Medikal Görüntülerde Doktor-Hasta Bilgi Gizliliğinin Sağlanması

Vedat Bayraklı[1], Erdal Güvenoğlu[2]
[1,2]Maltepe Üniversitesi, Bilgisayar Mühendisliği Bölümü, İstanbul
vedatbayrakli@hotmail.com, erdalg@maltepe.edu.tr

Özet: Günümüz teknolojisindeki gelişmeler, gizli tutulması gereken bilgilerin farklı kaynaklar arasında paylaşılması sırasında, bilgi kaynağı sahipleri için ciddi sorunlar oluşturmaktadır. Özellikle doktor ve hasta mahremiyetinin farklı yasalar korunduğu düşünüldüğünde veri gizliliğinin önemi daha iyi anlaşılmaktadır. Bu çalışmada, doktorun hasta hakkında yapmış olduğu teşhis ve tetkiklerin üçüncü şahıslardan gizlenmesini ayrıca doktorlar arasında bilgi alışverişinin güvenli yapılmasını sağlayan bir sistem önerilmiştir.

Anahtar Sözcükler: Steganografi, Medikal görüntüler, Hasta Hakları

Ensuring the Confidentiality of Medical Image Doctor-Patient Information

Abstract: The advancements in today's technology, while being shared among different sources of information to be kept secret, are causing serious problems for the people owing the source of information. The importance of the confidentiality of the date can be understood better especially when considering that doctor and patient privacy is being protected by different laws. In this study a system is recommended to keep diagnosis and investigations made by the doctor hidden from the third person and also to enable the secure exchange of the information among the doctors.

Keywords: Steganografi, Medical images, Patients' Rights

1. Giriş

Bilgisayar ve elektronik dünyasındaki gelişmeler, gizli tutulması gereken bilgilerin bir kaynaktan başka bir kaynağa aktarılması sırasında, bilgi kaynağı sahipleri için ciddi sorunlar oluşturmaktadır. Bilgi iletimi için ise genel kullanıma açık ortamlar yaygın olarak kullanılmaktadır. Bu ortamlarda bilgi güvenliği büyük önem taşıdığından, bilgi gizleme ve iletimi üzerinde yapılan çalışmalar da yoğun bir talep ve ilgi görmektedir.

Bilgi güvenliğinin sağlanması gereken en önemli durumlardan biri de doktor ve hasta arasındaki gizliliktir. Doktor, kendi vicdanına ve hastanın yararına hareket ederken, aynı zamanda hastanın özerkliğini ve haklarını da garanti etmelidir [1]. Dünya Tabipler Birliği, bu düşüncesinden hareketle, 1981'de ilk kez Lizbon Hasta Hakları Bildirgesi'ni yayımlamıştır. Bu metinde "Hasta, kendisiyle ilgili tüm tıbbi ve kişisel bilgilerin gizliliğine gereken saygıyı göstermesini hekiminden bekleme hakkına sahiptir" cümleleriyle karşımıza çıkan gizlilik hakkı, 1995 tarihli Bali Hasta Hakları Bildirgesi'nde daha da genişletilmiştir [2]. Bali Hasta Hakları Bildirgesi'nde hastanın gizlilik hakkı ile ilgili yayınlamış olduğu maddeler aşağıda verilmiştir [3].

- Hastanın sağlık durumu, tıbbi durumu, tanısı, tedavisi ve kişiye özel diğer tüm bilgiler ölümden sonra bile gizli olarak korunmalıdır. İstisna olarak hasta yakınlarının kendileri ilgili sağlık risklerini öğrenmeleri açısından bu bilgilere ulaşabilme hakkı olabilir.

Gizli bilgiler sadece hastanın açık izni veya mahkemenin kesin isteği üzerine açıklanabilir. Hastanın açık olarak izin vermediği durumlarda bu bilgiler sadece bilgilendirilmesi gereken diğer sağlık personeline verilebilir.

Hastanın kimliğine ait tüm bilgiler korunmalıdır. Bu bilgilerin korunması usulüne uygun yapılmalıdır. Bu tür verilerin alındığı insan ürünleri de aynı şekilde korunmalıdır.

