farklı varyasyonları kullanılmıştır. Bunlardan bazıları, veri gömme için kenarlara, dokuya, yoğunluk seviyesine ve örtü görüntülerinin parlaklığına dayalı uyarlanabilir LSB yöntemidir (Yang vd., 2009; Solak ve Altınışık, 2019; Konyar ve Solak, 2021, Sahu vd., 2021). Benzer şekilde, kedi sürüsü stratejisi kullanılarak optimize edilmiş LSB ikamesi (Wang vd., 2012), interpolasyon görüntüsü ile LSB ikamesi (Jung vd., 2015) ve LSB ikamesi kullanan tersine çevrilebilir şifreli tıbbi görüntü (Liu vd., 2016; Konyar ve Öztürk, 2020; Shivani, 2022), histogram saldırılarına karşı görsel kaliteyi ve güvenliği iyileştirmek için (Sarreshtedari vd., 2014) 1 bpp gömme kapasitesiyle ± 1 LSB tabanlı yaklaşımı, (Amirtharajan vd., 2012) çalışmasında, rastgele k-bit gömme yaklaşımının kullanıldığı uyarlanabilir bir LSB yöntemi, (Muhammad vd., 2016) tarafından farklı şifreleme seviyelerine sahip stego anahtar yönlendirmeli uyarlamalı LSB ikamesine dayanan güvenli bir gömme yöntemi, cyclic18 LSB ikamesi kullanan üç seviyeli şifreli bir algoritma (TLEA) (Muhammad vd., 2016), (Nguyen vd., 2015) tarafından geliştirilen uyarlanabilir LSB tabanlı çok sayıda yöntemin literatürde önerildiği görülmektedir. Benzer şekilde, (Xu vd., 2016)'da mod üç stratejisini kullanarak LSB şemasını iyileştirerek yükü artırmak için başka bir çalışma sunulmuştur. Bazı çalışmalarda, steganaliz yöntemlerini atlatmak amacıyla LSB yöntemi diğer tekniklerle birleştirmiştir. Örneğin, (Hussain vd., 2016), uyarlanabilir LSB'yi örtü görüntünün farklı alt ve yüksek doku bölgelerine dayalı olarak en doğru rakam değiştirme (RMDR) tekniğiyle entegre etmiştir. Pikseldeki bitler yerine rakamların kullanılması, yük kapasitesi ve görsel açısından iyileştirme sağlarken RS analizine (Fridrich vd., 2001) yakalanma riskini azaltmaktadır. Ancak önerilen yöntem modern steganaliz saldırılarına, kapasitenin 1 bpp den yüksek olduğu durumlarda dayanıklı değildir (Pevny vd., 2010).

LSB tabanlı yöntemler basit bir bilgi gizleme yöntemi olarak kabul edilse de, ana dezavantaj, gömme kapasitesinin

stego-görüntünün görsel kalitesiyle doğrudan bir ilişkisinin olmasıdır. Örneğin, bir pikselin LSB'sin de maksimum seviyeye uyum sağlayarak yükü artırmaya çalışırsak, stego-görüntünün genel görsel kalitesi düşmektedir. Görsel kalite sorununu çözmek için (Wu ve Tsai, 2003), piksel farkı değerine (Pixel Value Difference-PVD) dayalı bir steganografik yaklaşım önermiştir. İki komşu piksel arasındaki fark değeri, kaç tane gizli bitin gömülmesi gerektiğine karar vermek için kullanılmaktadır. Fark ne kadar büyükse (doku ne kadar yüksekse), piksel çiftine o kadar fazla bit gizlenebilmektedir. Genel olarak, PVD yöntemi, LSB yöntemine kıyasla daha yüksek görsel algılanamazlığa sahiptir ve görüntülere daha fazla gizli veri yerleştirilmektedir. Literatürde, PVD sınırlamalarını çözmek ve steganografik hedefleri geliştirmek için birçok çalışma sunulmuştur. Örneğin, Üç yollu PVD (Chang vd., 2008), LSB ile PVD' nin beraber kullanıldığı yaklaşımlar (Wu vd., 2005; Jung, 2010), Çoklu Piksel Farkı (MPD) (Yang vd., 2010), Modül İşlevi (MF) (Pan vd., 2011; Liao vd., 2012; Liao vd., 2013), blok tabanlı PVD (Yang vd., 2011) ve benzer hibrit yöntemler (Hussain vd., 2015; Hussain vd., 2017; Liao vd., 2018) sunulmaktadır.

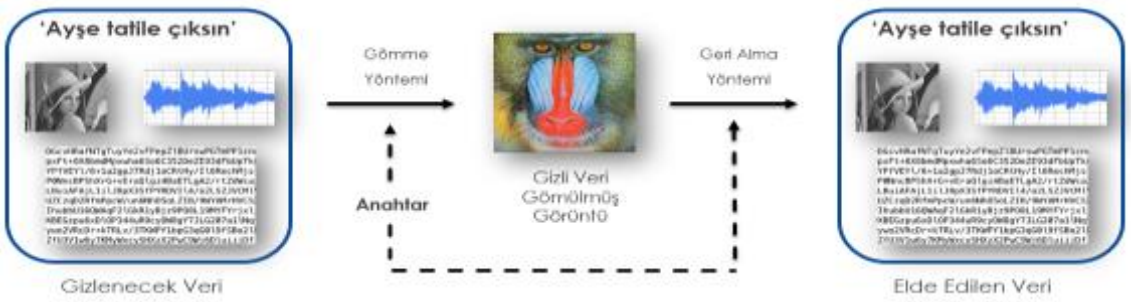
Uzaysal domainde yaygın kullanılan bir başka yöntem ise Değişim Yönünü Kullanma (Exploiting Modification Directions-EMD) tekniğidir. Bu yöntemde, stego görüntülerinin yüksek doğruluğunu koruyan iyi bilinen bir veri gizleme tekniğidir (Zhang ve Wang, 2006). Genel olarak, EMD veri gizleme tekniğinde gizli veriler (2n+1)'lik sayı sistemine dönüştürülür ki burada "n" kullanılan örtü görüntüden alınan piksellerinin sayısıdır. Bu n adet piksel grubunda değişim aralığı en fazla (± 1) 'dir. Öte yandan, EMD yönteminin maksimum kapasitesi, (n = 2) iki piksel değeri için 1,16 bpp'ye kadardır. Gömme yükü, seçilen pikseller arttıkça azalmaktadır. Bu nedenle, gömme kapasitesini iyileştirmek için farklı EMD tabanlı yöntemler önerilmiştir. (Kieu ve Chang, 2011; Liao vd., 2012; Kuo vd., 2013; Kuo ve Kao, 2013; Liao vd., 2017) yapılan çalışmalarda, yükü ve algılanamazlığı iyileştirmek için HoEMD ve AdEMD adlı iki EMD tabanlı veri gizleme teknikleri önermişlerdir. (Kieu ve Chang, 2011), Değişim Yönünü Tamamen Kullanan (FEMD) bir sistem önerdi. FEMD tekniği, (Zhang ve Wang, 2006) tarafından önerilen yöntemi geliştirerek iyi görsel algılanamazlık ile gömme kapasitesini de yükseltmiştir. (Kuo ve Wang, 2013) tarafından sunulan yöntem, EMD yönteminin kapasitesini geliştirmiştir ve literatürde Genelleştirilmiş Değişim Yönünü Kullanma (Generalized Exploiting Modification Directions-GEMD) olarak bilinmektedir. Yöntemde, (n+1) tabandaki bitler, n bitişik piksele doğrudan gizlenmektedir. Yapılan deneyler, gömme yükünün (1+(1/n)) ayarlanabilir piksel grupları ile koruyabildiğini göstermiştir.

Makale kapsamında, LSB, PVD, EMD ve GEMD yöntemlerine ait algoritmalar ve bu yöntemlerin başarım değerlendirmeleri sunulmaktadır. Makalenin, sonraki bölümünde, Steganografi hakkında temel bilgiler verilmiş, uzaysal alanda yaygın kullanılan veri gizleme teknikleri örnekleriyle açıklanmıştır. Bu yöntemlerin değerlendirilmesinde kullanılan ölçütler ve performans testleri Deneysel Çalışmalar bölümünde detaylıca sunulmaktadır. Sonuç ve Tartışma bölümünde ise elde edilen tüm veriler göz önünde bulundurularak teknikler hakkında yorumlar yapılmıştır.

