Düzce Üniversitesi Bilim ve Teknoloji Dergisi

Araştırma Makalesi

Tıbbi DICOM Veri Güvenliğinde Hibrit Yöntemlerin Kullanılması

Duygu BALCI [a,*], Rukiye KARAKIŞ [b], İnan GÜLER [c]

[a] *Bilgi Güvenliği Mühendisliği Bölümü, Fen Bilimleri Enstitüsü, Gazi Üniversitesi, Ankara, TÜRKİYE*
[b] *Yazılım Mühendisliği Bölümü, Teknoloji Fakültesi, Cumhuriyet Üniversitesi, Sivas, TÜRKİYE*
[c] *Elektrik Elektronik Mühendisliği Bölümü, Teknoloji Fakültesi, Gazi Üniversitesi, Ankara, TÜRKİYE*
* *Sorumlu yazarın e-posta adresi:* duygu.balci@gazi.edu.tr
DOI: 10.29130/dubited.583247

ÖZET

DICOM (Digital Imaging and Communications in Medicine – Tıpta Dijital Görüntüleme ve İletişim) tıbbi görüntülerin arşivlenmesi, daha sonradan kullanılması, farklı yerlere dağıtılması ve sunulmasını sağlayan bir dosya standartıdır. Bu standartta dosyalar, dosya başlığı ve görüntü piksellerinden oluşmaktadır. Tıbbi alanda veri güvenliğinin sağlanması için hem dosya başlığında hem de piksellerinde çeşitli güvenlik önlemleri alınması gerekmektedir. Yapılan çalışmada bu güvenlik önlemlerinin alınması için steganografi, kriptografi ve hash özet fonksiyonu bir arada kullanılmıştır. Dosya başlığında yapılan çalışmalar ile hastaya ait demografik bilgilerin güvenliği sağlanırken, pikseller üzerinde yapılan çalışmalarla ise doktor tanısı, hasta demografik bilgileri ve görüntü bütünlüğü sağlanmıştır. Bu çalışmada yapılan analizler PSNR, MSE, SSIM gibi karşılaştırma algoritmaları ile karşılaştırılmış ve geliştirilen yöntemin üstünlükleri belirtilmiştir. Önerilen yöntem ile birlikte hasta tanı ve tedavi süreci minimum düzeyde etkilenmiş ve hasta veri güvenliği sağlanmıştır.

Anahtar Kelimeler: *Tıbbi veri güvenliği, Steganografi, Kriptografi, Hash.*

Use of Hybrid Methods in Medical DICOM Data Security

ABSTRACT

DICOM (Digital Imaging and Communications in Medicine) is a file standard which allows the archiving, subsequent use, distribution and presentation of medical images. In this standard, the files are composed of file headers and image pixels. In order to ensure data security in the medical field, various security measures must be taken in both the file header and pixels. In this study, steganography, cryptography and hash function were used together to obtain these security measures. While the studies carried out in the file headers provided the safety of the patient's demographics information, the studies on the pixels provided a diagnosis of the patients, so ensure that patient demographic information security and image integrity. Analyzes conducted in this study were compared with comparison algorithms such as PSNR, MSE, SSIM and the superiority of the developed method is indicated. The patient diagnostic treatment process with the proposed method was minimally affected, and patient data security was provided.

Keywords: *Medical information security, Steganography, Cryptography, Hash*

I. GİRİŞ

İnsan soyunun gelişmesi ve devam etmesi için olması gereken en önemli etkenlerden birisi, toplumlar arasındaki iletişimin devam etmesidir. Eski çağlarda insanlar, birbirleri ile iletişim kurmak için dumanla haberleşmek ya da mağara duvarlarına çizimler yapmak gibi çeşitli yollar geliştirmiştir. Günümüzde iletişim noktasında en etkin ve yaygın olarak kullanılan yöntem ise internettir. Geliştirilen yeni teknolojilerle, bilgisayar sistemlerinin yaygınlaşması ve bu sistemlerin dünyadaki kullanıcı sayısının artması, internette güvenliğin sağlanmasını oldukça zorlaştırmaktadır. Gerek açık ağlarda gerekse kapalı ağlarda veri güvenliğinin sağlanması oldukça önemlidir. Tıbbi verilerin ağlar arasında paylaşılması, verilerin kopyalanması ya da değiştirilmesi gibi olası saldırıları ortaya çıkartmaktadır. Tıbbi verilerin korunması için çeşitli yazılım ve donanım teknolojileri kullanılmaktadır. Literatürde saldırılara karşı kullanılan en önemli iki yöntem steganografi ve kriptografi olarak belirtilmiştir [1-2].

Bu çalışma, tıbbi DICOM (Digital Imaging and Communications in Medicine - Tıpta Dijital Görüntüleme ve İletişim) görüntüler üzerinde yapılmış ve bu görüntüler üzerinde veri güvenliğinin sağlanması için kriptografi, steganografi ve hash algoritmalarının hibrit bir şekilde kullanılmasını yeni bir yaklaşım olarak önerilmiştir. Çalışmada, DICOM görüntü içerisinde bulunan verilerin güvenliği sağlanırken var olan görüntü üzerinde minimum değişiklik yapılarak tanı ve tedavi sürecinin minimum seviyede etkilemesi sağlanmıştır. Bu çalışmada ilk adım, hastaya ait bilgilerin DICOM görüntü üzerinden alınarak farklı alanda tutulması olmuştur. Elde edilen hasta bilgileri doktor tanısı ile birlikte şifrelenmiştir. Ayrıca, DICOM görüntüsünün değişmediğine dair güvence sağlamak için görüntüye hash özet fonksiyonu uygulanmıştır. Önerilen yöntemde gizlenecek mesaj; hasta demografik bilgilerini, doktorun teşhis raporunu ve görüntüye ait hash özet bilgisini içermektedir. Gömme işlemi için hazır hale getirilen veriler steganografi yöntemi kullanılarak görüntünün içerisine gizlenmektedir. Gömme işlemi beyin manyetik rezonans (MR) görüntülerinde tanı ve tedaviyi etkilememesi için kemik bölgelerine yapılmıştır. Gömme işleminden sonra, hastaya ait verilerin güvenliğinin sağlanması amacı ile DICOM görüntü dosya başlığından hasta demografik bilgileri silinmiştir. Farklı boyutlardaki 50 MR görüntüsü, geliştirilen hibrit sistemde çeşitli karşılaştırma algoritmaları ile karşılaştırılmış ve değerlendirilmiştir. Ayrıca, kriptografi algoritmaları hasta demografik bilgilerinin ve doktor tanısının siber saldırılara karşı direnç kazanmasını sağlarken hash özet bilgisi paylaşılan tıbbi verinin veri bütünlüğünü koruduğunun garantisini vermektedir.