Avrupa hasta haklarının geliştirilmesi bildirgesi olarak da 1994 tarihli Amsterdam Bildirgesi de aynı yaklaşımlar benimsenmiştir. Bildirgede, "Sağlık kurumlarına başvuran hastalar, kurumların özel hayatlarının korunmasını sağlayan fiziksel özelliklere sahip olmasını bekleme hakkına sahiptirler" düzenlemesiyse, hasta mahremiyetinin belki de en hassas noktasını oluşturmuştur. Nitekim İstanbul Tabip Odası başvuruları arasında yapılan bir çalışmaya göre; hastaların "mahremiyet" konusunda en büyük yakınmalarını, sağlık kuruluşlarının fiziksel koşullarının oluşturduğu ortaya konmuştur [2].

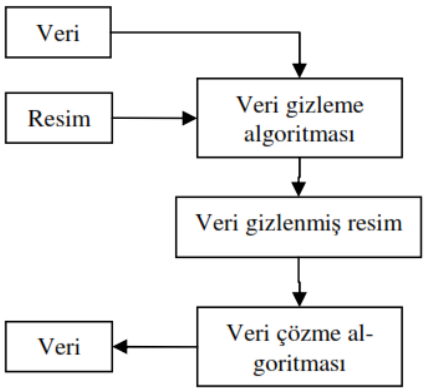
Tüm bu durumlar ve teknolojik gelişmeler göz önüne alındığında doktor ve hasta arasındaki mahremiyeti sağlamanın ve bilgilerin üçüncü şahısların eline geçmesini engellemenin yolu bilgileri şifrelemek veya gizlemektir. Şifrelenmiş veya gizlenmiş verinin bulunduğu ortamda görünmez olması ve tekrar eski haline getirebilme zorluğu bilgi güvenliğinin

sağlanabilmesi için önemli bir adımdır. Bunun için çeşitli algoritmalar geliştirilmiştir [4]. Veri gizleme disiplini içerisinde en yaygın kullanılan teknik Steganografi tekniğidir.

1.1. Steganografi

Bilgi gizleme yönteminin önemli bir alt disiplini olan Steganografi, bir nesnenin içerisine bir verinin gizlenmesi olarak tanımlanabilir [5]. Steganografi kelimesi kökleri "στεγαυος" ve "γραΦειν"'den gelen Yunan alfabesinden türetilmiştir. Tam olarak anlamı "kaplanmış yazı" (covered writing) demektir [6]. Steganografi' nin amacı gizli mesaj ya da bilginin varlığını saklamaktır. Taşınmak istenen mesaj bir başka masum görünüşlü ortamda saklanarak, üçüncü şahısların iletilen mesajın varlığından haberdar olması engellenmektedir. Bu yaklaşımla ses, sayısal resim, video görüntüleri üzerine veri saklanabilmektedir. Görüntü dosyaları içerisine saklanacak veriler metin dosyası olabileceği gibi, herhangi bir görüntü içerisine gizlenmiş başka bir görüntü dosyası da olabilmektedir [7].

Gizli bilgiyi bir resme gizleme işleminde iki dosya söz konusudur. Kapak resim ya da örtü verisi (cover image) olarak adlandırılan ilk dosya, gizli bilgiyi saklayacak resim dosyasıdır. İkinci dosya ise gizlenecek bilgi olan mesajdır. Bu mesaj da stego olarak isimlendirilmektedir. Mesaj, açık metin (plain text), şifreli metin (chipher text), başka resimler veya bit dizisi içinde saklanabilecek başka bir şey olabilmektedir. Veri gizleme işlemi sonucunda kapak resim ve gömülü mesajın oluşturduğu dosyaya "stego resim" adı verilmektedir [7]. Steganografi tekniği ile veri gizleme ve orijinal veriyi elde işleminin genel sistem yapısı Şekil 1' de gösterilmektedir.



Şekil 1. Steganografi Sistem Yapısı

Bilgi gizlemek amacıyla birbirinden farklı steganografi teknikleri geliştirilmiştir. Bu teknikler 3 ana başlık altında toplanmıştır.

En önemsiz bite ekleme
Maskeleme ve filtreleme
Algoritmalar ve dönüşümler [7].