2. Materyal ve Yöntem (Material and Method)

Bu bölümde, steganografi hakkında genel bilgiler, LSB, PVD, EMD ve GEMD tekniklerinin matematiksel örnekleriyle birlikte veri gizleme ve çıkarma işlemlerinin nasıl yapıldığı ele alınmaktadır.

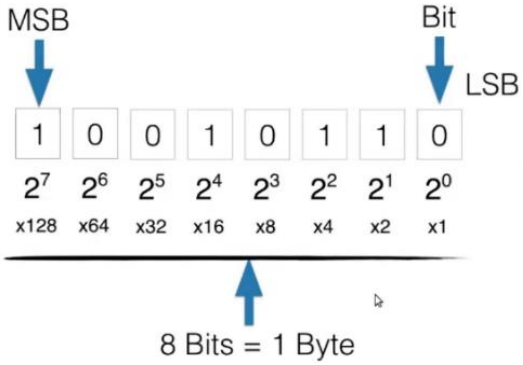
Steganografide, gizlenecek olan veri (secret-message) için önce bir örtü medya (cover-media) seçilmektedir. Örtü medya, veriyi içerisine gizleyecek olduğumuz sayısal nesnedir. Daha sonra, veri gizleme yöntemi kullanılarak alıcıya gönderilecek mesaj bu örtü-medyaya gizlenir. Örtü medyanın veri gizlenmiş haline stego medya (stego-media) denir. Bu gizleme işleminin çözülmesi sürecinde karşı tarafa ekstra bilgiler gerekecekse bu bilgiler için bir stego-anahtar (stego-key) oluşturulabilir. Steganografide izlenecek süreç, Şekil 1 'de genel hatlarıyla görülmektedir. Seçilmiş olan örtü medya içerisine, gizlenecek olan bilgi şifrelenerek veya şifrelenmeden, veri gizleme tekniği ile gömülmektedir. Bu işlem sonunda üretilen stego medya karşı tarafa gönderilir. Alıcı taraf, aynı veri gizleme tekniğini kullanarak gizli bilgiyi elde etmektedir. Bazı veri gizleme tekniklerinde, anahtar kullanıldığından mesajı alan tarafında bu anahtarı da bilmesi gerekmektedir. Bu sayede gönderici ve alıcı arasında güvenli bir iletişim sağlanmış olmaktadır.



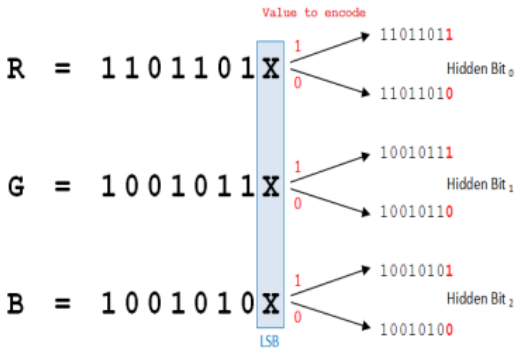
Şekil 1. Sayısal Steganografi Süreci (Digital Steganography Process)

2.1. En Düşük Anlamlı Bit (Least Significant Bit)

En düşük anlamlı bit tekniklerinde piksel değerleri ikili sayı tabanına çevrilir. Gri ölçekli bir görüntünün bir pikseli 8 bitten oluşur. Şekil 2'de görüldüğü üzere, 8 bitlik verimizin en soldaki yani değerce en büyük olan bite en yüksek anlamlı bit (Most Significant Bit); en sağdaki yani değerce en düşük olan bite ise en düşük anlamlı bit (Least Significant Bit) denir. LSB tekniğinde işlemler en az anlamlı bit ve bu bite yakın bitler üzerinde yapılır. Bunun nedeni, Şekil 3'te de görüldüğü üzere her bir renge ait en az anlamlı bitte yapılabilecek en büyük güncelleme 1 olduğundan, her bir rengin değerini en fazla 1/255 oranında değiştirecektir. Dolayısıyla, insan gözünün renkteki bu değişimi algılaması mümkün değildir.



Şekil 2. 8 Bitlik Veri İçin LSB (8-Bit Data for LSB)



Şekil 3. 24 Bitlik 3 Kanallı Renkli Görüntü İçin LSB (24-Bit 3 Channels Colored Image For LSB)

Şekil 4. 256x256 Gri Lena Görüntüsü (256x256 Gray-scale Lena Cover Image)

Şekil 4'te verilen 256x256 boyutlarındaki, gri ölçekli Lena örtü görüntüsüne, "sun" kelimesi gizlenecektir. Tablo 1'de görüldüğü üzere, gizlenecek olan kelimenin her bir harfini önce ASCII karşılığı, daha sonra ikilik sayı sistemindeki karşılığı bulunmaktadır. Her bir harf için aynı işlem gerçekleştirildikten sonra elde edilen 3 adet 8 bitlik veri, bir veri katarına dönüştürülmektedir (011100110111010101101110).

Tablo 1. "Sun" Kelimesinin ASCII ve İkili Taban Karşılıkları (ASCII And Binary Equivalent Of "Sun")

Karakterler	ASCII Karşılığı	İkili Sistem Değeri
"s"	115	01110011
"u"	117	01110101
"n"	110	01101110

Lena örtü görüntüsünün piksel değerleri belirli bir sırada alınmakta ve ikilik sayı sistemine dönüştürülmektedir. Gizlenecek veri katarından alınan her bir bit, lena örtü görüntüsündeki ilgili pikselin en düşük anlamlı biti ile değiştirilmektedir. Tablo 2 Lena örtü görüntüsüne ait piksel değerlerinin ASCII ve ikili sistem değerlerini, o piksele gizlenecek değeri, yeni piksel değerinin ikili sistemdeki ve ASCII değeri karşılığını sunmaktadır.

Tablo 2. LSB Örneği (LSB Example)

Lena Örtü Görüntü	ASCII	İkili Sistem Değeri	Gizli veri	Yeni Piksel Değeri	Yeni ASCII
1. Piksel	162	1010001**0**	0	1010001**0**	162
2. Piksel	162	1010001**0**	1	1010001**1**	163
3. Piksel	160	1010000**0**	1	1010000**1**	161
4. Piksel	162	1010001**0**	1	1010001**1**	163
5. Piksel	163	1010001**1**	0	1010001**0**	162
6. Piksel	160	1010000**0**	0	1010000**0**	162
7. Piksel	159	1001111**1**	1	1001111**1**	159
8. Piksel	158	1001111**0**	1	1001111**1**	159

Verinin geri elde edilme aşamasında ise, stego görüntüdeki ilgili pikselin son bitine bakılmaktadır. Gizli mesaj, gizleme yönteminde kullanılan sırada birleştirilmekte ve sonrasında ASCII karşılığından karaktere çevrilmektedir. Örnekte, stego görüntü piksel değerlerinin son bitleri incelendiğinde sırasıyla, 01110011 ikili verisi elde edilmekte, ASCII olarak 115 ve karakter karşılığı olarak "s" bulunmaktadır. LSB yönteminde, en düşük anlamlı bit sayısı değiştirilerek veri gizleme kapasitesi arttırılmaktadır. Bu durum LSB-k bit yöntemi şeklinde değerlendirilmektedir. Yöntemdeki k, örtü görüntüde bir piksele gizlenecek bit sayısını ifade etmektedir.

2.2. Piksel Değeri Farkı (Pixel Value Difference)

LSB tekniğinde sunulan örneklerden de görüldüğü üzere, yöntemin uygulanması çok basittir. Ayrıca, diğer yöntemlerle uyum sağlamak için de çok esnektir. Ancak, veri gizleme kapasitesindeki artış, stego görüntünün görsel kalitesini çok etkilemektedir. Görsel kalite sorununu çözmek için 2003 yılında piksel farkı değerine (Pixel Value Difference-PVD) dayalı yeni bir steganografik yaklaşım önerilmiştir (Wu ve Tsai, 2003). PVD, örtü

görüntüsünün ikişerli ardışık piksel gruplarına bölünmesine dayanmaktadır. Yöntemde ardışık iki piksel değeri arasındaki farka göre işlem yapılır. İki piksel arasındaki fark büyük yani doku yüksekse, o piksel çiftine daha fazla bit gizlenmektedir. Yöntem, piksel farklarına göre, o piksel aralığına kaç bitlik veri gizleneceğini belirlenmektedir. Veri gizleme kapasitesini gösteren referans değerler Tablo 3'te gösterilmektedir.

