Veri Gizleme ile Medikal Veri Güvenliği

Rukiye KARAKIŞ[1], Kali GURKAHRAMAN[2]

[1] Cumhuriyet Üniversitesi, Yazılım Mühendisliği Bölümü, Sivas

[2] Cumhuriyet Üniversitesi, Bilgisayar Mühendisliği Bölümü, Sivas

{rkarakis,kgurkahraman}@cumhuriyet.edu.tr

1. ÖZET

Medikal verilerin açık ağlarda saldırılarla ele geçirilmesi hastaların tanı veya tedavilerinin değiştirilmesine sebep olabilir. Bu sebeple medikal görüntülerin saklanması ve dağıtılması için kullanılan DICOM dosya formatının başlık kısmında yer alan hasta kişisel bilgilerinin de korunması gereklidir. Bu çalışmada epilepsi hastalarına ait kişisel bilgiler ve biyolojik sinyal bilgileri DNA tabanlı şifreleme algoritması ile şifrelenmiş ve bölütlenen görüntünün ilgi olmayan bölgelerine gizlenmiştir. Geliştirilen sistem hem hasta bilgilerinin güvenliğini sağlamaktadır hem de uzman hekimlere farklı biyolojik sinyalleri tek bir ortam üzerinde değerlendirme fırsatı sağlamaktadır.

2. DICOM Görüntü

DICOM (Digital Imaging and Communications in Medicine) medikal görüntülerin elde tutulması, kayıt edilmesi, yazdırılması ve iletilmesini sağlar. Dosya başlık kısmında hastaya ait kişisel bilgiler (ad, soyad, yaş, ağırlık, medikal özgeçmiş gibi), kurum, cihaz ve görüntü bilgilerini içerir. DICOM görüntülerin arşivlenmesi ve iletilmesi aşamalarında hastaya ait kişisel verilerin güvenliği sağlanmalıdır.

3. Medikal Veri Gizleme

Medikal veriler Internet ve açık ağlarda tehdit altındadır. Medikal verilerin ele geçirilmesi veya değiştirilmesi hem hasta haklarının ihlal edilmesine hem de hastaların hayatlarının tehlike girmesine sebep olabilir. Medikal veri güvenliği: güvenlik duvarı, sanal özel ağlar (VPN-virtual private networks) ve kriptografik yöntemler (simetrik, asimetrik ya da özet şifreleme) ile gerçekleştirilmektedir. Son yıllarda medikal görüntülerin (X-ray, MR, CT, PET, Ultrasound, Angiogram vb.) yada biyolojik sinyallerin (EEG, EKG, EMG vb.) içerisinde hasta kişisel bilgilerinin güvenliğinin sağlanması üzerine çalışılmaktadır. Medikal veri gizleme çalışmaları üç alanda değerlendirilebilir.

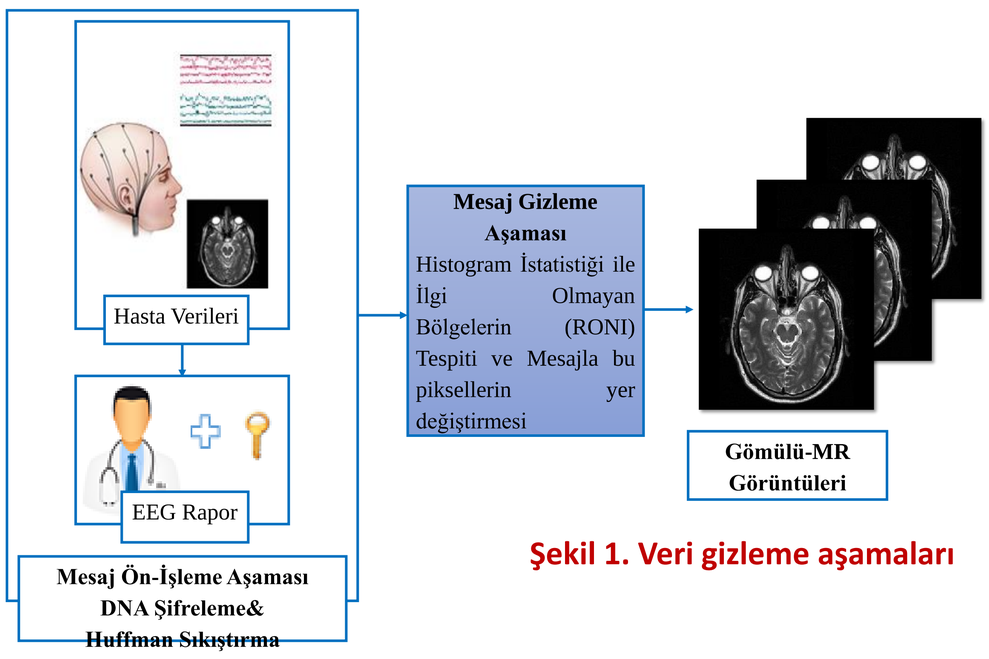
LSB Tabanlı Steganografi Yöntemleri (Uzamsal Düzlem) → **RONI Tabanlı Steganografi Yöntemleri (Uzamsal + Dönüşüm Düzlemleri)** → **Geri Elde Edilebilir (Reversible) Steganografi Yöntemleri (Uzamsal + Dönüşüm Düzlemleri)**

