

# İmge Histogramı Kullanılarak Geometrik Ataklara Dayanıklı Yeni Bir Veri Gizleme Tekniği Tasarımı ve Uygulaması

**Yıldırım Yalman, İsmail Ertürk**

Kocaeli Üniversitesi Elektronik ve Bilgisayar Eğitimi Bölümü  
yildiray.yalman@kocaeli.edu.tr, erturk@kocaeli.edu.tr

**Özet:** Histogram, bir işlem neticesinde elde edilen ölçüm sonuçlarının dağılımını gösteren grafiklerdir. İmge histogramı ise sayısal bir resmin renk tonlarının dağılımını gösterir. Son yıllarda çoklu ortam uygulamaları için veri gizleme (steganography) temelinde yapılan çalışmalar yoğun ilgi görmektedir. Bu bildiride sunulan yeni yöntemin ve uygulamanın temel amacı, sayısal imgelere ait histogram değerlerini kullanarak veri gizleme işlemi gerçekleştirmektir. Uygulama En Küçük Değerlikli Bitler (LSBs) kullanılarak yapılan veri gizleme tekniğini histogram işleme ile birleştirmektedir. Yapılan deneysel çalışma sonuçları, sonuç imgelerinin döndürme, görüntüleme oranını değiştirme ve eğme gibi geometrik ataklara karşı oldukça dayanıklı olduğunu göstermektedir. Klasik eşleniklerine kıyasla, önerilen uygulamanın başarımlar değerleri nispeten daha iyi PSNR değerleri için daha fazla gömü verisi kapasitesi sağlamaktadır.

**Abstract:** A histogram is used to graphically summarize and display the distribution of a process data set. An image histogram is type of histogram which acts as a graphical representation of the tonal distribution in a digital image. For the last decade, researches on secret information embedding have received considerable attention due to its potential applications in especially multimedia communications. The main objective of this research work is to implement a steganography application simply based on histogram modification. In this work, the proposed approach combines the LSB embedding technique and histogram processing. The stego images show robustness against geometrical attacks like rotation, change of aspect ratio and warping. The application of proposed method has relatively higher data embedding capacity than similar applications, as well as providing better PSNR results.

**Anahtar Kelimeler:** Steganografi, Veri Gizleme, Geometrik Atak, Histogram.

## 1. Giriş

Veri gizleme teknikleri, gelişen bilgisayar teknolojisi ile çok büyük ilerleme kaydetmiş, çeşitli matematiksel algoritmalarından oluşan bilgisayar yazılımlarıdır. Günümüze kadar oldukça fazla veri gizleme tekniği ortaya atılmış ve geliştirilmiştir. Fakat birçok farklı uygulamada olduğu gibi veri gizleme teknikleri de bilgi güvenliğinin sağlanması için mükemmel değildir. Gizliliğin öneminin arttığı uygulamalarda gizli bilgilerin, üçüncü kişilerin eline geçmeden ilgili hedefe ulaştırılması amaçlanır. Temeli çok eski çağlara dayanan gizli haber-

leşme, teknolojinin gelişimi ile birlikte şekil ve yöntem açısından değişikliklere uğrasa da önemini devamlı olarak korumuştur.

Steganografi uygulamalarında taşıyıcı dosyalar, içerdikleri gizli verilerin kaybolması/bozulması amacıyla kesme, kayıplı sıkıştırma, son bitlerin değiştirilmesi gibi bir takım ataklara maruz kalırlar (üçüncü kişiler tarafından). Bunlardan birisi de geometrik ataklardır. Bunlar, veri gizleme algoritmasının yapısına bağlı olarak gizli verilerin kaybolmasına yol açan saldırılardır. Geometrik atakların birçoğu imgenin sahip olduğu piksellerin yerlerinin de-

ğiştirilmesi esasına dayanır. Bu ise, imgeye ait histogram değerlerinin değişmediğini gösterir. Bu noktalardan hareketle geliştirilen ve bildiri- de sunulan çalışmada gizli verilerin taşıyıcı bir imge içerisine yerleştirilmesi ve veri gizleme algoritmasının geometrik ataklara karşı dayanı- klı (robust) olması hedeflenmektedir.