Tablo 3. PVD Referans Tablosu (PVD Reference Table)

Aralık (R)		**Genişlik (w)**	**Gizlenebilecek Bit Sayısı (t)**
Aralık (R_{alt})	**Aralık ($R_{üst}$)**		
0	7	8	3
8	15	8	3
16	31	16	4
32	63	32	5
64	127	64	6
128	255	123	7

PVD algoritması bir örnek üzerinde açıklanırsa; Lena örtü görüntüsünü oluşturan pikseller örtüşmeyecek şekilde alınarak ikili gruplar oluşturulmaktadır.

1.Grup : P1 = 162, P2 = 162
2.Grup : P1 = 160, P2 = 162
……..

Piksel grupları arasındaki fark belirlenir ve ilgili piksel grubuna saklanacak bit sayısı hesaplanır.

d=|P1 - P2| d=|162-162|=0 (1. Grup için)

Hesaplanan d değerinin, Tablo 3'e göre hangi aralıkta yer aldığı bulunmaktadır. Referans tabloya göre, $0 \leq d \leq 7$ olduğundan bu iki piksel arasındaki fark, 3 bitlik verinin gizlenmesi için uygundur. Gizlenecek verinin (01110011 0111010101101110) ilk 3 biti (011) alınmakta ve onluk sayı (Dec=3) sistemine dönüştürülmektedir. Sonrasında; d' = Ralt + Dec = 0 + 3 = 3 ve m =|d'-d|= |3 - 0|= 3 hesaplanır. Bu hesaplamalar yapıldıktan sonra denklem 1 kullanılarak stego piksel değerleri elde edilmektedir (P'1 =164 ve P'2 = 161) (Solak ve Altınışık, 2018).

$$(P'_i, P'_{i+1}) = \begin{cases} \left(P_i + \left\lceil \frac{m}{2} \right\rceil, P_{i+1} - \left\lfloor \frac{m}{2} \right\rfloor\right), eğer\ P_i \geq P_{i+1}\ ve\ d_i > d'_i \\ \left(P_i - \left\lceil \frac{m}{2} \right\rceil, P_{i+1} + \left\lfloor \frac{m}{2} \right\rfloor\right), eğer\ P_i < P_{i+1}\ ve\ d_i > d'_i \\ \left(P_i - \left\lceil \frac{m}{2} \right\rceil, P_{i+1} + \left\lfloor \frac{m}{2} \right\rfloor\right), eğer\ P_i \geq P_{i+1}\ ve\ d_i \leq d'_i \\ \left(P_i + \left\lceil \frac{m}{2} \right\rceil, P_{i+1} - \left\lfloor \frac{m}{2} \right\rfloor\right), eğer\ P_i < P_{i+1}\ ve\ d_i \leq d'_i \end{cases} \quad (1)$$

PVD yönteminde, gizlenen veriyi elde etmek için, gizleme işlemine çok benzer bir süreç işletilmektedir. Veri gizlenmiş örtü görüntüye ait piksel değerleri ikişerli gruplar şeklinde alınmaktadır (P1 =164 ve P2 = 161). Sonrasında bu piksel grupları arasındaki fark hesaplanmaktadır (d=|P1 - P2|, d=|164-161|=3). d=3 değeri, Tablo 3'de $0 \leq d \leq 7$ aralığında olduğundan bu iki piksel arasındaki fark, 3 bitlik verinin gizlendiğini göstermektedir. Sonrasında, Dec = |d – Ralt| işlemi yapılarak, Dec=|3-0|=3 (3)10 = (011)2 elde edilmektedir.

2.3. Değişim Yönünü Kullanma (Exploiting Modification Directions)

Değişim yönünü kullanma (Exploiting Modification Directions-EMD) stego görüntülerin yüksek doğruluğunu koruyan, iyi bilinen bir gömme tekniğidir (Zhang ve Wang, 2006). EMD algoritmasında örtü görüntüden n adet piksel alınarak işlem yapılmaktadır. Gizlenecek verinin ilk karakterinin ASCII değeri (2n+1) sayı sistemine dönüştürülüp piksellere uygulanmaktadır. Tüm bu işlemler sonunda, n pikselden sadece bir tanesinde ±1 değişim olmaktadır (Solak, 2020). Piksellerde hiç değişim de olmayabilir. Yani genel anlamda piksellerde değişim azdır. EMD'ye ait yük (payload) denklem (2) kullanılarak hesaplanmaktadır.

$$P_{EMD} = \frac{\log(2n+1)}{n} \quad (2)$$

Tablo 4. İşlem Gören Piksel Sayısına Göre Yük (Payload by Number of Pixels)

n	2	3	4	5	6	7	8	9
bpp	1,16	0,94	0,79	0,69	0,62	0,56	0,51	0,47

Tablo 4'te görüldüğü üzere EMD uygulanacak piksel sayısı arttıkça piksel başına gizlenecek bit (bpp) miktarı azalmaktadır. En yüksek bpp değerine n=2 için ulaşılmaktadır. EMD yönteminde denklem 3'te verilen eşitlik kullanılarak g_{EMD} değeri hesaplanmaktadır. Daha sonra gizlenecek olan veri (2n+1) sayı sistemine çevrilmektedir. Gizlenecek olan veri ile g_{EMD} değeri arasındaki fark denklem 4'e göre hesaplanmakta ve denklem 5'e uygun şekilde stego görüntü piksel değerleri elde edilmektedir.

$$g_{EMD}(P_1, P_2, \dots, P_n) = [\sum_{k=1}^{n}(p_k \; x \; k)\;] mod\;(2\;x\;n+1) \qquad (3)$$

$$fark = (veri - g_{EMD}) mod\;(2\;x\;n+1) \qquad (4)$$

$$\begin{cases} p_1, p_2, \dots p_n, \rightarrow\; fark\; =\; 0\; veya\; fark\; =\; g_{EMD} \\ p'_{fark} = p_{fark}\; +\; 1, \rightarrow\; fark\; \leq\; n \\ p'_{(2n+1-fark)} = p_{(2n+1-fark)}\; -\; 1, \rightarrow\; fark\; >\; n \end{cases} \qquad (5)$$

EMD yöntemini örnek ile açıklarsak;

Lena örtü görüntüsünden alınan ilk dört piksele veri gizlenecektir ((P1,P2,P3,P4)=(162,162,160,162)). Bu durumda n=4, sayı sistemi 2x4+1=9 olmaktadır. Denklem 3'e göre g_{EMD}=3 olarak hesaplanmaktadır. Örnekte gizlenecek olan veri=4 tür. Denklem 4'e göre fark=1 olarak bulunmaktadır. Bu işlemlere göre fark <= n (1<=4) olduğundan denklem 5'e göre, P1 = 163 olarak güncellenir ve diğer pikseller aynı kalmaktadır. Tablo 5, orijinal kapak görüntüsü piksel değerleri ile veri gizleme işlemi yapıldıktan sonra elde edilen yeni piksel değerlerini sunmaktadır.

Tablo 5. n=4 İçin EMD Piksellerindeki Değişim (For N=4 in EMD Method, Pixel Differences)

	P_1	**P_2**	**P_3**	**P_4**
Örtü görüntü	**162**	162	160	162
Stego görüntü	**163**	162	160	162

EMD yöntemi ile gizlenen veriyi tekrar elde etmek için denklem 6 kullanılmaktadır. Denklem 6 sonunda elde edilen veri (2n+1) sayı sistemindedir.

$$veri = [\sum_{k=1}^{n}(p_k \; x \; k)\;] mod\;(2\;x\;n+1) \qquad (6)$$

Örneğe göre stego görüntü piksel değerleri alınarak işlem yapıldığında (P1,P2,P3,P4)=(163,162,160,162), veri=4 olarak hesaplanmaktadır.