Önerilen metot hasta bilgilerini, tanı ve tedavi sürecini minimum seviyede etkileyerek güvenlik zafiyetlerinden korumaktadır. Kullanılan kriptografi algoritması hasta demografik bilgilerinin ve doktor tanısının olası saldırılara karşı direnç kazanmasını sağlarken hash özet fonksiyonu paylaşılan tıbbi verinin bütünlüğünün korunduğunun garantisini vermektedir.

Bölüm 2'de literatür taraması ve çalışmada kullanılan yöntemlerin anlaşılabilmesi için genel bilgiler aktarılmıştır. Bölüm 3 ve 4' te sırasıyla geliştirilen yöntem ve bulgular sunulmuştur. Son bölümde ise tartışma ve sonuç verilmiştir.

II. LİTERATÜR TARAMASI VE GENEL BİLGİLER

Tıbbi görüntülerin depolanması, iletilmesi ve gerekli durumlarda değiştirilebilmesi için tüm sistemlerin ortak bir dilde konuşması gerekmektedir. Bu gereklilikten doğan ihtiyaç karşısında DICOM (Digital Imaging and Communications in Medicine - Tıpta Dijital Görüntüleme ve İletişim) standardı geliştirilmiştir. Bu sadece bir standart değil aynı zamanda verilerin aktarımı, görüntülenmesi ve depolanmasını sağlayan bir protokoldür. DICOM dosya formatı, dosya başlığı ve görüntüyü oluşturan gri seviye piksel değerlerinden oluşmaktadır [2]. DICOM dosya başlığında, hastaların kişisel bilgileri (ad, soy ad, doğum tarihi, kimlik numarası, adres vb.), seri ve çalışma ile ilgili ayrıntılar, görüntü modalitesi, çekimi yapan radyoloji birimi ve uzman hakkında bilgiler yer almaktadır. Bu çalışmada,

dosya başlığında yer alan hasta kişisel bilgilerinin ve görüntü piksellerinin güvenliğini sağlamak adına görüntü steganografi temelli bir yaklaşım önerilmektedir.

Steganografi, iletilmek istenilen mesajın masum görünümlü içerikte saklanarak karşı tarafa ulaştırılması tekniğidir. Steganografi kelimesi Yunanca steganos-gizli ve graphy-yazı kelimelerin bir araya gelmesi ile ortaya çıkmıştır. İlk steganografik teknik antik Yunanistan'da M.Ö. 440'lı yıllarda Yunan hükümdarı Histaeus tarafından kullanılmıştır. Yunan hükümdarı Histaeus bir kölenin başını tıraş ederek kafa derisi üzerine iletmek istediği mesajı dövme olarak yaptırmıştır. Kölelerin saçlarının uzamasını bekledikten sonra köleleri hedef noktalara göndermiş ve böylelikle istediği mesajları iletmiştir [3].

Steganografi de, genel olarak resim, ses, video, müzik gibi medya dosyaları üzerine yine bu medya dosyaları gizlenir. Steganografi teknikleri insan duyularının eksiklikten yararlanarak verilerin multimedya dosyaları içerisine gizlenmesini sağlamaktadır [4]. Bir steganografi sisteminde, taşıyıcı (kapak) nesne; gizlenecek verinin yerleştirildiği ortamdır. Stego nesne, kapak görüntüsünün gizli veri ile birleşmiş halidir. Gizlenecek veri, saklanacak ya da açığa çıkacak olan verileri temsil etmektedir. Steganaliz ise gizlenmiş olan verilerin ortaya çıkartıldığı süreçtir.

Tıbbi görüntüler üzerinde yapılan steganografi çalışmalarında hasta kişisel verilerinin korunması için farklı güvenlik yöntemleri önerilmiştir. En az ağırlıklı bit (LSB-Least Significant Bit) yöntemi taşınacak dosya üzerine büyük miktarda veri gizlenmesini sağlayan ve uzamsal düzlemde gerçekleştirilen en yaygın steganografi yöntemlerinden birisidir. Yüksek kapasite ve şeffaflık avantajları bulunmaktadır. Ancak, gereklilikleri yerine getirilmezse veri kayıplarına neden olabilir. Bu çalışmanın da konusu olan tıbbi görüntü steganografisinde, görüntülerin yapısı gereği her piksel 8 bitlik değerler içermektedir. LSB yönteminde ilk pikselden son piksele kadar tüm piksel değerleri üzerinde işlem gerçekleştirilebilir. Ancak, sondaki bitlerde işlem yapıldığında insan gözü fark edememekte ön taraftaki bitlere gelindikçe görüntüdeki oluşan bozulmalar fark edilebilmektedir [4-6]. Literatürde LSB ile veri gizleme dışında, dönüşüm uzayında geliştirilen pek çok steganografi yöntemi mevcuttur. Dönüşüm uzayında, tıbbi görüntülerin önce Fourier, Ayrık Dalgacık ya da Ayrık Kosinüs katsayıları elde edilmektedir ve ardından bu katsayıların LSB'leri ile mesajın bitleri yer değiştirilmektedir. Dönüşüm uzayı teknikleri steg saldırı olarak tanımlanan döndürme, kesme, filtreleme gibi işlemlere karşı dayanıklıdır. Ancak bu yöntemlerin kapasite ve işlem performans sınırları mevcuttur.

Uluslararası sağlık standartlarına göre veri gizleme sonrası DICOM görüntülerinde oluşacak bozulmalar bir hastalığın tanı ve teşhisini etkileyebilir. Bu sebeple, literatürde veriler tıbbi DICOM görüntülerinin ilgi olmayan bölgelerine de (RONI-Region of Noninterest) saklanmaktadır [1,7]. İlgi olmayan bölgeler; görüntünün arka planı, sert doku ya da kemik bölgeleri ve hastalığa sebep olmayan sağlıklı dokular olarak tanımlanabilir [7]. Tıbbi görüntü steganografisinde, RONI alanları bir görüntüleme yazılımı üzerinde dikdörtgen gibi bir araç kullanılarak elle ya da çeşitli eşikleme yöntemleri kullanılarak yarı otomatik olarak uzmanlarca seçilmektedir [7]. Otsu eşikleme çalışması ile tıbbi görüntülerden belirlenen RONI alanlarında LSB tekniği ile veri gizlemişlerdir [8]. Yapılan çalışmada dikdörtgen aracı kullanarak eşik değer ile RONI alanlarını belirlemişlerdir [9].