En önemsiz bite ekleme (LSB - Least Significant Bit) en yaygın kullanılan bilgi gizleme yöntemlerinden biridir. Dolayısı ile bu çalışmada önerilen yöntemde LSB yöntemi tercih edilmiştir.

1.2. En Düşük Bite Ekleme Yöntemi

En önemsiz bite ekleme yöntemi yaygın olarak kullanılan ve uygulanması basit bir yöntemdir. Bu yöntemde; resmi oluşturan piksellerin her byte' nın en önemsiz bitinin yerine gizlenmesi istenen verinin bitleri sırasıyla verinin başlangıcından itibaren birer birer yerleştirilmektedir.

Örneğin; resmin piksel değerlerinin binary karşılığının;

10001001 11101001 11101001 10011011
10011011 10001001 00011111 00011101

şeklinde olduğunu düşünelim. Buna S (01010011) karakterini eklersek resim;

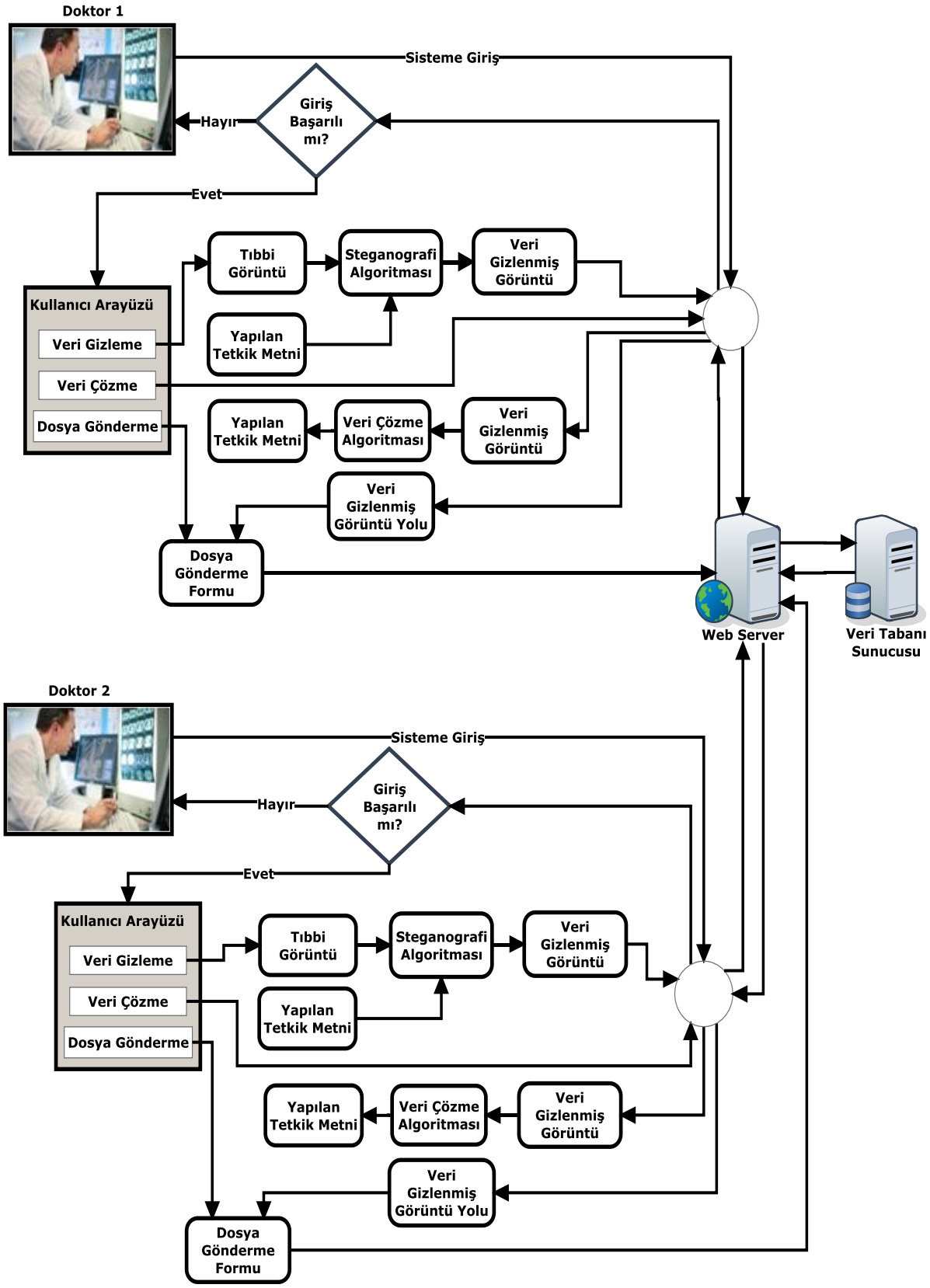
1000100**0** 1110100**1** 1110100**0** 1001101**1**
1001101**0** 1000100**0** 0001111**1** 0001110**1**