2.4. Genelleştirilmiş Değişim Yönünü Kullanma (Generalized Exploiting Modification Directions)

EMD yönteminde, veri gizleme kapasitesini iyileştirmek için farklı EMD tabanlı yöntemler geliştirilmiştir. Bunlardan birisi de Genelleştirilmiş Değişim Yönünü Kullanma (Generalized Exploiting Modification Directions - GEMD) yöntemidir (Kuo ve Wang, 2013). Yöntem yük kapasitesini 1 bpp üzerinde tutarak daha iyi bir stego görüntü kalitesi sunmaktadır. GEMD yöntemine ait yük, denklem 7 kullanılarak hesaplanmaktadır. Tablo 6'da ise piksel sayısına göre bpp cinsinden yük değişim miktarları sunulmaktadır.

$$P_{GEMD} = \frac{n+1}{n} \qquad (7)$$

Tablo 6. İşlem Gören Piksel Sayısına Göre Yük (Payload by Number of Pixels)

n	2	3	4	5	6	7	8	9
bpp	1,5	1,33	1,25	1,2	1,17	1,14	1,13	1,11

Tablo 6'da görüldüğü üzere GEMD uygulanacak piksel sayısı arttıkça bpp değeri azalmaktadır. En yüksek bpp değerine ise n=2 olduğu durumda 1,5 bpp olarak hesaplanmaktadır. Yöntemde seçilen n değerine n+1 bitlik bilgi gizlenmektedir. Dolayısıyla gizlenecek bilgi bit katarına çevrilmekte ve her seferinde n+1 bitlik kısım alınarak onluk sayı sistemindeki karşılığı bulunarak işlem yapılmaktadır.

$$g_{GEMD}(P_1, P_2, \dots, P_n) = [\sum_{k=1}^{n}(p_k \; x \; (2^k - 1))\;] mod\;(2^{n+1}) \qquad (8)$$

$$fark = (veri - g_{GEMD}) mod\ (2^{n+1}) \quad (9)$$

Eğer $fark = 2^n \rightarrow p'_1 = p_1 + 1, p'_n = p_n + 1$
Eğer $0 < fark < 2^n \rightarrow fark$ (n+1) bitlik ikili sayı sistemine çevrilir. $(s_n, s_{n-1}, \ldots s_0)_2$ Sonrasında aşağıdaki işlemler uygulanır.

```
for (x = n; x ≥ 1; x = x − 1)
  if (s_x = 0 ve s_{x−1} = 1) → n; p'_x = p_x + 1
  else if (s_x = 1 ve s_{x−1} = 0) → n; p'_x = p_x − 1
  else p'_x = p_x
end
```

(10)

Eğer $fark > 2^n \rightarrow temp = 2^{n+1} - fark\ temp$ değeri (n+1) bitlik ikili sayı sistemine çevrilir. $(s_n, s_{n-1}, \ldots s_0)_2$

```
for (x = n; x ≥ 1; x = x − 1)
  if (s_x = 0 ve s_{x−1} = 1) → n; p'_x = p_x − 1
  else if (s_x = 1 ve s_{x−1} = 0) → n; p'_x = p_x + 1
  else p'_x = p_x
end
```

EMD yönteminde olduğu gibi bu yöntemde de g_{GEMD} değeri hesaplanmaktadır. EMD yönteminde kullanılan 2n+1, bu yöntemde 2^{n+1} şeklinde kullanılmaktadır. Yöntemde ilk olarak denklem 8'de g_{GEMD} değerinin hesaplanması sunulmaktadır. Sonrasında bit katarından alınan n+1 bitlik veri onluk sayı sistemine çevrilir ve denklem 9'da sunulduğu gibi fark değeri hesaplanmaktadır. Elde edilen fark değeri ve n değeri ile denklem 10'da sunulan eşitlikler kullanılarak stego piksel değerleri hesaplanmaktadır. Denklem 10'da sunulan eşitlik incelendiğinde EMD yöntemine göre GEMD yönteminde birden fazla piksel değerinde değişiklik olduğu görülmektedir.

GEMD yöntemini örnek ile açıklarsak;

Lena örtü görüntüsünden alınan ilk üç piksele veri gizlenecektir $(P_1,P_2,P_3)=(162,162,160)$. Böylece n=3, ve gizlenecek veri 4 bit olacaktır. Diğer bölümlerde sunulan bit katarından (0111) dört bitlik veri alınarak onluk sisteme çevrilir (veri=7). Denklem 8'e göre hesaplanan g_{GEMD} değeri 8 olarak bulunmaktadır. Denklem 9'a göre hesaplanan fark değeri 15 çıkmaktadır. Elde edilen bu değerler kullanılarak denklem 10 sunulan eşitlikler ve işlemler uygulandığında, fark>2^n olduğundan temp = 2^{n+1}-fark=1 bulunmakta ve stego piksel değerleri $(P'_1, P'_2, P'_3)=(161, 162, 160)$ elde edilmektedir. Tablo 7, orijinal kapak görüntüsü piksel değerleri üzerinde GEMD yöntemi ile veri gizleme işlemi yapıldıktan sonra elde edilen yeni piksel değerlerini sunmaktadır. GEMD yöntemi ile gizlenen veriyi tekrar elde etmek için denklem 11 kullanılmaktadır.

Tablo 7. n=3 İçin GEMD Piksellerindeki Değişim (For N=3 in GEMD Method, Pixel Differences)

	P_1	**P_2**	**P_3**
Örtü görüntü	**162**	162	160
Stego görüntü	**161**	162	160

$$veri = [\ \textstyle\sum_{k=1}^{n}(p'_k\ x\ (2^k - 1))\ ] mod\ (2^{n+1}) \quad (11)$$

Örneğe göre stego görüntü piksel değerleri alınarak işlem yapıldığında; n=3 ve stego pikseller (P'1, P'2, P'3)=(161, 162, 160); Veri=161x1+162x3+160x5 mod 16 = 7 çıkmaktadır. Sonrasında n+1 bitlik ikili sayı sistemine çevrilerek (0111) değeri bulunmaktadır.

3. Deneysel Çalışmalar (Experimental Studies)

Bu bölümde, LSB, PVD, EMD ve GEMD yöntemlerinin taşıma yükü, tepe sinyal gürültü oranı, yapısal benzerlik endeksi gibi başarım ölçütleri kullanılarak performansları sunulmaktadır. Ayrıca ilgili yöntemlerin, histogram analizi ve RS analiz testleri gerçekleştirilerek steganaliz ataklarına karşı dayanıklılığı test edilmektedir. Deneysel çalışmalar, AMD Phenom II X6 1090T işlemci, 10 GB 1600Mhz RAM ve Windows 7 Professional 64-bit işletim sistemine sahip bir masaüstü bilgisayar kullanılarak Matlab R2020a yazılımı ile gerçekleştirilmiştir. Ayrıca, veri gizleme işleminde standart veri tabanlarında yer alan ve şekil 5'te sunulan 512x512 boyutlarında Lena, Baboon, Pepper ve Airplane renkli örtü görüntüleri kullanılmıştır.

(a) Lena (b) Baboon (c) Peppers (d) Airplane

Şekil 5. Renkli Örtü Görüntüler (Colored Cover Images)

Veri gizleme yöntemlerini karşılaştırırken kullanılan en önemli başarım ölçütlerin den biri yüktür. Stego-görüntüdeki piksel başına düşen gömülü gizli bitlerin sayısı yük (payload) olarak adlandırılmaktadır. Genellikle piksel başına bit (bpp) olarak temsil edilir. Denklem 12'de sunulduğu üzere gömülen bit sayısının stego görüntüsündeki toplam piksel sayısına bölünmesiyle elde edilmektedir. İyi bir veri gizleme yönteminde, görsel kalite korunurken yükün mümkün olduğunca yüksek olması istenmektedir.

$$yük\ (bpp) = \frac{Gizlenen\ bit\ sayısı}{Stego\ görüntüdeki\ toplam\ piksel\ sayısı} \qquad (12)$$

Gizli verileri örtü görüntüsünün içerisine saklarken piksel değerlerinde değişiklikler olmaktadır. Bu durum, stego görüntüsünün algılanamazlığını doğrudan etkilediği için değişikliklerin analiz edilmesi gerekir. Tepe sinyal gürültü oranı (Peak Signal-to-Noise Ratio – PSNR), örtü ve stego görüntüleri arasındaki ortalama karesel hata değerini analiz ederek stego-görüntüsünün kalitesini ölçmek için kullanılan popüler ve birinci sınıf metriklerden biridir. PSNR değeri, 0 ile 100 arasında değerler alır ve 100'e yakın değerler çıkması örtü ve stego görüntünün birbirine benzediğini ifade eder. Ayrıca, veri gizleme tekniklerinde görüntü kalitesini koruyabilmek için PSNR değerinin 30'dan büyük olması hedeflenmektedir. PSNR değerini hesaplamak için önce ortalama karesel hata (Mean Squared Error - MSE) denklem 13 kullanılarak hesaplanır. Ardından denklem 14 ile PSNR değeri elde edilir (Pradhan vd., 2016).