4. Materyal ve Metot

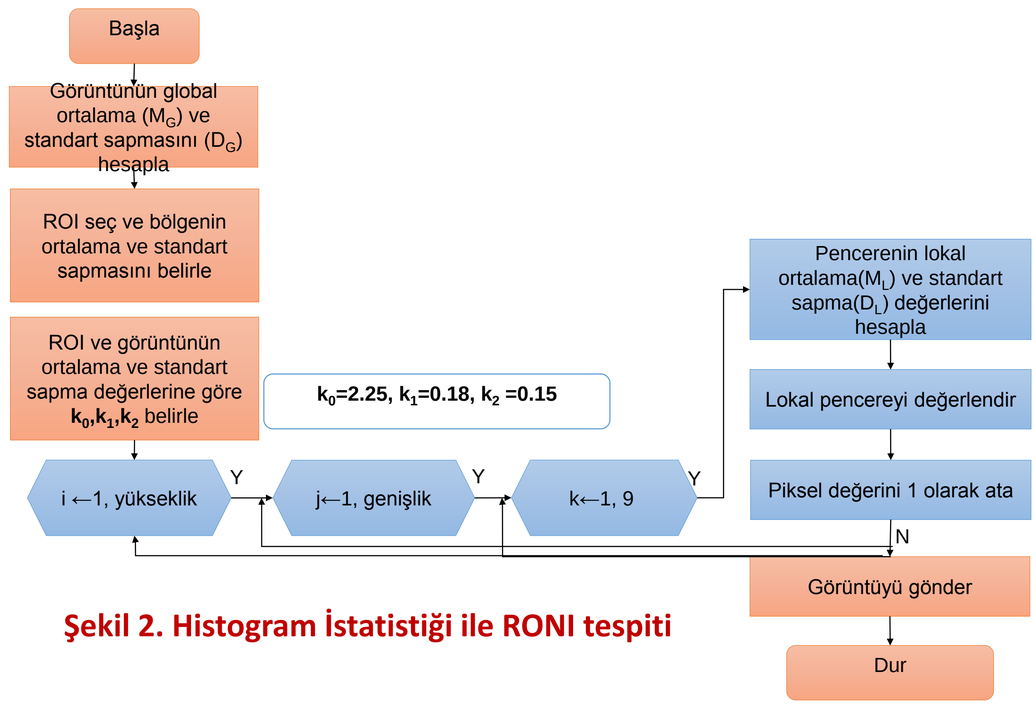
Veri seti: Cumhuriyet Üniversitesi Tıp Fakültesi Nöroloji Bölümü'ne başvuran epilepsi hastasına ait 27 MR görüntüleri ve epileptik EEG verisi,

Mesaj gizlemek için: Epilepsi hastasına ait farklı boyutlardaki MR görüntüleri (16 bit)

Gizlenecek mesaj: MR görüntülerinde yer alan hasta kişisel bilgileri, EEG raporu yorumu, bölütlenen EEG ve EEG dosyasına ait dosya başlık bilgileri.