Bildiri bölümleri kısaca şöyle organize edil- miştir: Bölüm 2’de çalışmanın önemine ve başlatılma sebeplerine değinilmektedir. Bölüm 3’te sayısal imge kavramı kısaca açıklanarak, gizli veri gömme işlemi için önerilen algorit- ma ve akış şemaları verilmektedir. Ayrıca bu bölümde, gerçekleştirilen uygulamanın olumlu ve olumsuz yanları da vurgulanmaktadır. Son bölümde ise bildiri sonuçları ve genel bir de- ğerlendirme sunulmaktadır.

## 2. Geliştirilen Steganografi Yönteminin Temelleri ve Önemi

Günümüzdeki bilindiği şekli ile veri gömmeye ilişkin ilk uygulama geçtiğimiz yüzyılın ortala- rında bir şirketinin yapmış olduğu müzik kayıtlarına sahiplik bilgisi içeren kodun yerleştiril- mesi uygulamasıdır [1].

1990’larda veri gizleme tekniklerinden imge iş- leme üzerine yapılan çalışmalara yoğunlaşılarak; bir çalışmada faks gibi ikili imgelerin korunması kavramı ortaya atılmıştır [2]. 1993 yılında yapı- lan bir çalışmada ise gerçekleştirilen veri göm- me tekniğine; daha sonra “watermark” olarak birleştirilecek olan “water mark” ismi verilmiştir [3]. 1995 yılında bu konuda yapılan çalışmaların sayısı sadece 2 iken, 2001 yılında 376 sayısına ulaşmıştır [4]. Steganografi uygulaması için mutlaka ses, resim, video gibi bir taşıyıcı veri (örtü verisi) gerekmektedir (Şekil 1). Steganog- rafide üçüncü kişilerin steganaliz işlemini yap- maması için, gizli veri (gömü verisinin) gömme algoritmasının ya da yönteminin bilinmemesi ve taşıyıcı dosyada oluşturulan bozukluğun kullanıcılar tarafından fark edilememesi, gizli verilerin güvenliği açısından büyük önem taşır.



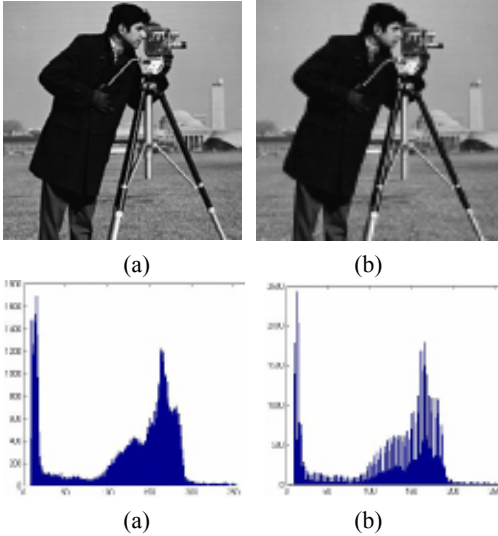
Şekil 1. Veri gizleme yöntemlerinin sınıflandırılması

Kriptoloji bilgi güvenliğini inceleyen ve anlaşılabileni anlayılamaz yapan bir bilim dalıdır. Güvenilirlik, veri bütünlüğü, kimlik doğrulama gibi bilgi güvenliği konularıyla ilgilenen matematiksel yöntemler üzerine geliştirilen yöntem ve tekniklerin tümü kriptolojinin ilgi alanına girmektedir [5].

Modern steganografi yöntemleri, bir veriyi (mesaj) bir nesnenin içine gizli biçimde yerleştirmeyi esas almaktadır. Yani, sadece alıcı, kendisine iletilmek istenen mesajı nesneden (imge, video, ses dosyası vb.) ayırabilmekte ve diğer gözlemcilerin (üçüncü şahısların) o nesnenin içindeki mesajın varlığından haberleri olmamaktadır. Kriptolojinin bir kolu olarak da görülen steganografi, bu özelliğiyle kriptolojiyi bir adım ileri taşımaktadır. Kriptoloji güvenirliliği sağlasa da bir bakıma mesajın gizliliğini sağlayamamaktadır [6].