$$MSE = \frac{\sum_{i=1}^{n}(C_i - C'_i)^2}{n} \qquad (13)$$

$$PSNR(dB) = 10log_{10}\frac{255^2}{MSE} \qquad (14)$$

Yapısal benzerlik endeksi adı verilen (Structural Similarity Index Measure - SSIM), örtü ve stego görüntüler arasındaki benzerliği incelemek için kullanılan başarım ölçütüdür. SSIM değeri, 0 – 1 arasında değerler almakta olup, veri gizleme yöntemlerinde bu değerin 1'e yakın bir bir değer olması istenmektedir. Denklem 15 kullanılarak SSIM değeri hesaplanmaktadır.

$$SSIM(x,y) = \frac{(2\mu_x\mu_y + c_1)(2\sigma_x\sigma_y + c_2)}{(\mu_{x^2} + \mu_{y^2} + c_1)(\sigma_{x^2} + \sigma_{y^2} + c_2)} \qquad (15)$$

Deneysel çalışmalarda ilk olarak LSB tekniği kullanılarak 512x512 boyutlarındaki renkli Lena örtü görüntüsüne 512x512 boyutlarında gri ölçekli Lena görüntüsünden sırayla alınan veriler gizlenmiştir. Bu yöntemde, en düşük anlamlı bit sayısı arttıkça, gizli mesaj saklama kapasitesi de artmaktadır. Ancak, bu artış beraberinde, görüntü kalitesinde azalmayı da yanında getirir. Şekil 6 da LSB-1, LSB-2, LSB-3 ve LSB-5 bit stego-görüntüler sunulmaktadır. Gizli veriler, stego-görüntünün üst tarafında bulunan piksellere LSB-1, LSB-2 ve LSB-3 bit ile sırayla yerleştirilmesine rağmen insan gözünün bunu fark etmesi kolay değildir. Ancak LSB-5 bit uygulanmış stego görüntüde ise, görüntü kalitesinin bozulduğu gözle görülür hale gelmektedir.

(a) LSB-1 bit (b) LSB-2 bit (c) LSB-3 bit (d) LSB-5 bit

Şekil 6. LSB Yöntemi Karşılaştırma (LSB Method Comparison)

Tablo 8'de LSB-k bit (k=1,2,3) yöntemi için farklı örtü görüntülere veri gizleme sonucunda elde edilen PSNR, SSIM, yük ve kapasite karşılaştırmaları sunulmaktadır. LSB-1 yönteminin daha yüksek PSNR ve SSIM değerleri sunduğu gözlenirken, yük ve kapasitelerinin diğer LSB-k bit yöntemlerinden daha düşük olduğu görülmektedir. LSB-3 bit yönteminde ise, yük ve kapasitenin yüksek olduğu ancak PSNR ve SSIM gibi görüntü kalitesini ifade eden ölçütlerin düşük olduğu görülmektedir. LSB-3 bit yönteminde yüksek kapasitede veri gizlenmesine rağmen PSNR değerinin literatürde sunulan kabul edilebilir (30dB) seviyenin üzerinde olduğu görülmektedir.

Tablo 8. LSB-K Bit Veri Gizleme Yönteminin Karşılaştırması (Comparison of LSB-K Bit Methods)

Görüntü	Yöntem	PSNR	SSIM (%)	Yük (bpp)	Kapasite
Lena	LSB-1	51,1312	99,5977	1,0000	262144
	LSB-2	43,4300	98,5131	2,0000	524288
	LSB-3	36,3669	94,7375	3,0000	786432
Baboon	LSB-1	51,1449	99,8732	1,0000	262144
	LSB-2	43,4296	99,5682	2,0000	524288
	LSB-3	36,3591	98,4665	3,0000	786432
Airplane	LSB-1	51,1247	99,5913	1,0000	262144
	LSB-2	43,4726	98,5088	2,0000	524288
	LSB-3	36,4745	95,1675	3,0000	786432
Peppers	LSB-1	51,1460	99,5120	1,0000	262144
	LSB-2	43,4035	98,4278	2,0000	524288
	LSB-3	36,2793	94,9210	3,0000	786432

Tablo 9. Veri Gizleme Yöntemlerinin Karşılaştırması (Comparison of Data Hiding Methods)

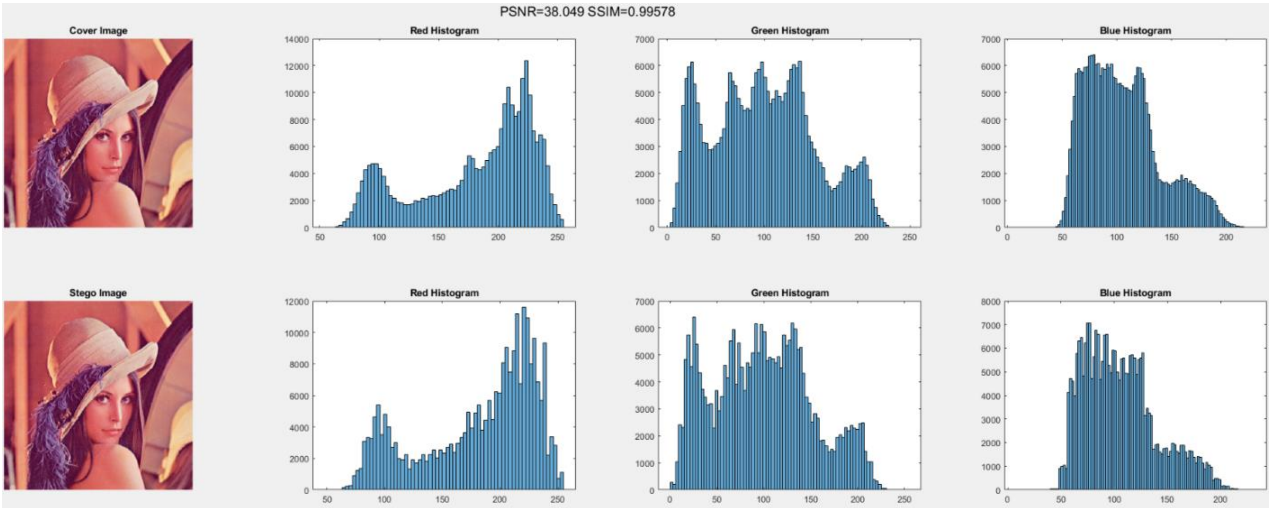
Görüntü	Yöntem	PSNR	SSIM	bpp	Kapasite
Lena	LSB-1	51,1312	99,5977	1,0000	262144
	LSB-2	43,4300	98,5131	2,0000	524288
	LSB-3	36,3669	94,7375	3,0000	786432
	PVD	41,3744	97,8010	1,5632	409785
	EMD	52,1571	99,6833	0,9888	259200
	GEMD	50,1999	99,5110	1,4905	390728
Baboon	LSB-1	51,1449	99,8732	1,0000	262144
	LSB-2	43,4296	99,5682	2,0000	524288
	LSB-3	36,3591	98,4665	3,0000	786432
	PVD	37,1233	98,7128	1,7440	457169
	EMD	52,1544	99,9000	0,9888	259200
	GEMD	50,1982	99,8456	1,4905	390728
Airplane	LSB-1	51,1247	99,5913	1,0000	262144
	LSB-2	43,4726	98,5088	2,0000	524288
	LSB-3	36,4745	95,1675	3,0000	786432
	PVD	40,3124	96,8166	1,5633	409817
	EMD	52,1765	99,6482	0,9888	259200
	GEMD	50,1796	99,4455	1,4905	390728
Peppers	LSB-1	51,1460	99,5120	1,0000	262144
	LSB-2	43,4035	98,4278	2,0000	524288
	LSB-3	36,2793	94,9210	3,0000	786432
	PVD	41,5773	96,7045	1,5297	401007
	EMD	52,1537	99,5926	0,9888	259200
	GEMD	50,1600	99,3613	1,4905	390728

Şekil 5'te sunulan örtü görüntülere, gri ölçekli Lena görüntüsünden alınan veriler LSB-1, LSB-2, LSB-3, PVD, EMD ve GEMD yöntemleri kullanılarak maksimum kapasitelerinde gizlenmiştir. Bu işlem sonunda yük, toplam taşıma kapasitesi, PSNR ve SSIM değerlendirme ölçütlerine ait başarım Tablo 9'de sunulmaktadır.