RONI tabanlı tıbbi görüntü steganografisinde, steg saldırılara karşı daha güvenilir olduklarından dönüşüm uzayı teknikleri de kullanılmaktadır. Ravali ve arkadaşlarının yaptığı çalışmada elle seçtikleri RONI'lerin ayrık kosinüs katsayılarını elde etmişler ve burada veri gizlemişlerdir [10]. Shukla ve arkadaşlarının yaptığı çalışmada, tıbbi görüntülerin RONI'lerini elle belirlemişler ve bu alanların ayrık dalgacık (AD) katsayıları ile mesaj bitlerini değiştirmişlerdir [11]. Benzer şekilde, Fatemizadeh ve arkadaşlarının yaptığı çalışmada, gizleme işlemi ile ilgili bilgileri ROI'de, gizli bilgiyi ise yarı otomatik olarak belirledikleri RONI'lerin üçüncü seviye AD katsayılarında saklamışlardır. Ancak, bu yaklaşımların kapasitesi sınırlı olup, elle bölütleme işlemi ile bilgilerin ROI'lerde gizlenmesi gerekmektedir [12].

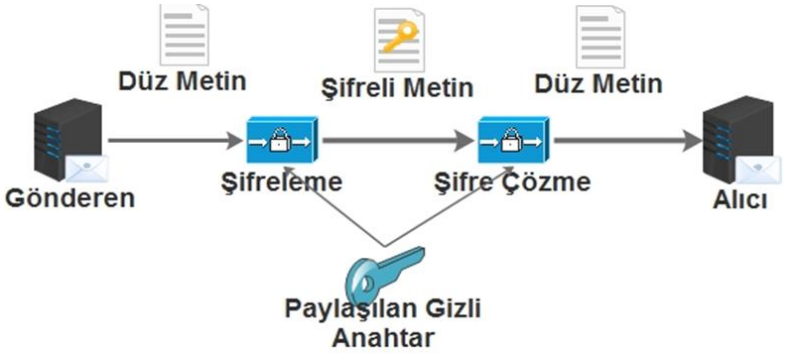
Bu çalışmada, görüntü üzerinde yapılan değişikliklerden dolayı hasta tanı ve tedavi sürecinin olumsuz etkilenmemesi ve veri gizleme sonrası oluşturulan stego tıbbi görüntülerde fark edilebilirliği minimumda tutmak için otomatik belirlenen RONI bölgelerinde uzamsal düzlemde LSB tekniği ile veri

gizleme yapılmıştır. Olası steg saldırılara karşı veriyi gizlemek içinde aşağıda genel bilgileri verilen şifrelemeden faydalanılmıştır.

A. KRİPTOGRAFİ YÖNTEMLERİ

Kriptografi veri iletim ve aktarımında güvenlik gereksinimlerini gidermek için oldukça önemli bir yöntemdir. Sadece hedeflenen alıcının gizli mesajı açıp okuyabilmesine olanak sağlayan, gizlenen mesajların gönderilmesi aşamasıdır. Kriptografi, cep telefonu iletişiminden finansal verilerin iletimine kadar tüm alanlarda kullanılmaktadır. Bilgi güvenliğinin vazgeçilmez üçlüsü olarak bilinen gizlilik, bütünlük ve erişilebilirliği sağlamaktadır. Kriptografide gizli anahtar şifrelemesi, açık anahtar şifrelemesi ve anahtarsız şifreleme olmak üzere üç temel yöntem bulunmaktadır.

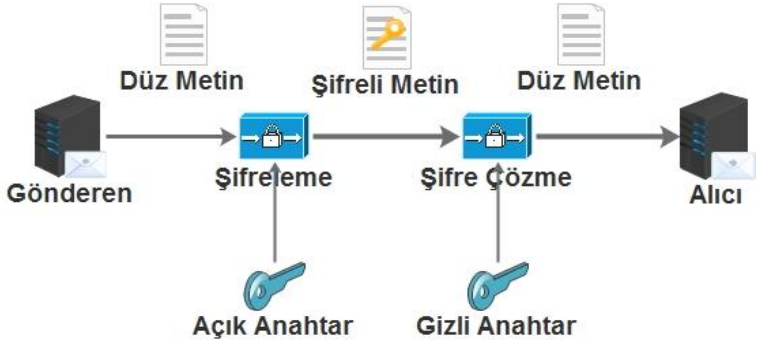
Gizli anahtarlı (simetrik) şifreleme yönteminde Şekil 1' de gösterildiği gibi mesajı gönderen kişi, düz metini şifrelemek için paylaşılan bir gizli anahtar kullanarak mesajın alıcıya gitmesini sağlamaktadır. Alıcı ise şifreli metinin şifresini çözmek için aynı paylaşılan gizli anahtarı kullanmaktadır. Bu sistemdeki temel zorluk ise gönderen ve alıcı arasında anahtar paylaşımının sağlanabilmesidir. Anahtar paylaşımı esnasında farklı kişiler tarafından ele geçirilmesi şifreli mesajın kolayca ulaşılabilir olmasına neden olabilmektedir. Bu yüzden de iletişim esnasında anahtar güvenliği oldukça önemlidir [13-14].



Şekil 1. *Gizli anahtarlı şifreleme algoritması*

Asimetrik şifreleme olarak da bilinen açık anahtarlı şifreleme algoritması Şekil 2'de gösterildiği gibi iki farklı anahtar kullanmaktadır. Bu iki anahtar birlikte üretilmektedir. Açık anahtar verinin gizlenmesinde kullanırken gizli anahtar gizli verinin çözümlenmesinde kullanılmaktadır.

Güvenlik sistemlerinde kullanılan bu yöntemlerden iki anahtarlı asimetrik şifreleme algoritması simetrik şifreleme algoritmasından daha yavaştır. Bunun sebebi ise asimetrik şifreleme algoritmalarında anahtar üretimi sırasında kullanılan asal sayıların üretiminin yavaş yapılabilmesidir.



Şekil 2. *Açık anahtarlı şifreleme algoritması*

Veri bütünlüğünün sağlanması noktasında kullanılan, anahtarsız ve tek yönlü şifreleme algoritması olarak da adlandırılan fakat tam olarak şifreleme algoritması olmayan, gerekli işlemler sonrasında özet

değer üreten hash fonksiyonu bulunmaktadır. Mesajı gönderen kişi hash kodu üretir, mesajı alan kişi de hash kodunu üretir ve bu kodlar karşılaştırılır. Kodlar birbirine uyuşuyorsa veriler üzerinde değişiklik yapılmamıştır. Aksi halde verilerde değişiklik yapıldığı düşünülmelidir [13-15].

Steganografi yöntemlerinin yetersiz kaldığı durumlarda ek önlemler alınması için kriptografi yöntemleri de kullanılmaktadır. Her iki yöntem güvenliğin sağlanması için ayrı ayrı kullanılsa da birlikte kullanımı verilerin güvenliğini artırmaktadır [16].