Çoğu kriptoloji uygulamalarında bilgi, sadece gönderen ve alanın anlayabileceği şekilde şifrelenirken, steganografik uygulamalarda bilgi sadece gönderen ve alanın varlığını bildiği şekilde saklanmakta, bazen de şifrelenip fazladan (kriptografik) koruma sağlanabilmektedir [7]. Bu bilgiden hareketle, kriptoloji uygulamalarında bilginin saklandığı, steganografi uygulamalarında ise bilginin varlığının saklandığı sonucuna varılmaktadır. Literatürde imge içerisine veri gömülmesi temelinde geliştirilmiş birçok uygulama bulunmaktadır. Ve bu uygulamaların neredeyse tamamı İnsan Görme Sistemi (İGS) tarafından algılanamayacak bir değişikliğe sebep olmakta ve böylece bilgi güvenliği sağlan-

maktadır. Ancak İGS tarafından bozulmaların algılanamaz oluşu, imgenin veri taşıma ihtimalini ortadan kaldırmamaktadır. Örneğin, sahip olduğu piksellerin son 2 bitine veri gömülmüş olan bir imgedeki değişiklik İGS tarafından algılanamasa da imgeye ait histogramlar bu durumu tersine çevirmektedir (Şekil 2). Yeni oluşan imgeye ait histogramdaki dengesiz dağılıma sebep olan etken literatürde tarak etkisi (comb effect) olarak anılmaktadır. Bu sonuç, imgede istatistiksel (doğal) olarak bir dengesizliğe işaret etmektedir. Bu durum ise gizli veriyi taşıyan imgeler için önemli bir risk oluşturmaktadır.



Şekil 2. Orijinal imge (a) ve içerisine gizli veri gömülmüş olan imgeye (b) ait ilk (c) ve son (d) histogram görüntüleri

Bu bildiride sunulan yöntem ve uygulama çalışmalarının temel başlatılma sebebi, yukarıda anılan ve Şekil 2’de özetlenen sakıncaların ortadan kaldırılması için bir imgeye ait piksel değerlerine gömülecek olan bilginin histogram üzerinde belirgin bir etki oluşturmamasını ve geometrik ataklardan etkilenmemesini sağlamaktır.

### 3. Sayısal İmgeye Veri Gizleme

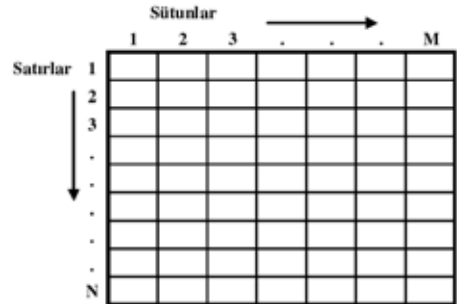
Bu bölümde geliştirilen steganografi yöntemine ve uygulamasına temel oluşturan sayısal imge

kavramı ile ilgili kısa bilgiler verilerek, veri gizleme tekniğinin algoritması açıklanmaktadır. Ayrıca uygulama için geliştirilen yöntemin akış şemaları sunulmaktadır.

#### 3.1. Sayısal İmge

Sayısal (dijital) imgeler, N satır ve M sütunluk bir dizi ile temsil edilir (Şekil 3). Bir imge dizisinin her bir elemanına “piksel” denir. En basit durumda pikseller 0 veya 1 değerini alır ve bu şekilde oluşan resimlere ikili (binary) imge adı verilir. 1 ve 0 değerleri sırasıyla aydınlık ve karanlık bölgeleri ya da nesne ve zemini temsil ederler [8].

Sayısal görüntü dosyaları renkli olarak genellikle 24 bit (Yeşil-Kırmızı-Mavi ana renk değerlerinin her biri için 8’er bit olmak üzere), gri-seviye görüntüler ise 1, 2, 4, 6 ya da 8 bit olabilirler. İmgeler genel olarak bilgiyi görsel bir biçimde saklar ve kullanıcılara gösterilmesini sağlarlar. Bu açıdan resimler ve fotoğraflar imge kapsamında ele alınabileceği gibi, geniş bir bakış açısı ile her türlü iki boyutlu veri imge olarak değerlendirilebilmektedir.



Şekil 3. Sayısal imgenin temel yapısı.