Şekil 7. Veri Gizleme Yöntemlerinin Karşılaştırması (Comparison of Data Hiding Methods)

Şekil 7 LSB-1, LSB-2, LSB-3, PVD, EMD, GEMD yöntemlerinin, PSNR, SSIM, yük ve toplam kapasite yönünden grafiksel olarak karşılaştırmasını sunmaktadır. EMD yönteminde PSNR ve SSIM gibi değerlerin yüksek olduğu grafiklerden görülmektedir. Veri gizleme kapasitesi olarak LSB-3 bit yönteminin yüksek olduğunu grafikler sunmaktadır.

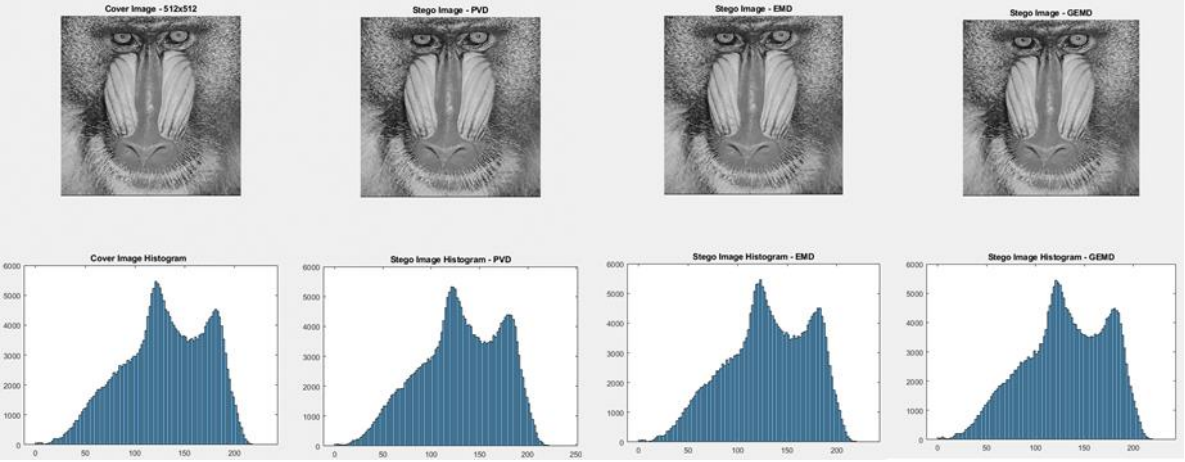
Şekil 8'de Lena örtü görüntüsü, kırmızı, yeşil ve mavi renk kanalına ait histogramlar, LSB-3 yöntemi kullanılarak tam kapasitede veri gizlenmiş stego görüntüsü ve histogramları sunulmaktadır. Görüldüğü üzere, stego görüntüye ait histogramlarda, görüntü içinde veri olduğunu gösteren taraklanma etkisi gözlemlenmektedir.



Şekil 8. LSB-3 İçin Histogram Karşılaştırması (Histogram Comparison For LSB-3)

Şekil 9'da gri ölçekli Baboon örtü görüntüsüne maksimum kapasitede PVD, EMD ve GEMD yöntemleri ile veri gizlemesi yapılmış stego görüntüler ve histogramları sunulmaktadır. Görüldüğü üzere üç yönteme ait histogramlarda da taraklanma etkisi gözlenmemiştir. Yani bu yöntemlerle veri gizleme yapıldığında, görüntü

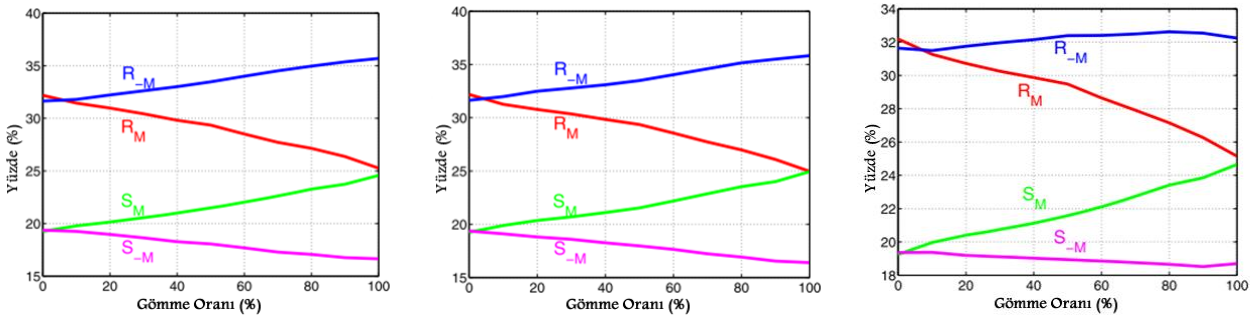
histogramı, stego görüntü içerisinde gizli veri olduğuna dair net bir bilgi vermemektedir. Bu durum, PVD, EMD ve GEMD yöntemlerinin, LSB yöntemine göre daha dayanıklı olduğunu ve algılanamazlığının daha yüksek olduğunu göstermektedir.



(a) Örtü Görüntü (b) PVD (c) EMD (d) GEMD

Şekil 9. PVD, EMD ve GEMD Histogram Karşılaştırması (Histogram Comparison For PVD, EMD and GEMD)

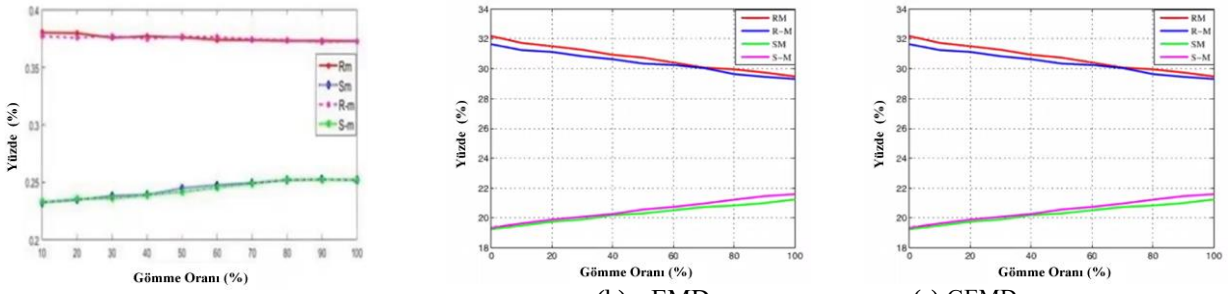
Veri gizleme tekniklerin güvenlik testleri için kullanılan bir başka yöntem ise RS analizidir. Makale çalışması kapsamında gerçekleştirilen LSB-1, LSB-2 ve LSB-3 bit tekniklerine ait RS analiz sonuçları Şekil 10'da verilmiştir. Şekilden görüldüğü üzere, örtü ve stego-görüntü için düzenli (Regular-R) ve tekil (Singular-S) piksel grupları örtüşmemektedir. Bu bilgi görüntü içinde gizlenmiş veri olduğunu ifade etmektedir. Bu yüzden LSB teknikleri her ne kadar uygulaması kolay ve yüksek kapasite sunabilse de algılanamazlık açısından yetersizdir.



(a) LSB-1 bit (b) LSB-2 bit (c) LSB-3 bit

Şekil 10. LSB İçin RS Analiz Testleri (RS Analysis Tests for LSB)

Şekil 11'de PVD, EMD ve GEMD yöntemleri için RS analiz testleri sunulmaktadır. Testler incelendiğinde, örtü ve stego görüntülerin düzenli ve tekil piksel gruplarının birbirinden ayrışmadığı görülmektedir. Bu bilgiye göre, PVD, EMD ve GEMD yöntemlerinin RS analiz ataklarına karşı dayanıklı olduğu görülmektedir.