B. KARŞILAŞTIRMA METOTLARI

Steganografide kapak ve stego görüntü arasındaki benzerliklerin karşılaştırılmasında ortalama kare hatası (MSE-Mean Square Error), tepe sinyal gürültü oranı (PSNR-Peak Signal-to-Noise Ratio) ve yapısal benzerlik endeksi (SSIM-Structural Similarity Index) değerleri kullanılmaktadır. MSE, iki görüntü arasındaki kümülatif kare hatasını gösteren temel bir karşılaştırma yöntemidir. Bu değer düşükse, gömme işleminin kaliteli olduğu ve fark edilme ihtimalinin düşük olduğu anlamına gelmektedir. MSE değeri Eşt.1 kullanılarak hesaplanmaktadır [17-18].

$$MSE = \frac{1}{MN}\sum_{i=0}^{M-1}\sum_{j=0}^{N-1}(f(x_i, y_j) - g(x_i, y_j))^2 \quad (1)$$

Burada f ve g değerleri sırasıyla referans ve test görüntüleridir. M ve N, görüntünün satır ve sütun değerlerini ifade etmektedir. x ve y ise sırası ile referans ve test görüntülerinin aynı piksel numaralarındaki değerlerini temsil etmektedir. PSNR, gömme kalitesini ölçen iki görüntü arasındaki desibel (dB) cinsinden tepe sinyal-görüntü oranıdır. Bu nedenle literatürde yapılan çalışmalarda iyi bir sonuç elde edebilmek için PSNR değerinin 35 dB' den büyük olması gerektiği belirtilmiştir. PSNR değeri, Eşt. 2 ile birlikte MSE değeri kullanılarak hesaplanmaktadır [17-18].

$$PSNR(f, g) = 10\log\left(\frac{(C_{max})^2}{MSE(f,g)}\right) \quad (2)$$

Buradaki *Cmax*, görüntünün maksimum gri seviyesi değerini belirtmektedir. MSE değeri sıfıra yaklaştığında, PSNR değeri sonsuza gitmektedir. Daha yüksek PSNR değeri daha iyi görüntü kalitesini temsil etmektedir. Aksine, daha küçük PSNR değeri, kapak ve stego görüntüleri arasındaki farkın arttığını ve iyi bir gömme işlemi olmadığını belirtmektedir [17-18]. SSIM, iki resim arasındaki benzerliği ölçmektedir. Geleneksel hata karşılaştırma yöntemlerini kullanmak yerine, SSIM değeri, korelasyon kaybı, parlaklık bozulması ve kontrast bozulması olmak üzere üç faktörün bir kombinasyonunu modelleyerek Eşt. 3 ile tasarlanmaktadır.

$$SSIM(f, g) = l(f, g)c(f, g)s(f, g) \quad (3)$$

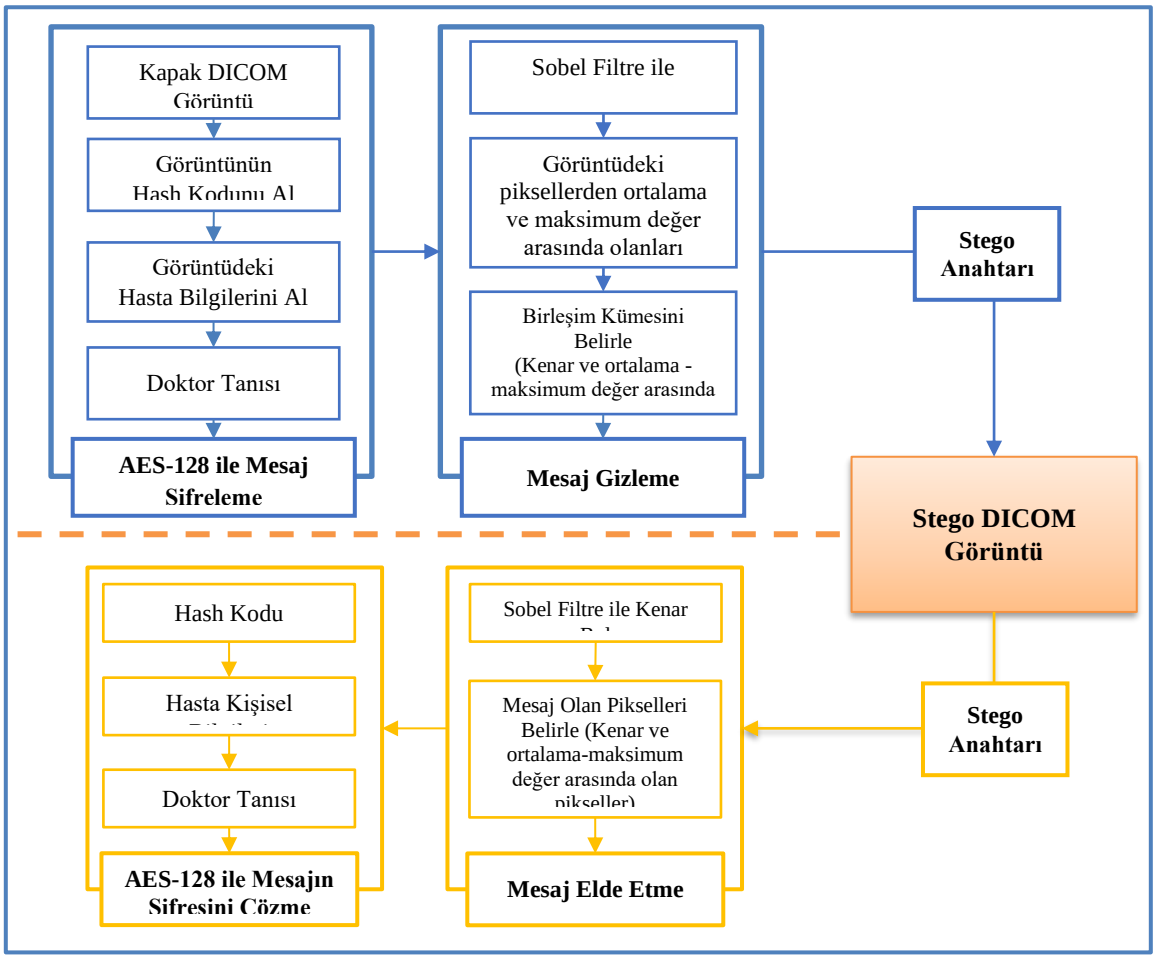
$$\begin{aligned} l(f, g) &= \frac{2\mu_f\mu_g + C_1}{{\mu_f}^2 + {\mu_g}^2 + C_1} \\ c(f, g) &= \frac{2\sigma_f\sigma_g + C_2}{{\sigma_f}^2 + {\sigma_g}^2 + C_2} \\ s(f, g) &= \frac{\sigma_{fg} + C_3}{\sigma_f\sigma g + C_3} \end{aligned} \quad (4)$$

Eşt. 4' teki ilk terim, iki görüntünün (μf ve μg) yaklaşık parlaklığını ölçen parlaklık karşılaştırma işlevidir. Bu faktör sadece iki görüntünün eşit olması durumunda 1'e eşittir. Eşt. 4' teki ikinci terim, iki görüntü arasındaki kontrast yakınlığını hesaplayan kontrast karşılaştırma işlevidir. Kontrast σf ve σg standart sapması ile ölçülür. Eğer $\sigma f = \sigma g$ ise, bu terim 1 olarak maksimum değer alır. Eşt. 4' teki üçüncü terim, iki görüntü arasındaki korelasyon katsayısını ölçen yapı karşılaştırma işlevidir. SSIM endeksi [0, 1] aralığındadır ve Eşt. 3 kullanılarak hesaplanır. İki resim arasında az korelasyon var ise 0'dır. Bu değerin 1 olması yüksek korelasyonun göstergesidir. Eşt. 4' teki pozitif sabitler (C_1, C_2 ve C_3) bölenin sıfır olmasını önlemek için kullanılmıştır [7, 17, 18].