(a) RGB:(38, 176, 70)

(b) RGB:(39, 175, 76)

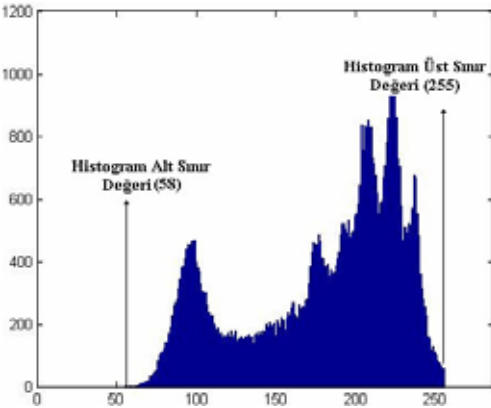
Şekil 4. İçerisine veri gizlenmiş bir pikselin büyültülmüş ilk (a) ve son (b) görüntüleri.

Bir imgeye ait sayısal değerlerdeki farklılıklar ya da bozulmalar İGS tarafından kolaylıkla algılanamaz. İmgeler içerisine gizli veri gömülmesi süreci bu doğal durumdan faydalanılarak gerçekleştirilir (Şekil 4).

### 3.2. Önerilen Steganografi Yöntemine Ait Algoritma, Akış Şemaları ve Uygulama Örnekleri

Veri gizleme işlemi yapan algoritma ile yukarıda da ayrıntılı bir şekilde değinildiği gibi histogram üzerinde İGS tarafından fark edilemeyecek değişiklikler oluşturulması hedeflenmiştir. Bu amaca yönelik olarak her piksel değerine (0-255) ait tekrarlanma sayıları dikkate alınarak veri gizleme işlemi yapılmaktadır.

Önerilen yaklaşımda, öncelikle imgeye ait histogram oluşturularak bu histograma ait sınır değerleri tespit edilmektedir. Böylece veri gizleme işleminin hangi parlaklık değerleri üzerinde yapılacağı belirlenmekte, imgede karşılığı olmayan parlaklık değerleri göz ardı edilmektedir (Şekil 5). Bu sınır değerlerinden hareketle veri gizleme işlemi bir örnek üzerinde aşağıda anlatılmaktadır.



Şekil 5. Bir imge histogramına ait parlaklık değerlerinin alt ve üst sınırlarının belirlenmesi

Gizlenmek istenen ilk 2 bit değeri  $(10)_2$  kabul edilsin. Verilerin gizleneceği imgenin ise Şekil 5'teki gibi bir histograma sahip olduğu, alt sınır değerine ve sonraki birkaç değere ait tekrar-

lanma sayıları Tablo 1'deki gibi kabul edilsin. Uygulama yazılımı öncelikle gömü verisinin (yani  $(10)_2$ ) ilk biti olan 1 değerini ele almaktadır. Histogram bilgileri kullanılarak alt sınır değerinin tekrarlanma sayısının 2 ile bölümünden kalan hesaplanmakta (" $20 \bmod 2 = 0$ ") ve gömü verisi ile uyuşmadığından imge içerisindeki piksellerden parlaklık değeri "58" olan birisi "59" olarak değiştirilmektedir. Böylece "58" parlaklık değerine ait tekrarlanma sayısı "19" olurken, "59"un tekrarlanma sayısı "18"e yükselmektedir. RGB gibi üç kanallı resimlerde bu algoritma her kanal için histogramların hesaplanarak aynı işleme tabi tutulması ile gerçekleştirilmektedir.

Parlaklık Değeri	58	59	60
İmge İçerisindeki Tekrarlanma Sayısı	20	17	13

Tablo 1. İmge histogramına ait bazı sayısal değerler

İlk gizli veri biti imge içerisine gömüldükten sonra histograma ait yeni değerler Tablo 2'deki gibi olacaktır.

Parlaklık Değeri	58	59	60
İmge İçerisindeki Tekrarlanma sayısı	19	18	13

Tablo 2. İmge histogramının 1 değeri gizlendikten sonraki sayısal durumu.