(a) PVD (b) EMD (c) GEMD

Şekil 11. PVD, EMD ve GEMD İçin RS Analiz Testleri (RS Analysis Tests For PVD, EMD, GEMD)

4. Sonuç ve Tartışma (Result and Discussion)

Makalede, görüntü steganografisinde yaygın kullanılan LSB, PVD, EMD ve GEMD yöntemlerin karşılaştırmalı

başarım analizi gerçekleştirilmiştir. Görüntü steganografisi kapsamında bahsi geçen yöntemler, birbirlerine farklı kriterlerde üstünlük sağlamaktadır. Bu nedenle, yöntemin belirlenmesinde, ne için kullanılacağı ve kullanılacağı alanda hangi kriterlerin daha gerekli olduğunun belirlenmesi büyük önem taşımaktadır. LSB yöntemi, uygulaması çok kolay bir yöntemdir. Bunun yanında LSB-3 bit yüksek kapasitede veri gizleme imkanı sunmaktadır. 512x 512 boyutlarında renkli örtü görüntülerde, LSB-3 bit ile 786432 bitlik en yüksek kapasite değerine ulaşılırken, LSB-k bit yöntemi dışında bu değere en yakın kapasite, Baboon örtü görüntüsünde PVD yöntemi ile elde edilen 457169 bittir. PVD yöntemi için diğer görüntülerde ise kapasite 400000-410000 bit arasında değişmektedir. Aynı görüntüde LSB-3 bit yöntemi, PVD yöntemine göre %42-49 daha fazla kapasite sunmaktadır. Ancak, LSB-3 bit ile elde edilen görüntü kalitesi (PSNR), yaklaşık %36 ile uygulanan yöntemler arasında en düşük değere sahiptir. Buna karşın PVD, tüm görüntülerde LSB-3 bit'e göre daha iyi görüntü kalitesi sunmuştur. En iyi görüntü kalitesi ise EMD, GEMD ve LSB-1 yöntemleri ile elde edilmiştir. LSB-1 iyi bir görüntü kalitesi sunsa da RS analizi sonuçlarından ve görüntü histogramında meydana gelen taraklanma etkisinden anlaşıldığı üzere algılanamazlık konusunda problemler yaşatabilmektedir. PVD yöntemi, EMD yöntemine göre %18-25 daha fazla kapasite sunabilmekteyken EMD yöntemi PVD yöntemine göre %20-29 daha iyi görüntü kalitesi sunabilmektedir. GEMD yöntemi, EMD yöntemine göre yaklaşık %34'lük bir kapasite artışı sağlarken GEMD ile elde edilen görüntü kalitesinde yaklaşık %4'lük bir kayıp yaşanmıştır.

PVD, LSB-1 yöntemine göre, yüksek kapasitede veri gizlemekte, histogram ve RS analizlerine göre veri daha dayanıklı olmakta ve yüksek kalitede bir stego-görüntü sağlamaktadır. Diğer yandan EMD ve GEMD yöntemleri, LSB'ye göre kapasite açısından daha az olanaklar sunsa da görsel kalite ve algılanamazlık konusunda gayet başarılı sonuçlar vermektedir. Yüksek kapasite ihtiyacının olduğu ancak algılanamazlığın ön planda olmadığı durumlarda LSB, algılanamazlığın ön planda olduğu durumlarda GEMD, kenar bölgelerinin yani doku farklılıklarının yoğun olduğu örtü görüntülerinde yüksek kapasite için PVD tercih edilmelidir.

Teşekkür (Acknowledgement)

Bu çalışma Kocaeli Üniversitesi Bilimsel Araştırma Projeleri Koordinasyon Birimi tarafından FBA-2021-2488 numaralı proje kapsamında desteklenmiştir.

Çıkar Çatışması (Conflict of Interest)

Yazarlar tarafından herhangi bir çıkar çatışması beyan edilmemiştir. No conflict of interest was declared by the authors.

Kaynaklar (References)

Amirtharajan, R., & Rayappan, J. B. B., 2012. An intelligent chaotic embedding approach to enhance stego-image quality. Information Sciences, 193, 115-124. https://doi.org/10.1016/j.ins.2012.01.010.

Chan, C. K., & Cheng, L. M., 2004. Hiding data in images by simple LSB substitution. Pattern recognition, 37(3), 469-474.https://doi.org/10.1016/j.patcog.2003.08.007.

Chang, K. C., Chang, C. P., Huang, P. S., & Tu, T. M., 2008. A Novel Image Steganographic Method Using Tri-way Pixel-Value Differencing. Journal of multimedia, 3(2). https://doi.org/10.4304/jmm.3.2.37-44.

Fridrich, J., Goljan, M., & Du, R., 2001. Reliable detection of LSB steganography in color and grayscale images. In Proceedings of the 2001 workshop on Multimedia and security: new challenges (pp. 27-30).

Hussain, M., Wahab, A. W. A., Anuar, N. B., Salleh, R., & Noor, R. M., 2015. Pixel value differencing steganography techniques: Analysis and open challenge. In 2015 IEEE International Conference on Consumer Electronics-Taiwan (pp. 21-22). IEEE. https://doi.org/10.1109/ICCE-TW.2015.7216859.

Hussain, M., Abdul Wahab, A. W., Javed, N., & Jung, K. H., 2016. Hybrid data hiding scheme using right-most digit replacement and adaptive least significant bit for digital images. Symmetry, 8(6), 41. https://doi.org/10.3390/sym8060041.

Hussain, M., Wahab, A. W. A., Ho, A. T., Javed, N., & Jung, K. H., 2017. A data hiding scheme using parity-bit pixel value differencing and improved rightmost digit replacement. Signal Processing: Image Communication, 50, 44-57. https://doi.org/10.1016/j.image.2016.10.005

Hussain, M., Wahab, A. W. A., Idris, Y. I. B., Ho, A. T., & Jung, K. H., 2018. Image steganography in spatial domain: A survey. Signal Processing: Image Communication, 65, 46-66. https://doi.org/10.1016/j.image.2018.03.012.

Jung, K. H., 2010. High-capacity steganographic method based on pixel-value differencing and LSB replacement methods. The Imaging Science Journal, 58(4), 213-221. https://doi.org/10.1179/136821910X12651933390584.

Jung, K. H., & Yoo, K. Y., 2015. Steganographic method based on interpolation and LSB substitution of digital images. Multimedia Tools and Applications, 74(6), 2143-2155. https://doi.org/10.1007/s11042-013-1832-y.

Kadhim, I. J., Premaratne, P., Vial, P. J., & Halloran, B., 2019. Comprehensive survey of image steganography: Techniques, Evaluations, and trends in future research. Neurocomputing, 335, 299-326. https://doi.org/10.1016/j.neucom.2018.06.075.

Kieu, T. D., & Chang, C. C., 2011. A steganographic scheme by fully exploiting modification directions. Expert systems with Applications, 38(8), 10648-10657. https://doi.org/10.1016/j.eswa.2011.02.122.

Konyar, M. Z., & Solak, S., 2021. Efficient data hiding method for videos based on adaptive inverted LSB332 and secure frame selection with enhanced Vigenere cipher. Journal of Information Security and Applications, 63, 103037. https://doi.org/10.1016/j.jisa.2021.103037.

Konyar, M. Z., & Öztürk, S., 2020. Reed solomon coding-based medical image data hiding method against salt and pepper noise. Symmetry, 12(6), 899. https://doi.org/10.3390/sym12060899.

Kuo, W. C., & Wang, C. C., 2013. Data hiding based on generalised exploiting modification direction method. The Imaging Science Journal, 61(6), 484-490. https://doi.org/10.1179/1743131X12Y.0000000011.

Kuo, W. C., Kuo, S. H., & Huang, Y. C., 2013. Data hiding schemes based on the formal improved exploiting modification direction method. Applied Mathematics & Information Sciences Letters, 1(3), 1-8.

Kuo, W. C., & Kao, M. C., 2013. A steganographic scheme based on formula fully exploiting modification directions. IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences, 96(11), 2235-2243. https://doi.org/10.1587/transfun.E96.A.2235.

Kuo, W. C., Wang, C. C., & Hou, H. C., 2016. Signed digit data hiding scheme. Information Processing Letters, 116(2), 183-191. https://doi.org/10.1016/j.ipl.2015.08.003.

Lamiles, O. E. M., 2016. Analysis and Experimental Study of EMD and GEMD Steganographic Methods (Master's thesis, Eastern Mediterranean University (EMU)-Doğu Akdeniz Üniversitesi (DAÜ)).

Liao, X., Wen, Q. Y., Zhao, Z. L., & Zhang, J., 2012. A novel steganographic method with four-pixel differencing and modulus function. Fundamenta Informaticae, 118(3), 281-289. https://doi.org/10.3233/FI-2012-714.

Liao, X., Wen, Q., & Zhang, J., 2013. Improving the adaptive steganographic methods based on modulus function. IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences, 96(12), 2731-2734. https://doi.org/10.1587/transfun.E96.A.2731.

Liao, X., Guo, S., Yin, J., Wang, H., Li, X., & Sangaiah, A. K., 2018. New cubic reference table based image steganography. Multimedia Tools and Applications, 77(8), 10033-10050. https://doi.org/10.1007/s11042-017-4946-9.