III. ÖNERİLEN METOT

Bu çalışmada, veri güvenliğini arttırmak için veri gizleme ve kriptolojiyi bir arada kullanan hibrit bir yöntem önerilmiştir. Şekil 3' de ayrıntıları verilen yöntemde ilk olarak gizlenecek olan mesaj önişlem aşamasından geçmekte, daha sonra mesaj gömülme aşaması uygulanmakta ve son olarak mesaj deşifre aşaması ile bitirilmektedir. Mesaj önişleme aşamasında, DICOM görüntü dosyasının bir hash özeti oluşturulmaktadır. Bunun için, DICOM görüntü başlığında bulunan, hastaya ait demografik bilgiler, doktor teşhis raporu ile birlikte AES-128 algoritması ile şifrelenerek gömme işleminde kullanılacak veriler haline getirilmiştir. Ayrıca veri bütünlüğünün kontrolü için DICOM görüntünün hash özet bilgisi de gizlenen verilere eklenmiştir.

Veri gizleme aşamasında, görüntünün RONI alanlarını belirlemek için önce Sobel filtre algoritması kullanılarak kapak görüntüdeki sert kemik dokuları elde edilmiştir. Ardından, görüntünün gri seviye piksel değerlerinin ortalaması ve maksimumu hesaplanmıştır. Görüntüdeki yumuşak dokuları ve ilgi alanlarını (beyin) atabilmek için görüntüden seçilen kenarlar ile ortalama ve maksimum değer arasında kalan piksellerin kesişimi alınmıştır. Bu kesişim pikselleri ise veri gizleme için seçilmiş ve piksellerin LSB'leri ile mesajın bitleri sıralı olarak yer değiştirilmiştir. Gizlenecek veriler doktor tanısı, hasta demografik bilgileri ve görüntü hash özet bilgisidir. Ayrıca çalışmada, literatürde RONI seçmede kullanılan istatistiksel yaklaşımlar (ortalama üstü, ortalama altı ve maksimum değer algoritmaları) ile de kıyaslama yapılmıştır. Bu yaklaşımlarda, sırasıyla mesajın uzunluğu kadar görüntünün ortalamasının üstünde ya da altında yer alan pikseller ve maksimum değer taşıyan pikseller seçilerek veri gizleme gerçekleştirilmiştir. Ortalama üstü, ortalama altı ve maksimum değer algoritmaları ile elde edilen sonuçlar hibrit yöntemin bulguları ile karşılaştırılmıştır [19].



Şekil 3. *Geliştirilen yöntemin genel akış diyagramı*

Veri gizleme için Eşt. 5 kullanılmıştır.

$$Gm: K \oplus A \oplus M \rightarrow S \quad (5)$$

G_m: mesaj gizleme işlemini, K: kapak görüntü, A: şifreleme için kullanılan anahtar, M: gizlenecek mesaj, S: stego görüntüyü ifade etmektedir. Veri elde etme aşamasında ise Eşt.6 kullanılmıştır.

$$Em\big(Gm(K, A, M)\big) = M \quad (6)$$

Em: mesaj elde etmeyi ifade etmektedir.

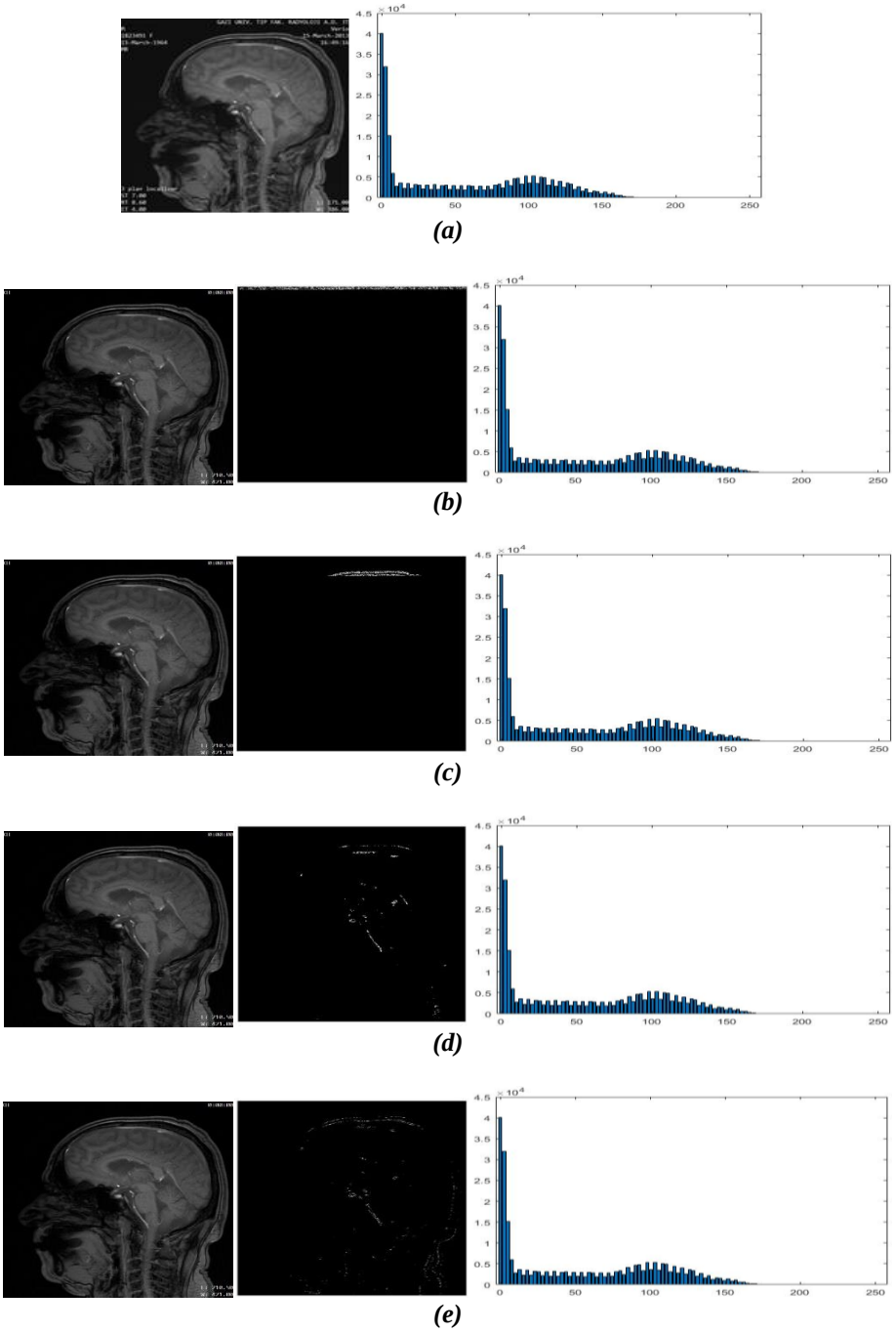
Veri elde etme aşamasında ise stego görüntü ve AES şifrelemeyi çözmek için steg anahtar gerekmektedir. Stego görüntünün önce Sobel filtre ile kenarları bulunmuş ve ardından bu kenarlar ile görüntünün ortalama ve maksimum değerleri arasında kalan piksellerin kesişimi elde edilmiştir. Bu piksellerin LSB'lerinden ise mesaj bitleri sırayla toplanmış, ardından şifreleme geri çözülerek, sırasıyla hash kodu, hasta kişisel bilgileri ve doktor tanısı kullanıcıya gönderilmiştir. Ayrıca, görüntüye ait hash kodu kontrol edilerek görüntünün herhangi bir saldırıya ya da araya girmeye maruz kalıp kalmadığı tespit edilmiştir.