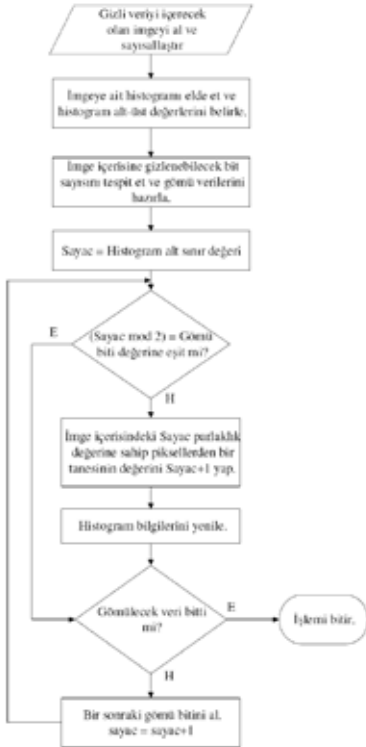
Bu aşamadan sonra, gömülecek olan diğer bit (0 değeri) ele alınarak "59" parlaklık değerinin tekrarlanma sayısının 2'ye bölümünden kalan değer kontrol edilmektedir (" $18 \bmod 2 = 0$ "). Elde edilen değer gömü verisi ile farklılık göstermediğinden herhangi bir işlem yapılmamakta dolayısıyla imgeye ait değerler Tablo 2'de olduğu gibi sabit kalmaktadır.

Histogram üst sınır değerinin "255" olduğu durumlarda, bu değere sahip olan piksellerden bir tanesinin (gömü bitinin değerine bağlı olarak) "256" olması gerekebilmektedir. Ancak her bir renk kanalı sekiz bit ile gösterildiğinden "256" parlaklık değeri geçersiz bir değer olacaktır.

Bu ihtimal göz önünde bulundurularak, önerilen yaklaşımda "255" parlaklık değerine sahip pikseller veri gizlemede kullanılmamaktadır. Gizli verilerin ayırt edilmesi işlemi ise uygulama açısından çok daha kolay gerçekleşmektedir. Öncelikle imgeye ait histogram değerleri elde edilmekte ve histogram sınırları tespit edilmektedir. Bu sınır değerleri dikkate alınarak parlaklık değerlerine ait tekrarlanma sayılarının 2 ile bölümünden kalan, gömü verisi olarak elde edilmektedir. Bu durumda histogram değerlerine ait bilgileri Tablo 2'deki gibi olan bir imgeye,

$$19 \bmod 2 = 1, 18 \bmod 2 = 0, 13 \bmod 2 = 1$$

işlemleri uygulanmakta ve  $(101)_2$  değerinin imge içerisine gizlendiği tespit edilmektedir. Şekil 6 ve Şekil 7'de, geliştirilen veri gizleme yönteminin, sırasıyla gizli veriyi gömme ve gömülü/gizli veriyi elde etme akış şemaları verilmektedir.



Şekil 6. Gizli veri gömme akış şeması.



Şekil 7. Gömülü/gizli veriyi elde etme akış şeması.

Lena, Baboon ve Peppers referans resimleri kullanılarak önerilen algoritmanın uygulanması ile elde edilmiş olan sonuç imgeleri Şekil 8'de verilmektedir. İGS'nin aradaki farkları algılayabilmesi çok zordur. Ancak gizli veri içeren resimlerin histogramlarında tarak etkisi oluşmakta ve parlaklık değerlerine ait frekanslar aşırı düzensizlik göstermektedir.

Şekil 9 gizli veri içeren Lena resminin R, G ve B kanallarına ait histogramlarının ilk ve son durumları hakkında bilgi vermektedir. Diğer veri gömme yaklaşımlarının tersine, histogramların birbirine çok benzer olması sayesinde resim üçüncü kişilerce incelendiğinde gizli veri içerdiğine dair şüphe uyandırmayacaktır.

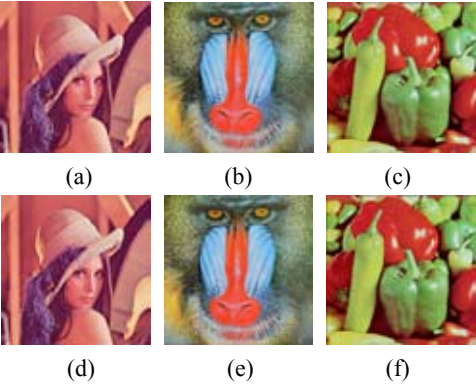
Deneysel sonuçların değerlendirilmesi aşamasında, gizli veri içeren imgelerin istatistiksel kalitelerini ölçmek için Tepe Sinyal Gürültü Oranı (Peak Signal to Noise Ratio - PSNR) kıstası kullanılmıştır. PSNR, orijinal görüntü ile gizli veri içeren görüntü arasındaki benzerlik kalitesini hesaplar. Hesaplama sonucunda PSNR tek bir değer üretir. Bu değer yüksek olması kalitenin de yüksek olduğu (resim üzerinde yapılan işlemin, değişimin algılanabi-

lirlik düzeyine etkisinin az olması) anlamına gelmektedir. Elde edilen sonuçlar benzer bir teknik kullanan [9]'un sonuçları ile Tablo 3'te karşılaştırılmaktadır.

