YILDIZ TEKNİK ÜNİVERSİTESİ
FEN BİLİMLERİ ENSTİTÜSÜ

E-DEVLET KAPSAMINDA SAYISAL COĞRAFİ VERİLERİN KORUNMASINA YÖNELİK UYGULAMALAR

Harita Müh. Murat ÜNLÜ

FBE Jeodezi ve Fotogrametri Mühendisliği Anabilim Dalında Hazırlanan

YÜKSEK LİSANS TEZİ

Tez Danışmanı : Prof.Dr. Zübeyde ALKIŞ

İSTANBUL, 2008

YILDIZ TEKNİK ÜNİVERSİTESİ
FEN BİLİMLERİ ENSTİTÜSÜ

E-DEVLET KAPSAMINDA SAYISAL COĞRAFİ VERİLERİN KORUNMASINA YÖNELİK UYGULAMALAR

Harita Müh. Murat ÜNLÜ

FBE Jeodezi ve Fotogrametri Mühendisliği Anabilim Dalında Hazırlanan

YÜKSEK LİSANS TEZİ

Tez Danışmanı : Prof.Dr.Zübeyde ALKIŞ(YTÜ)
Jüri Üyeleri : Prof.Dr.Sıtkı KÜLÜR(İTÜ)
: Doç.Dr.:Fatma Gül BATUK(YTÜ)

İSTANBUL, 2008

İÇİNDEKİLER

Sayfa

SİMGE LİSTESİ

F_M	Orta frekans bandı
$h(x, y)$	Altlık görüntü piksel koordinatı fonksiyonu
H	Altlık görüntü
H_b	8x8 bloğa ayrılmış altlık görüntü
I	bloktaki piksel yeri
I_w	Sonuç mühürlü görüntü
i	Başlangıç sayısı
K	Rasgele sayı üretmek için seçilen anahtar sayısı
M	20x50 piksel boyutlarındaki siyah-beyaz mesajı
$\dot{I}$	İkilik mesajı
M_p	Permutasyon uygulanmış ikilik mesaj
N_1	Altlık görüntü piksel satır sayısı
N_2	Altlık görüntü piksel sütun sayısı
P	Permutasyon
π	Pi sayısı
W	Orta frekans bandındaki katsayısı

KISALTMA LİSTESİ

ABD	Amerika Birleşik Devletleri
BMP	Bitmap
CAD	Computer Aided Design
CBS	Coğrafî Bilgi Sistemi
CBT	Coğrafi Bilgi Teknolojiler
CVT	Coğrafî Veri Tabanı
DCT	Discrete Cosine Transform
DFT	Discrete Fourier Transform
DGM	Devlet Güvenlik Mahkemesi
DXF	Drawing Exchange Format
DVD	Digital Versatile Disc
DWT	Discrete Wavelet Transform
FFT	Fast Fourier Transform
FSEK	Fikir ve Sanat Eserleri Kanunu
GATT	General Agreement on Tarrifs and Trade
GIF	Graphic Interchange Format
HKMO	Harita ve Kadastro Mühendisler Odası
IBM	International Business Machines
JPEG	Joint Photographic Experts Group
LSB	Least Significant Bit Insertion
MDB	Microsoft Database
PKCS	Cpabilities of Pblic Key Cryptosystems
SKYS	Seri Kopya Yönetim Sistemi
TBMM	Türkiye Büyük Millet Meclisi
TRIPs	Trade Related Aspects of Intellectual Property Rights
UTM	Universal Transverse Mercator
WAV	Waveform
WCT	WIPO Copyright Treaty
WIPO	World Intellectual Property Organization
WNS	White Noise Storm

ŞEKİL LİSTESİ

ÖNSÖZ

E-Devlet kapsamında sayısal coğrafi verilerin korunmasına yönelik uygulamaları konulu bu tezde, çalışmamın teorik ve uygulama bölümünde yardımlarını esirgemeyen, değerli fikir ve katkıları ile çalışmama yön veren tez danışmanım Prof. Dr. Zübeyde ALKIŞ'a çok teşekkür ederim.

Çalışmam sırasında bana her türlü manevi desteği sağlayarak sürekli yanımda olan eşim İmran ÜNLÜ'ye çok teşekkür ederim.

ÖZET

Coğrafi Bilgi Sistemlerinin temel bileşenini, sayısal coğrafi veriler oluşturmaktadır. Bu veri setlerini oluşturmak pahalı ve kopyalanması çok kolaydır. Bundan dolayı fikri mülkiyet haklarıyla bu verileri korumak gerekir. Birçok uzmanın, yüksek maliyet ve uzun çalışmalarla ürettiği bu ürünlerin, bire bir kopya edilmesinin veya taklit edilerek benzerinin üretilmesinin diğer ürünlere göre daha kolay ve ucuz olması, bunların hukukî koruma olmadan, yalnızca teknik yollarla korunmasının hiçbir anlamı olmadığını göstermiştir. Üzerinde değişiklik yapılması, kopyalanması ve çoğaltılması belki de en kolay olan ürünler sayısal görüntülerdir. Sayısal görüntülerdeki bu sorunun çözümü için yapılan çalışmalardan biri, görüntülere çalışmanın sahibi, yapım yılı ya da firma logosu gibi bir bilginin damgalanmasıdır. Bu bilgi, taşıyıcı görüntü üzerine görünür bir şekilde damgalanabileceği gibi görüntüye insan gözünün algılayamayacağı bir teknikle de yapılabilir.