III. BULGULAR

Bu çalışmada, önerilen hibrit yöntem ve karşılaştırma için kullanılan diğer istatistiksel yöntemler epilepsi hastalarına ait 50 farklı MR görüntüleri üzerinde test edilmiştir [19]. Ayrıca, SSIM, PSNR ve MSE karşılaştırma ölçütleri, istatistiksel yöntemlerin ve önerilen hibrit yöntemin sonuçlarının testi için kullanılmıştır.

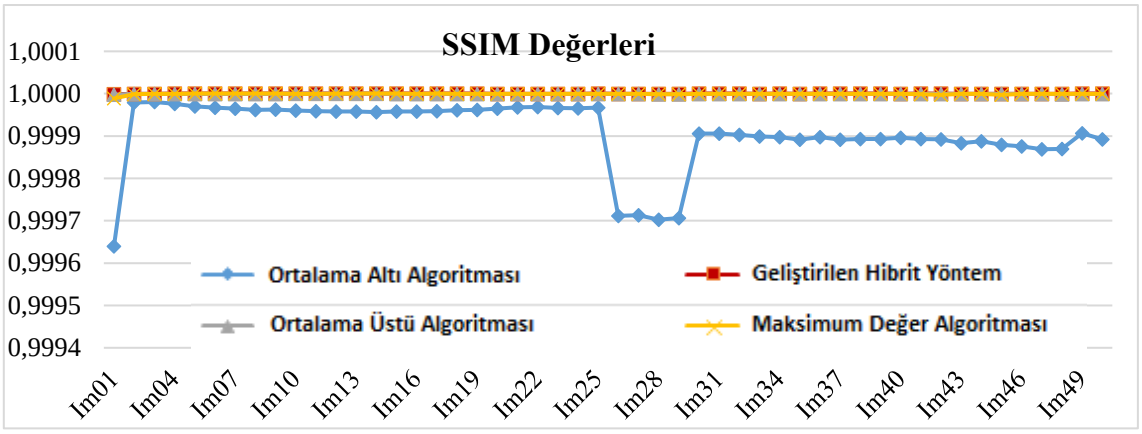
Şekil 4' te önerilen hibrit yöntem ve diğer yöntemlerle veri gizleme sonrasında elde edilen stego görüntüler, fark görüntüler ve histogramları verilmiştir. Yöntemlerin fark görüntülerine göre, ortalama altı algoritması, Şekil 4b' de gösterildiği gibi kapak DICOM görüntünün arka planına gizli mesajı gömdüğü için, görüntü içerisinden fark edilip elde edilme ihtimali oldukça yüksektir. Benzer şekilde, ortalama üstü algoritması, Şekil 4 (c)' de gizli mesajı sırasıyla kafatasın içindeki piksellere gizler. Ayrıca, eğer mesaj kapasitesi çok yüksekse, bu yöntem mesajı gizlemek için beyin piksellerini de kullanabilir. Bununla birlikte, maksimum değer algoritmasında mesajı gömmek için maksimum gri seviye değerine sahip yeterli piksel değeri yoksa mesaj kapasitesi sorunu ortaya çıkmaktadır. Bu çalışmada ise hastalığın tanı ve tedavisini etkilememek için beynin sert dokularına yapılan gömme işlemine odaklanılmıştır.

Şekil 4' te gösterildiği gibi, stego görüntülerinin dosya başlığındaki herhangi bir hasta demografik bilgisi DICOM Viewer ile görüntülenememektedir. Kapağın histogramlarında ve tüm yöntemlerin stego görüntülerinde gözle görülür bir fark bulunmamaktadır.



Şekil 4. *Kapak ve stego görüntüler arasındaki farklar:* ***(a)*** *kapak resmi ve histogramı,* ***(b)*** *ortalama altı algoritmasının stego görüntüsü, fark görüntüsü ve histogramı,* ***(c)*** *ortalama üzeri algoritmasının stego görüntüsü, fark görüntüsü ve histogramı,* ***(d)*** *maksimum değer algoritmasının stego görüntüsü, fark görüntüsü ve histogramı,* ***(e)*** *önerilen hibrit algoritmanın stego görüntüsü, fark görüntüsü ve histogramı.*

SSIM değerleri, Tablo 1' de verilmiştir. Ortalama altı, ortalama üstü, maksimum değer ve geliştirilen hibrit yöntem algoritmalarının SSIM değerlerinin ortalaması sırasıyla 0,99990695, 0,99999971, 0,99999947 ve 0,99999990 olarak bulunmuştur. Ortalama altı algoritmasının minimum SSIM değeri 0,99963965 bulunmuş ve 0,99998034 ± 0,00008053 arasında değişmiştir. Ortalama üstü algoritmasının ortalama SSIM değeri 0,99999774 bulunmuş ve 0,99999997 ± 0,00000039 arasında değişmiştir. Maksimum değer algoritmasının minimum SSIM değerleri 0,99998868 bulunmuş ve 0,99999999 ± 0,00000165 arasında değişmiştir. Geliştirilen hibrit yöntemin minimum SSIM değeri ise 0,99999856 ile 0,99999999 ± 0,00000021 arasında değişmiştir.