şeklinde değiştirilmiş olacaktır. Ancak, ekleme sırayla yapıldığında içine metin gizlenmiş bir resim üçüncü şahıslar tarafından kolaylıkla çözülebilmektedir. Bu dezavantajın giderilebilmesi için yöntemde [8] tarafından önerilen ve yine LSB yöntemini kullanan Shuffle Algoritması kullanılmıştır.

Bu çalışmada, doktor-hasta mahremiyetini sağlanmak amacıyla steganografi tekniğini benimseyen bir veri gizleme ve veri çözme sistemi önerilmiştir.

2. Önerilen Sistem Mimarisi

Doktor – hasta gizliliğinin sağlanması için steganografi tekniğinin kullanılarak önerilen sistem mimarisi Şekil 2' de gösterilmektedir. Mimari, veri gizleme, veri çözme ve verinin başka bir doktor ile paylaşılarak görüş alınması bileşenlerinden oluşmaktadır. Her bir bileşenin görevi ve sistemdeki rolü mantıksal olarak ayrıktır. Ancak sistem gerçek uygulamada her bir kullanıcı için bu bileşenleri içermektedir. Örneğin, Doktor 1 için veri gizleme, veri çözme ve dosya gönderme bileşenleri kullanılmaktadır. Bu bileşenler diğer tüm doktorlar içinde benzer biçimdedir.



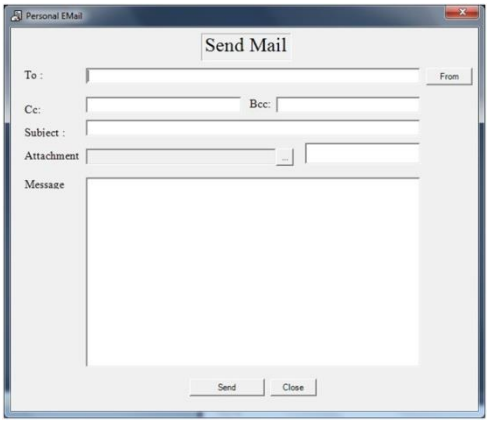
Şekil 2. Sistemin genel işleyiş mimarisi

Önerilen sistem mimarisi şu şekilde çalışmaktadır. Öncelikle doktorların işlem yapabilmesi için sisteme giriş yapmaları zorunludur. Doktorlara kullanıcı adı ve şifre bilgileri sistem yöneticisi tarafından verilmektedir. Sisteme giriş yapan doktor veri gizleme, veri çözme ve dosya gönderme menü seçenekleri ile karşılaşmaktadır. Doktorlar için kullanılan menü seçenekleri Şekil 3' de gösterilmektedir.