Liao, X., Wen, Q., & Zhang, J., 2012. A novel steganographic method with four-pixel differencing and exploiting modification direction. IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences, 95(7), 1189-1192. https://doi.org/10.1587/transfun.E95.A.1189.

Liao, X., Qin, Z., & Ding, L., 2017. Data embedding in digital images using critical functions. Signal Processing: Image Communication, 58, 146-156. https://doi.org/10.1016/j.image.2017.07.006.

Li, B., He, J., Huang, J., & Shi, Y. Q., 2011. A survey on image steganography and steganalysis. J. Inf. Hiding Multim. Signal Process., 2(2), 142-172.

Liu, Y., Qu, X., & Xin, G., 2016. A ROI-based reversible data hiding scheme in encrypted medical images. Journal of Visual Communication and Image Representation, 39, 51-57. https://doi.org/10.1016/j.jvcir.2016.05.008.

Lu, T. C., &Vo, T. N., 2020. Reversible steganography techniques: A survey. In Digital Media Steganography (pp. 189-213). Academic Press.

Muhammad, K., Ahmad, J., Rehman, N. U., Jan, Z., & Sajjad, M., 2017. CISSKA-LSB: color image steganography using stego key-directed adaptive LSB substitution method. Multimedia Tools and Applications, 76(6), 8597-8626. https://doi.org/10.1007/s11042-016-3383-5.

Muhammad, K., Sajjad, M., & Baik, S. W., 2016. Dual-level security based cyclic18 steganographic method and its application for secure transmission of keyframes during wireless capsule endoscopy. Journal of medical systems, 40(5), 114. https://doi.org/10.1007/s10916-016-0473-x.

Navadiya, C., & Sanghani, N., 2021. Comparative Survey of Digital Image Steganography Spatial Domain Techniques. In Data Science and Intelligent Applications (pp. 491-497). Springer, Singapore. https://doi.org/10.1007/978-981-15-4474-3_54.

Nguyen, T. D., Arch-Int, S., & Arch-Int, N., 2016. An adaptive multi bit-plane image steganography using block data-hiding. Multimedia tools and applications, 75(14), 8319-8345. https://doi.org/10.1007/s11042-015-2752-9

Pan, F., Li, J., & Yang, X., 2011. Image steganography method based on PVD and modulus function. In 2011 International Conference on Electronics, Communications and Control (ICECC) (pp. 282-284). IEEE.

Pevny, T., Bas, P., & Fridrich, J., 2010. Steganalysis by subtractive pixel adjacency matrix. IEEE Transactions on information Forensics and Security, 5(2), 215-224. https://doi.org/10.1109/TIFS.2010.2045842.

Petitcolas, F. A., Anderson, R. J., & Kuhn, M. G., 1999. Information hiding-a survey. Proceedings of the IEEE, 87(7), 1062-1078. https://doi.org/10.1109/5.771065.

Pradhan, A., Sahu, A. K., Swain, G., & Sekhar, K. R., 2016. Performance evaluation parameters of image steganography techniques. In 2016 International Conference on Research Advances in Integrated Navigation Systems (RAINS) (pp. 1-8). IEEE. https://doi.org/10.1109/RAINS.2016.7764399.

Puteaux, P., Ong, S., Wong, K., & Puech, W. (2021). A survey of reversible data hiding in encrypted images–The first 12 years. Journal of Visual Communication and Image Representation, 77, 103085. https://doi.org/10.1016/j.jvcir.2021.103085.

Sahu, M., Padhy, N., Gantayat, S. S., & Sahu, A. K., 2021. Shadow image based reversible data hiding using addition and subtraction logic on the LSB planes. Sensing and Imaging, 22(1), 1-31. https://doi.org/10.1007/s11220-020-00328-w.

Sahu, A. K., Swain, G., Sahu, M., & Hemalatha, J. (2021). Multi-directional block based PVD and modulus function image steganography to avoid FOBP and IEP. Journal of Information Security and Applications, 58, 102808. https://doi.org/10.1016/j.jisa.2021.102808.

Sarreshtedari, S., & Akhaee, M. A., 2013. One-third probability embedding: a new±1 histogram compensating image least significant bit steganography scheme. IET image processing, 8(2), 78-89. https://doi.org/10.1049/iet-ipr.2013.0109.

Shivani, S., 2022. Verifiable medical images for E-healthcare: A novel watermarking approach using robust bit-wise association of self-mutating offsprings of pixels. Microprocessors and Microsystems, 104483. https://doi.org/10.1016/j.micpro.2022.104483.

Solak, S., & Altınışık, U., 2018. LSB Substitution and PVD performance analysis for image steganography. International Journal of Computer Sciences and Engineering, 6(10), 1-4. https://doi.org/10.26438/ijcse/v6i10.14.

Solak, S., & Altınışık, U., 2019. A new approach for Steganography: Bit shifting operation of encrypted data in LSB (SED-LSB). Bilişim Teknolojileri Dergisi, 12(1), 75-81. https://doi.org/10.17671/gazibtd.435437.

Solak, S., & Altınışık, U., 2019. Image steganography based on LSB substitution and encryption method: adaptive LSB+ 3. Journal of Electronic Imaging, 28(4), 043025. https://doi.org/10.1117/1.JEI.28.4.043025.

Solak, S., 2020. High Embedding Capacity Data Hiding Technique Based on EMSD and LSB Substitution Algorithms. IEEE Access, 8, 166513-166524. https://doi.org/10.1109/access.2020.3023197.

Solak, S., & Altınışık, U., 2021. Image Steganography-Based GUI Design to Hide Agricultural Data. Gazi University Journal of Science, 34(3), 748-763. https://doi.org/10.35378/gujs.703803.

Thambiraja, E., Ramesh, G., & Umarani, D. R., 2012. A survey on various most common encryption techniques. International journal of advanced research in computer science and software engineering, 2(7).

Tuncer, T., & Sönmez, Y., 2019. A Novel Data Hiding Method based on Edge Detection and 2k Correction with High Payload and High Visual Quality. Balkan Journal of Electrical and Computer Engineering, 7(3), 311-318. https://doi.org/10.17694/bajece.573514.

Wan, W., Wang, J., Zhang, Y., Li, J., Yu, H., & Sun, J., 2022. A Comprehensive Survey on Robust Image Watermarking. Neurocomputing. https://doi.org/10.1016/j.neucom.2022.02.083.

Wang, S., Zheng, D., Zhao, J., Tam, W. J., & Speranza, F., 2006. An image quality evaluation method based on digital watermarking. IEEE transactions on circuits and systems for video technology, 17(1), 98-105. https://doi.org/10.1109/TCSVT.2006.887086.

Wang, Z. H., Chang, C. C., & Li, M. C., 2012. Optimizing least-significant-bit substitution using cat swarm optimization strategy. Information Sciences, 192, 98-108. https://doi.org/10.1016/j.ins.2010.07.011.

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.

Wu, H. C., Wu, N. I., Tsai, C. S., & Hwang, M. S., 2005. Image steganographic scheme based on pixel-value differencing and LSB replacement methods. IEE Proceedings-Vision, Image and Signal Processing, 152(5), 611-615. https://doi.org/10.1049/ip-vis:20059022.

Xu, W. L., Chang, C. C., Chen, T. S., & Wang, L. M., 2016. An improved least-significant-bit substitution method using the modulo three strategy. Displays, 42, 36-42. https://doi.org/10.1016/j.displa.2016.03.002.

Yang, H., Sun, X., & Sun, G., 2009. A high-capacity image data hiding scheme using adaptive LSB substitution. Radioengineering, 18(4), 509-516.

Yang, C. H., Wang, S. J., & Weng, C. Y., 2010. Capacity-raising steganography using multi-pixel differencing and pixel-value shifting operations. Fundamenta Informaticae, 98(2-3), 321-336. https://doi.org/10.3233/FI-2010-229.

Yang, C. H., Weng, C. Y., Tso, H. K., & Wang, S. J., 2011. A data hiding scheme using the varieties of pixel-value differencing in multimedia images. Journal of Systems and Software, 84(4), 669-678. https://doi.org/10.1016/j.jss.2010.11.889.

Zhang, X., & Wang, S., 2006. Efficient steganographic embedding by exploiting modification direction. IEEE Communications Letters, 10(11), 781-783. https://doi.org/10.1109/LCOMM.2006.060863.