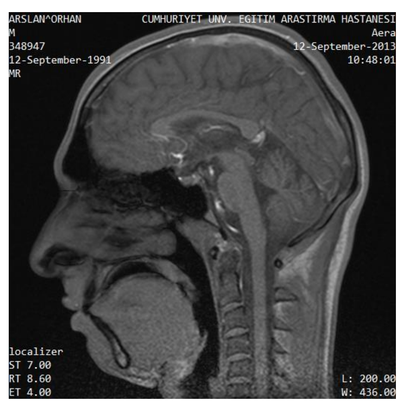


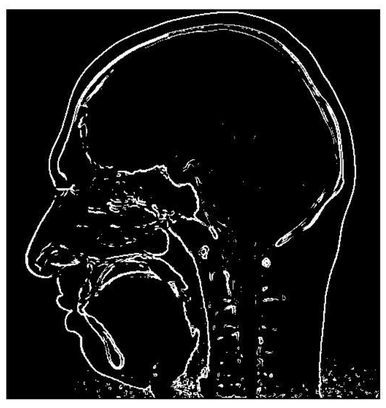
Şekil 1. Veri gizleme aşamaları

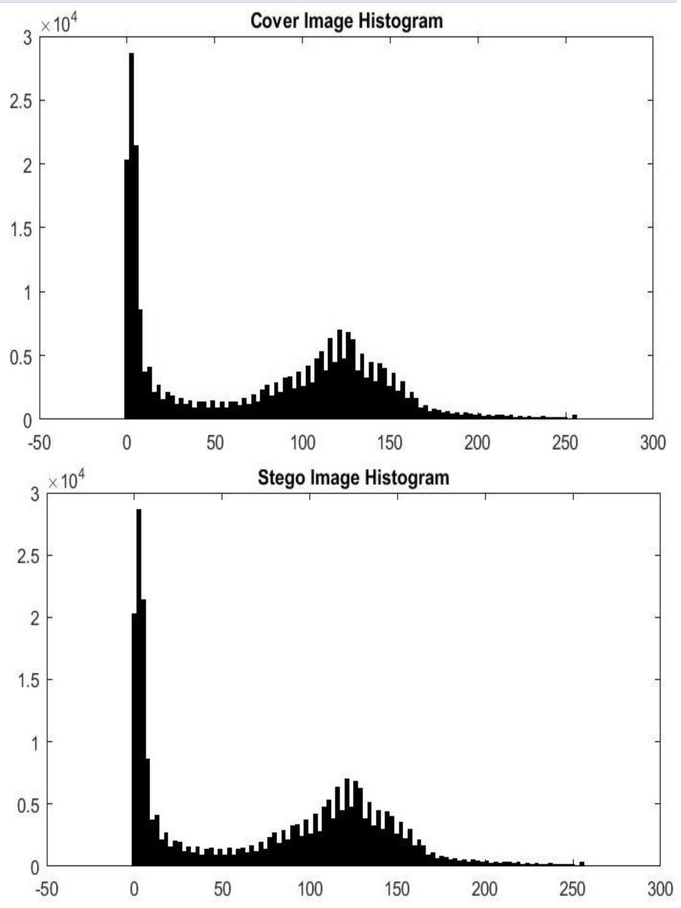


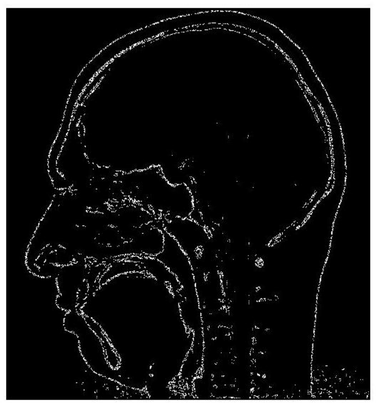
Şekil 2. Histogram İstatistiği ile RONI tespiti

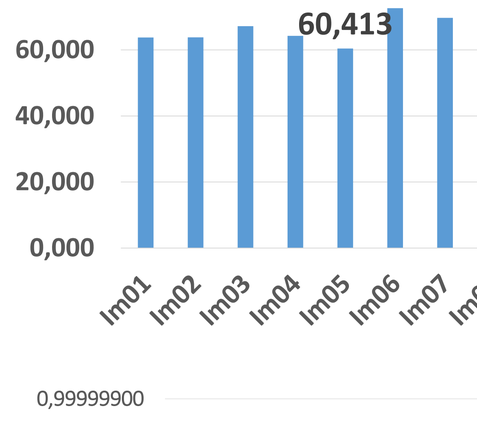
5. Elde Edilen Sonuçlar







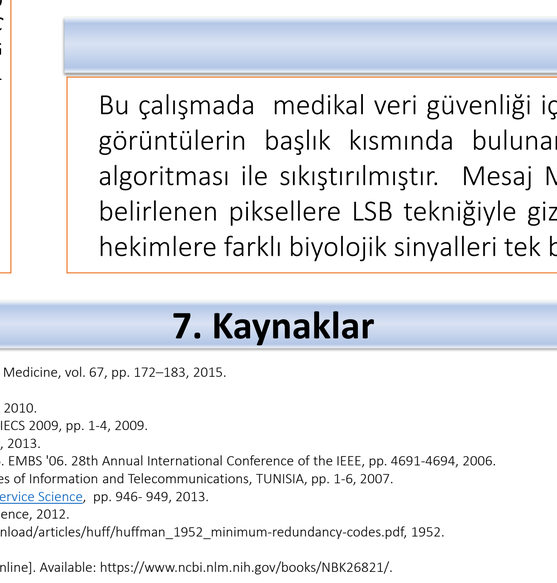




Şifreli Mesaj: *TCTCAATGAC*
Tek Kullanımlık (OTP) anahtarı:
TATGAGTTTGCCGAGACCTCGTCGATCTCT. …
Şifresi Çözülen Mesaj: 01…
Şifreli Mesajın 1. değeri: *T*
OTP anahtarın 1. değeri: *T*
Çözülen Mesajın İkilik Değeri: 0
Şifreli Mesajın 2. verisi : *C*
OTP anahtarın 2. değeri : G
Çözülen Mesajın İkilik Değeri : 1