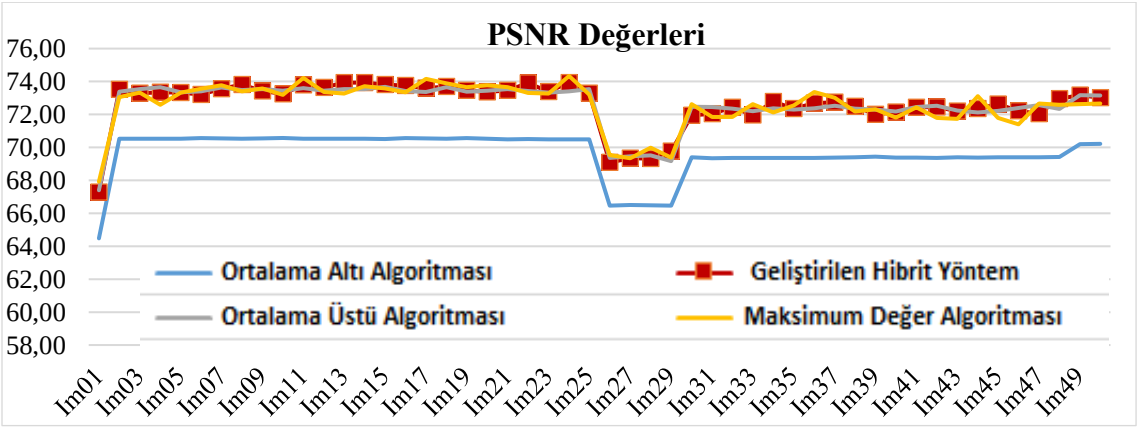
Şekil 5. *Önerilen yöntemin ve diğer istatistiksel yöntemlerin SSIM değerleri*

Tablo 1*. SSIM, PSNR ve MSE Değerleri*

Yöntemler	SSIM			PSNR			MSE		
	Min[a]	Ort[b]	Std[c]	Min[a]	Ort[b]	Std[c]	Min[a]	Ort[b]	Std[c]
Ortalama Altı	0,99963965	0,99990695	0,99998034 ± 0,00008053	64,48	69,64	70,57 ± 1,34	0,00570	0,00755	0,02340 ± 0,00330
Ortalama Üstü	0,99999774	0,99999971	0,99999997 ± 0,00000039	67,92	72,59	74,33 ± 1,35	0,00280	0,00383	0,01190 ± 0,00170
Maksimum Değer	0,99998868	0,99999947	0,99999999 ± 0,00000165	67,40	72,48	73,68 ± 1,36	0,00280	0,00385	0,01060 ± 0,00156
Geliştirilen Hibrit Yöntem	0,99999856	0,99999990	0,99999999 ± 0,00000021	67,29	72,63	73,94 ± 1,41	0,00260	0,00381	0,01220 ± 0,00176

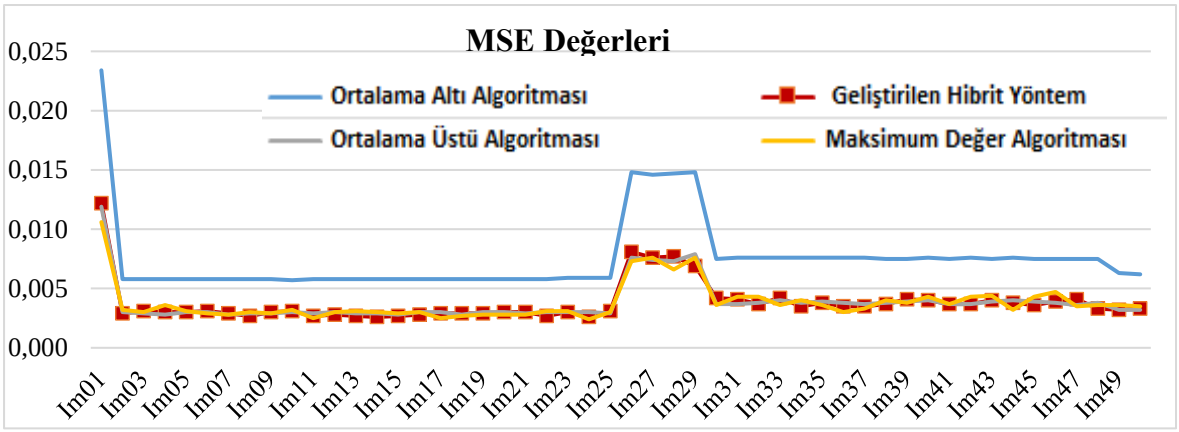
a Min=Minumum, b Mak=Maksimum, c Std=Standart Sapma.

PSNR değerleri, Tablo 1'de verilmiştir. Ortalama altı, ortalama üstü ve geliştirilen hibrit yöntemler için PSNR değerlerinin ortalaması sırasıyla 69,64 dB, 72,59 dB ve 72,63 dB olarak bulunmuştur. Ortalama altı algoritmanın minimum PSNR değerleri 64,48 dB ve 70,57 dB ± 1,34 arasında değişmiştir. Ortalama üstü algoritmasının minimum PSNR değerleri 67,92 dB ve 74,33 dB ± 1,35 arasında değişmiştir. Maksimum algoritmanın minimum PSNR değerleri 67,40 dB ve 73,68 dB ± 1,36 arasında değişmiştir. Geliştirilen hibrit yöntemin minimum PSNR değerleri 67,29 dB ve 73,94 dB ± 1,41 arasında değişmiştir. Elde edilen sonuçlara göre, önerilen yöntem en yüksek PSNR değerlerine ulaşırken ortalama altı algoritması da en kötü PSNR değerlerine ulaşmıştır [19].



Şekil 6. *Önerilen yöntem ve diğer istatistiksel yöntemlerin PSNR değerlerinin karşılaştırılması*

MSE değerleri Tablo 1'de gösterilmiştir. Ortalama altı, ortalama üstü ve geliştirilen hibrit yöntemlerin MSE değerlerinin ortalaması sırasıyla 0,00755, 0,00383 ve 0,00381 olarak bulunmuştur. Ortalama altı algoritmasının minimum MSE değerleri 0,00570 ve değerler 0,02340 ± 0,00330 arasında değişmektedir. Ortalama üstü algoritmasının minimum MSE değerleri 0,00280 ve değerler 0,01190 ± 0,00170 arasında değişmiştir. Maksimum algoritmanın minimum MSE değerleri 0,00240 ve değerler 0,01060 ± 0,00156 arasında değişmiştir. Geliştirilen hibrit yöntemin ortalama MSE değerleri 0,00260 ve değerler 0,01220 ± 0,00176 arasında değişmiştir [19].