PSNR değerleri ve veri gizleme kapasitesi açısından yeni yaklaşım kullanılarak gerçekleştirilen uygulama, literatürde kabul görmüş birçok yönteme üstünlük sağlayabilmektedir. Tablo 3'te de görüldüğü gibi geliştirilen yöntem, daha fazla sayıda bit imge içerisine yerleştirirken, daha yüksek bir PSNR başarımı da sağlamaktadır.

	Chrysochos ve ark.		Öngörülen algoritma	
	P S N R Değeri	Gömü Verisi	P S N R Değeri	Gömü Verisi
Lena	54,12	360bit	62,75	665bit
Baboon	53,10	300bit	59,25	747bit
Peppers	55,18	300bit	56,01	700bit

**Tablo 3.** Elde edilen sonuçların karşılaştırılması

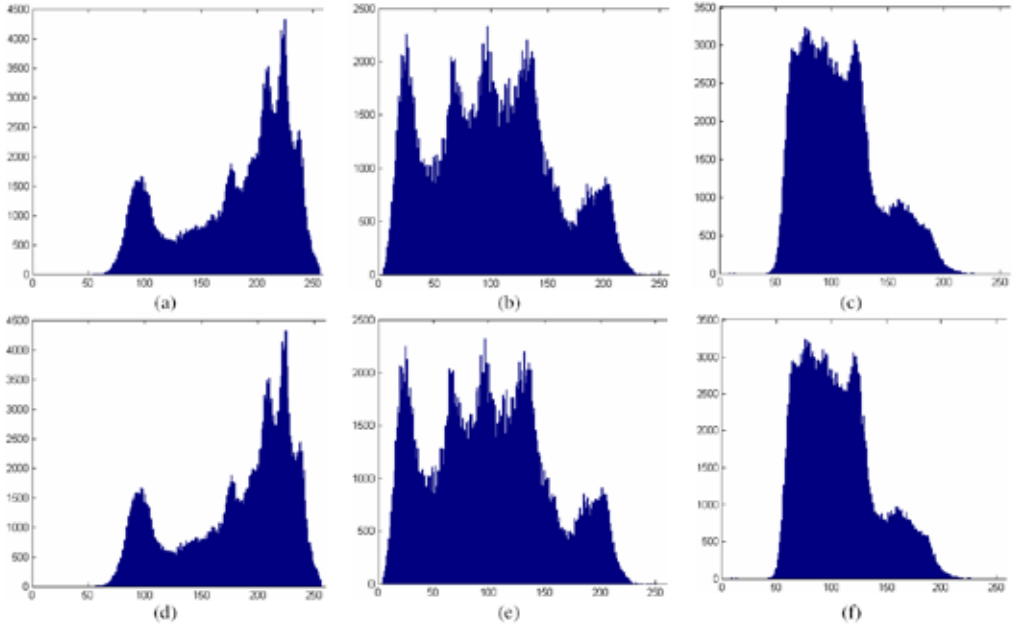


**Şekil 8.** Algoritmanın uygulandığı referans resimlerin ilk (a-b-c) ve son halleri (d-e-f)

### 3.3. Geliştirilen Yöntemin ve Uygulamanın Olumlu ve Olumsuz Yanları

Yapılan çalışmalar ve uygulamalarda geliştirilen yaklaşıma ait önemli özellikler özetle şöyle sıralanabilir:

- Önerilen algoritmanın, uygulandığı sisteme getirdiği işlem yükü açısından eşleniklerine oranla daha iyi bir başarımla gösterdiği tespit edilmiştir.
  - Taşıyıcı imge üzerinde oluşturduğu neredeyse fark edilemez bozulmalar sayesinde veri güvenliğini bir adım ileriye taşımaktadır.
  - Veri gizleme aşaması sonrasında birçok klasik uygulama, histogramı büyük oranda değiştirirken, geliştirilen yaklaşımın histogramda da İGS'nin algılamayacağı kadar küçük değişimlere neden olduğu görülmektedir.
  - Taşıyıcı imgenin eğme, farklı oranlarda görüntüleme ve döndürme ataklarına olan dayanıklılığı sayesinde gizli veriler korunmaktadır (Şekil 10). Zira bu ataklarda piksellerin yerlerinin değişmesine rağmen histogramlarda değişim meydana gelmemektedir. Bu durum histogram temelli veri gizleme yaklaşımlarını ataklara karşı bir adım öne çıkarmaktadır.
- Geliştirilen veri gizleme sisteminin çeşitli olumsuzlukları da bulunmaktadır:
- Kayıplı sıkıştırılmaya maruz kalan taşıyıcı imge içerdiği gizli veriyi kaybetmektedir.
  - Çok düşük bir ihtimalle de olsa veri gizleme algoritmasının ve taşıyıcı dosyanın bilinmesi durumunda üçüncü kişiler tarafından gizli veri elde edilebilmektedir. Bu durumun veri gizleme algoritmasına şifreleme fonksiyonu eklenerek aşılabileceği önerilmektedir.



Şekil 9. Lena resmine ait sırasıyla R, G ve B histogramlarının ilk (a-b-c) ve son (d-e-f) görünüşleri



Şekil 10. Çeşitli geometrik atak örnekleri

#### 4. Sonuç ve Değerlendirmeler

Bu bildiri de bir imge içerisine histogram temelli bir kodlama yöntemi ile veri gömülmesi uygulaması gerçekleştirilmiştir. Geliştirilen yeni yaklaşımın akış şemaları, algoritmaları ve uygulama örneklerinden elde edilen sonuç imgeler ile PSNR değerleri sunulmuştur. Bu çalışmada önerilen yaklaşım, klasik veri gömme uygulamalarından farklı olarak, istatistiksel bir

yaklaşımla elde edilen histogramları kullanmaktadır ve yazılım tabanlı olması nedeniyle birçok eşleniğine nazaran daha yüksek başarımlı (örneğin daha iyi PSNR değerleri için daha yüksek miktarda gizli veri gömme kapasitesi sağlaması), esnek ve maliyeti düşüktür. Geliştirilen uygulamanın bahsi geçen özelliklerinin ileride yapılacak olan çalışmalara önemli bir dayanak olabileceği değerlendirilmektedir.

## 5. Kaynaklar

- [1] Cox, I. J., Miller, M.L., ‘The First 50 Years of Electronic Watermarking’, *Journal of Applied Signal Processing*, 2002, vol. 16, no. 4, pp 126-132.
- [2] Tanaka, K., Nakamura, Y., Matsui, K., ‘Embedding a Secret Information into a Dithered Multi-level Image’, *Proceedings of IEEE Military Communications Conference*, 1990, pp 216-220.
- [3] Hartung, F., Kutter, M., ‘Multimedia Watermarking Techniques’, *Proceedings of the IEEE*, 1999, vol. 87, No. 7, pp 1079-1107.
- [4] Shahreza, M., ‘A New Method for Real-Time Steganography’, *ICSP2006 Proceedings*, 2006.
- [5] Kodar, H., ‘RSA Şifreleme Algoritmasının Uygulanması’, *Akademik Bilişim Konferansları*, Şubat, 2003.
- [6] Yalman, Y., ‘Sayısal Ses İçerisinde Gizli Veri Transferinin Kablosuz Ortamda Gerçekleştirilmesi’, *Yüksek Lisans Tezi*, 2007, Kocaeli Üniversitesi F.B.E.
- [7] Yalman, Y., Ertürk, İ., ‘Sayısal Ses İçerisinde Gizli Metin Transferinin Kablosuz Ortamda Gerçekleştirilmesi’, *UMES’07*, 20-22 Haziran 2007, Kocaeli, pp 41-45.
- [8] Şahin, A., Buluş, E., Sakallı, M.T., ‘24-bit Renkli Resimler Üzerinde En Önemli Bileşen Ekleme Yöntemi Kullanarak Bilgi Gizleme’, *Trakya Üniversitesi J. Sci.*, 2006, pp 17-22.
- [9] Chrysochos E., Fotopoulos V., Skodras A., Xenos M., ‘Reversible Image Watermarking Based on Histogram Modification’, *11th Panhellenic Conference on Informatics with international participation*, vol. B, pp. 93-104, 18-20 May 2007, Patras, Greece.