Şekil 3. Doktor işlem menüsü

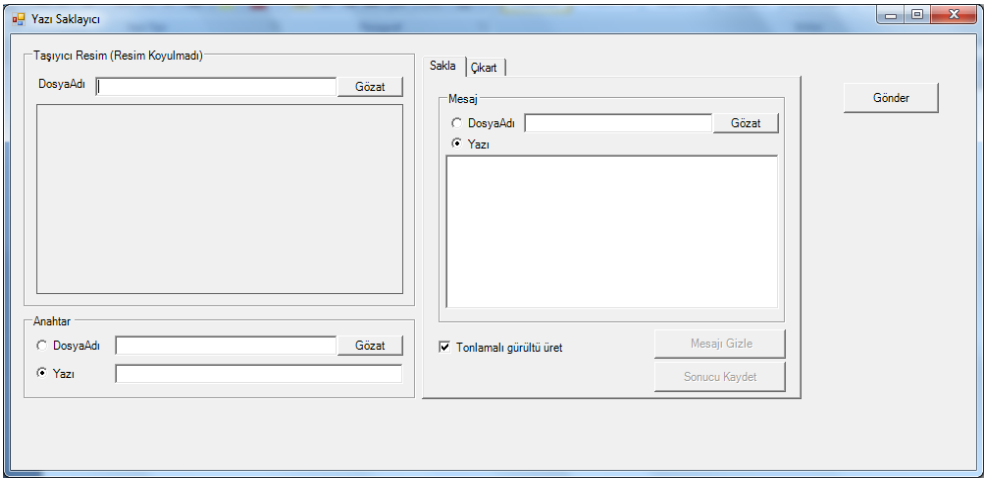
Doktor, veri gizleme seçeneğini kullanarak hasta hakkında yapmış olduğu teşhis ya da tetkik sonucunu steganografi tekniğini kullanılarak gizlenmektedir. Veri gizlenen tıbbi görüntü hasta veritabanında saklanmaktadır. Hasta veritabanında görüntü sistematik bir şekilde kaydedilmektedir. Yani hangi doktorun hangi hasta için teşhis yaptığı kolaylıkla öğrenilebilmektedir. Tıbbi görüntünün hasta adı ve vatandaşlık numarası kullanılarak kaydedilmesi de dosya karışıklığını önlemektedir.
Steganografi tekniği olarak LSB yöntemi ve [8] ' de önerilen yöntem kullanılmaktadır. Veri gizliliği son derece önemlidir. Bu nedenle yöntem, sadece teşhisi ve tetkiki yapan doktor tarafından bilinen bir şifre eklenerek güçlendirilmiştir.

Veri gizleme ve veri çözme işlemleri aynı ekran üzerinde yapılmaktadır. Doktor, elde etmiş olduğu tıbbi görüntüyü kendi branşı dışındaki doktorlar ile paylaşabilmekte ve geri bildirim alabilmektedir. Bu veri iletimi sırasında hasta hakkında belirtilen görüşler LSB yöntemi ile gizlendiğinden, üçüncü şahısların görüşlere ulaşabilmesi oldukça güçtür. Kullanılan veri gizleme ve veri çözme ekran görüntüleri Şekil 4' de gösterilmektedir.



Şekil 4. Veri gizleme ve veri çözme ekran görüntüsü

Tıbbi görüntünün karşı doktorlara iletilebilmesi için dosya gönderme seçeneği kullanılmıştır. Dosya gönderme formu, dosyanın hangi doktor tarafından hangi doktora iletileceği, konusu, mesajı ve iletilecek dosyanın yolu bilgilerini içermektedir. Karşı doktora iletilen mesajda dosya yolu yardımı ile veri gizlenmiş görüntü elde edilebilmektedir. Görüntü içerisine gizlenmiş veri, veri çözme algoritması yardımı ile elde edilmektedir. Elde edilen veriye yeni teşhis eklenerek yine karşı tarafa aynı yollarla iletilmektedir. Şekil 5' de dosya gönderme formu ekran görüntü verilmektedir.

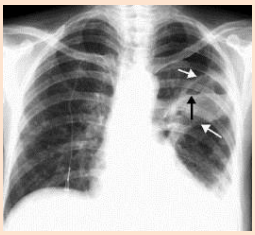
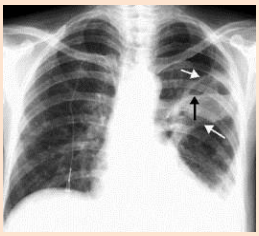