Şekil 7. *Dört farklı algoritma için MSE değerlerinin karşılaştırılması*

Karşılaştırma sonuçlarına göre, önerilen yöntem yüksek PSNR ve SSIM değerlerine sahipken düşük MSE değerlerine sahiptir. Ayrıca, tanı ve tedaviyi etkilememesi için görüntüde ilgi alanı olmayan bölgelerin belirlenmesi ve ilgi alanı olan bölgelerden gizleme noktasında uzak durulması gerektiği belirlenmiştir. Güvenliği artırmak için, gömme mesajı AES-128 algoritması tarafından şifrelenmiş ve tıbbi görüntünün hash özeti saldırılara karşı bütünlüğün sağlanması için kullanılmıştır. Bu nedenle, önerilen hibrit yöntem, elde edilen sonuçlara göre tıbbi steganografide kullanılabilir [19].

IV. SONUÇLAR

DICOM standardı gereği görüntüler içerisinde hastaya ait önemli kişisel bilgiler bulunmaktadır ve bunlar Internet üzerinden kolaylıkla elde edilebilen herhangi bir DICOM gösterici tarafından okunabilmektedir. Bu çalışmada, steganografi ve kriptoloji kullanılarak tıbbi görüntülerde bilgi güvenliğinin sağlanması amaçlanmıştır. Gizlenecek mesajın gömülmesi için görüntüdeki kemik noktaları belirlenmiştir. Bu mesaj görüntü hash özeti, hasta demografik bilgileri ve doktor teşhisinden oluşmaktadır. Doktor teşhis raporu ve hasta demografik bilgileri AES-128 algoritması şifrelenmiştir. Bu şifreleme steganaliz ile mesajın kolaylıkla elde edilmesini engellemek için veri güvenliğini sağlamaktadır. Aynı zamanda görüntünün hash özeti üretilmiş ve gömülecek veriler arasına eklenmiştir. Bu hash özeti ise veri bütünlüğü olduğunu kanıtlamaktadır. Önerilen yöntemde, şifrelenen veriler için görüntüdeki ilgi olmayan bölgeler analiz edilmekte ve yüksek oranlarda kemiklere gömme işleminin gerçekleşmesi sağlanmaktadır. Böylece DICOM görüntüde tanı ve teşhisini etkileyecek bir bozulmanın ilgi bölgesi olan beyinde gerçekleşmemesi sağlanmaktadır. Gömülecek veri boyutuna hash özetinin de eklenmesinden dolayı doktor teşhis raporu belirli uzunluklarda alınılabilmektedir.

Gelecekte, tıbbi veri güvenliği alanında yapılacak olan çalışmalarda her doktorun parmak izinin olduğu bir havuz oluşturulabilir. Herhangi bir hasta, sadece kendi belirlediği doktorların MR görüntülerini incelemesini isterse doktorlara ait parmak izlerinin hash özetleri DICOM görüntüye gömülebilir. Bu sayede, MR görüntülerinin yetkisiz doktorlar ya da kişiler tarafından görülmesi önlenmiş olacaktır.

V. KAYNAKLAR

[1] A. Cheddad, J. Condell, K. Curran, P. Mc Kevitt, "Digital image steganography: Survey and analysis of current methods," *Signal Processing*, vol. 90, pp.727-752, 2010.

[2] O.S. Pianykh, "A brief history of dicom," in *Digital Imaging and Communications in Medicine (DICOM)*, Germany: Springer-Verlag Berlin and Heidelberg GmbH & Co. K, 2008, pp. 17-25.

[3] A. Siper, R. Farley, C. Lombardo, "The rise of steganography", in *Proceedings of Student/Faculty Research Day*, New York: CSIS Pace University, 2005, pp. D1.1-D1.7.

[4] R. Gawande, S. Gawande, "A review on steganography methods," *International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering*, vol. 2, no 10, pp. 4635-4638, 2013.

[5] P. Mortazavian, M. Jahangiri, E. Fatemizadeh, "A low-degradation steganography model for data hiding in medical images," in *Proceeding of the Fourth IASTED International Conference Visualization, Imaging, and Image Processing*, 2004, pp. 914-920.

[6] R. Karakış, İ. Güler, "Medikal dicom görüntüler için steganografi uygulaması," 7. Uluslararası Bilgi Güvenliği ve Kriptoloji Konferansı-ISCTurkey, İstanbul, Türkiye, 2014, ss. 340-344.

[7] R. Karakis, İ. Guler, "Steganography and medical data security," in *Cryptographic and Information Security Approaches for Images and Videos*, 2019, ch. 22, pp. 627-660.

[8] N.A. Memon, S.A.M. Gilani, "Watermarking of chest CT scan medical images for content authentication," *International Journal of Computer Mathematics*, vol. 88, no. 2, pp. 265-280, 2011.

[9] H. Al-Dmour, A. Al-Ani, "Quality optimized medical image steganography based on edge detection and hamming code," in *2015 IEEE 12th International Symposium on Biomedical Imaging (ISBI)*, 2015, pp. 1486-1489.

[10] K. Ravali, A.P. Kumar, S. Asadi, "Carrying digital watermarking for medical images using mobile devices," *IJCSET*, vol. 1, no. 7, pp. 366-369, 2011.

[11] A. Shukla, C. Singh, "Medical image authentication through watermarking," *International Journal of Advanced Research in Computer Science & Technology (IJARCST 2014)*, vol. 2, no. 2, pp. 292-295, 2014.

[12] E. Fatemizadeh, M. Maneshi, "A new watermarking algorithm based on human visual system for content integrity verification of region of interest," *Computing and Informatics*, vol. 31, pp. 877-899, 2012.

[13] K. Atul, *A Model For Network Security, Cryptography And Network Security Principles And Practices*, 4th ed., New York, USA: Tata McGraw-Hill Companies, 2003, pp. 28-62.

[14] N. Smart, "Public key encryption and signatures, cryptography: An introduction" in *Cryptography: An Introduction*, 3rd ed., University of Bristol, 2015, pp. 165-436.

[15] D. Balcı, R. Karakış, İ. Güler, "Hibrit yöntemlerle medikal görüntülerin güvenliğinin sağlanması üzerine araştırma," in *International Congress on Engineering and Architecture*, Alanya, Türkiye, 2018, ss. 869-877.

[16] P. Kaur, S. Dhiman, K. Kaur, "A methodology on cryptography and stegnography applicant to mobile adhoc network & wireless sensor network," *International Journal of Data & Network Security*, pp. 47-54, 2013.

[17] A. Horé, D. Ziou, "Image quality metrics: PSNR vs. SSIM," in *International Conference on Pattern Recognition*, 2010, pp. 2366-2369.

[18] R. Karakis, İ. Güler, İ. Çapraz, E. Bilir, "A novel fuzzy logic-based image steganography method to ensure medical data security," *Computers in Biology and Medicine*, vol. 67(C), pp. 172-183, 2015.

[19] D. Balcı, "Hibrid yöntemler kullanılarak tıbbi dicom verilerinin güvenliğinin sağlanması," Yüksek Lisans tezi, Bilgi Güvenliği Mühendisliği Bölümü, Gazi Üniversitesi, Ankara, Türkiye, 2019.