4.1. DNA Şifreleme ve Şifre Çözme

Metin: *ZOO*
Metnin ASCII koda dönüşmesi:
ZOO: 90 79 79: 01111010 01101111 01101111
DNA Şifreleme:
Adenine (A) =00. Thymine (T)=01.
Cytosine (C)=10. Guanine (G)=11
TCGGTGCCTGCC- İkili Veri
01010100 01000011 01000111 01000111 01010100 01000111
Tek Kullanımlık (OTP) anahtarı:
TATGAGTTTGCCGAGACCTCGTCGATCTCT. …
DNA Hibritleşme:
- İkili verinin ilk biti: 0
OTP anahtarının ilk değeri: T
Şifreli Mesaj: T
- İkili verinin 2. biti : 1
OTP anahtarının 2.değeri: G
Şifreli Mesaj: C



6. Tartışma

Bu çalışmada medikal veri güvenliği için DNA şifreleme ile epilepsi hastasına ait epileptik EEG, EEG raporu ve DICOM görüntülerin başlık kısmında bulunan kişisel bilgiler önce şifrelenmiş ve ardından Huffman kayıpsız sıkıştırma algoritması ile sıkıştırılmıştır. Mesaj MR görüntülerin ilgi olmayan alanlarına histogram tabanlı istatistik yöntemi ile belirlenen piksellere LSB tekniğiyle gizlenmiştir. Geliştirilen sistem hasta bilgilerinin güvenliğini sağlamıştır ve uzman hekimlere farklı biyolojik sinyalleri tek bir ortam üzerinde değerlendirme fırsatı sunmuştur.

7. Kaynaklar

1. R. Karakış, R., 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, pp. 172–183, 2015.
2. M. Haidekker, "Image Storage, Transport, and Compression", Wiley-IEEE Press, Edition: 1, pp. 386-412, 2011.
3. A. Cheddad, J. Condell, K. Curran, P. McKevitt, "Digital image steganography: Survey and analysis of current methods". Signal Processing, vol. 90, pp. 727–752, 2010.
4. L.-Q. Kuang, Y. Zhang, X. Han, "Watermarking Image Authentication in Hospital Information System", Information Engineering and Computer Science, 2009. ICIECS 2009, pp. 1-4, 2009.
5. H. Nyeem, W. Wageeh Boles, C. Colin Boyd, "A Review of Medical Image Watermarking Requirements for Teleradiology", J. Digit. Imaging, vol. 26, pp. 326-343, 2013.
6. G. Coatrieux, L. Lecornu, B. Sankur, C. Roux, "A Review of Image Watermarking Applications in Healthcare, Engineering in Medicine and Biology Society", 2006. EMBS '06. 28th Annual International Conference of the IEEE, pp. 4691-4694, 2006.
7. K. A. Navas, M. Sasikumar, "Survey of Medical Image Watermarking Algorithms", SETIT 2007 4rth International Conference: Sciences of Electronic, Technologies of Information and Telecommunications, TUNISIA, pp. 1-6, 2007.
8. Z. Wang, X. Zhao, H. Wang, G. Cui, "Information hiding based on DNA steganography", 2013 IEEE 4th International Conference on Software Engineering and Service Science, pp. 946- 949, 2013.
9. A.P. Thiruthuvadoss, "Comparison and Performance Evaluation of Modern Cryptography and DNA Cryptography", Royal Institute of Technology, Masters of Science, 2012.
10. Huffman, D., "A Method for the Construction of Minimum-Redundancy Codes, Proceedings of the IRE, vol. 40 (9), pp. 1098–1101, http://compression.ru/download/articles/huff/huffman_1952_minimum-redundancy-codes.pdf, 1952.
11. Huffman Coding. [0nline]. Available: http://en.wikipedia.org/wiki/Huffman_coding.
12. B. Alberts, A. Johnson, J. Lewis and et al. "The Structure and Function of DNA", Molecular Biology of the Cell. 4th edition. New York: Garland Science, 2002 [Online]. Available: https://www.ncbi.nlm.nih.gov/books/NBK26821/.