Şekil 5. Dosya gönderme formu

2. Sonuç ve Öneriler

Bu bölümde önceki kısımlarında detayları verilen yöntemin uygulanması ile elde edilen sonuçlar ele alınmaktadır. Günümüzde bilinen pek çok steganografi algoritması, uygulanmasının kolay olması nedeni ile gri resimler üzerinde gerçekleştirilmektedir. Bu çalışmada kullanılan yöntemde, resmin türünün ve biçiminin ve hatta çözünürlüğünün önemli olmadığı görülmüştür.
Geliştirilen sistemi test etmek amacıyla oluşturulan yazılım, Visual Studio 2010 C# programlama dilinde kodlanıp ve Windows 7 işletim sisteminde Intel Core 2 DUO 2.1 GHz işlemci ve 4GB ana belleğe sahip bilgisayar üzerinde çalıştırılmıştır. Önerilen sistem gelişim ve test aşamasında olduğundan yerel ağ üzerinde denenmiştir.
Uygulamanın gerçekleştirilmesinde kullanılan farklı çözünürlüklerdeki gri ve renkli tonlamalı röntgen görüntülerine tetkik metni gizlenmiş ve veriler tekrar elde edilmiştir. Kullanılan orijinal ve veri gizlenmiş görüntüler Tablo1' de gösterilmektedir.

Tablo1. Uygulamadan elde edilen sonuç görüntüleri ve metinler

Orijinal Görüntü	Gizlenen Metin	Veri Gizlenmiş Görüntü	Çözülmüş Metin
	Sol akciğer üzerinde bilinmeyen bir leke görülmüştür.		Sol akciğer üzerinde bilinmeyen bir leke görülmüştür.
	Beyne yakın bir noktaya kadar 20 cm lik bir çivi saplanmıştır		Beyne yakın bir noktaya kadar 20 cm lik bir çivi saplanmıştır

Tablo 1' den de görüldüğü üzere, veri gizleme ve veri elde etme işlemleri başarılı bir şekilde gerçekleştirilmiştir. Veri gizlenmiş görüntülere dikkat edildiğinde gözle görülebilir bir bozulmanın olmadığı ve görüntü kalitesinde bir değişlik yaşanmadığı görülmektedir. Tasarlanan bu sistem doktor – hasta mahremiyeti dışında, veri gizliliğinin ihtiyaç duyulduğu her alanda rahatlıkla kullanılabilecektir.

4. Kaynaklar

[1]http://www.istanbulsaglik.gov.tr/w/hashak/bali.asp, Erişim Tarihi: 22.11.2012

[2] http://www.hastane.com.tr/saglik/hekim-ve-hasta-mahremiyeti-hakkinda-neler-biliyorsunuz.html, Erişim Tarihi: 22.11.2012

[3] http://www.istanbulsaglik.gov.tr/w/hashak/bali.asp, Erişim Tarihi: 22.11.2012

[4] Tuncer, T., Doğan, Ş., Avcı, E., "Renkli İmgelerde Gizlenen Verilerin Görsel Ataklara Karşı Dayanıklılığının Tespiti İçin Bir Steganografi Uygulaması", 6th International Advanced Technologies Symposium (IATS'11), 16-18 May 2011, Elazığ, Turkey.

[5] Petitcolas F.A.P., Anderson R.J., Kuhn M.G., "Information Hiding–A Survey", Proceedings of the IEEE, Special Issue on Protection of Multimedia Content, 87(7):1062-1078, July 1999.

[6] Murray A.H., Burchfiled R.W (eds.), "The Oxford English Dictionary: Being a Corrected Re-issue", Oxford, England: Clarendon Pres, 1933.

[7] Şahin, A., Buluş, E., Sakallı, M.T., Buluş, N., "Resim İçerisindeki Gizli Bilginin RQP Steganaliz Yöntemiyle Sezilmesi", Akademik Bilişim 2007 Dumlupınar Üniversitesi, Kütahya 31 Ocak–2 Şubat 2007.

[8] E.M. Esin, E. Güvenoğlu, "Resim İçine Yazı Gizlenmesi Amacıyla Kullanılan EDB Ekleme Yönteminin Shuffle Algoritmasıyla İyileştirilmesi", Türkiye Bilişim Vakfı Bilgisayar Bilimleri ve Mühendisliği Dergisi, Sayı:02, pp. 73-79, 2006.