Bu çalışmada, sayısal coğrafi verilerinde eser sahibi hakları 5846 sayılı Fikir ve Sanat Eserleri Kanunu dâhilinde ele alınmış, sayısal coğrafi verilerin yetkisiz kullanımına karşı korumasına yönelik yasal ve teknik yöntemler incelenmiş, uygulanmakta olan raster harita sayısal mühürleme sistemlerin yetkisiz şahısların girişini engelleyen, yasal kullanımı sağlayacak uygulamalar açıklanmıştır.

Anahtar kelimeler: Sayısal coğrafi veri koruma, eser sahibini haklarını koruma, Steganografya, sayısal mühürleme, mühürleme, işaretleme, görüntülerin telif haklarını koruma, teknik önlemler, yasal önlemler, FSEK, eser haklarını koruma, bilgi saklama sanatı, mülkiyet, fikri mülkiyet hakları, DCT.

ABSTRACT

The base core component of geographic information systems consists of digital spatial data sets. Spatial data sets are expensive to create and are now very easy to copy. So, we need intellectual property rights to protect them. The easiness and cheapness in copying or counterfeiting these products, which require high costs and long studies of many specialists when compared to other products, proved that only technical without legal protection, is nonsense. Digital images are the products which can be easily modified, copied and duplicated. One of the studies to solve copyright protection on the digital images is to embed some information about the author, production year or logo. This information can be embedded into an image where it can be perceptually either visible or invisible.

This study, mentions the copyrights in digital spatial data within the frame of the Intellectual Property Rights Law numbered 5846 and discusses the legal and technical methods to protect digital spatial data against unauthorized use and explains how to utilize the raster map watermarking systems that illegal use by preventing unauthorized access to data and from execution of protected applications.

Keywords: Digital spatial data protection, copyright protection, steganography, digital watermarking, watermarking, fingerprinting, copyright protection of images, technical measures, legal measures, FSEK, copyright, art of hiding information, ownership, intellectual property rights, DCT.

1. GİRİŞ

Harita mühendisliği eğitiminde genel olarak jeodezi, fotogrometri, kartografya, astronomi, matematik, jeofizik, bilgisayar ile birlikte Türkiye'de, hukuk dersleri de verilmekte ancak bunun kapsamı yalnızca büyük ölçekli haritalarda mülkiyet kavramlarında ortaya çıkacak problemlerin çözümüne yönelik eşya hukuku ile sınırlı kalmaktadır. Ancak harita mühendisliğinin hukukla bağlantısını yalnızca eşya hukuku ile sınırlandırmak doğru değildir. Gerek haritaların, gerekse üretim maliyetleri çok yüksek olan coğrafi verilerin ve artık günümüzde vazgeçilmez bir parçası olan CBS (Coğrafî Bilgi Sistemi) yazılımları ve dolayısıyla e-devlet kapsamında coğrafî veri tabanlarının kurumlar arası paylaşımından doğan sorunlarda; eşya hukukundan ayrı olarak fikrî hukuk devreye girmektedir. Ancak bu konuda herhangi bir bilgi üniversitelerimizin Jeodezi ve Fotogrametri Mühendisliği Bölümlerinde verilmemektedir.

Coğrafî bilgi ihtiyacına cevap verebilmek üzere bu alanda yapılan yatırımlarının ve gösterilen çabaların teknik olarak korunmasının gelişen teknolojiye bağlı olarak çok kolay olmadığı, bu konudaki fikir ve emek hırsızlığının, bilgisayarın bir tuşuna basmaktan ibaret olduğu maalesef bir gerçektir.

Milyarlarca para ve büyük emekler verilerek oluşturulan bir birikimin, izinsiz olarak bir ortama kaydedilmesini ve bunların çoğaltılmasını önlemek için dünyada hukukî birçok esaslar belirlenmekte ve teknoloji ihraç eden ülkeler tarafından bunlar diğer ülkelerle yapılacak işbirliğinde bir şart olarak aranmaktadır. Çünkü bu konuda getirilecek teknolojik tedbirler yine aynı teknoloji ile çok kısa bir sürede bertaraf edilmekte ve korsan olarak piyasaya sürülmektedir. Gelinen bu teknolojik seviyede şu bir gerçektir ki; hukukî olarak korunmayan bir şeyin teknik olarak korunması imkânsızdır.

Bu kapsamda geçen 10 yılda dünyada hukukî olarak bilgisayar programları ve veri tabanlarının korunmasına yönelik birçok gelişme yaşanmıştır. Bunlardan en önemli olanı ise Avrupa Birliği'nde veri tabanlarındaki verilerin de korunmasına imkân veren ve kendine özgü bir niteliği olması nedeniyle adını bundan alan "Sui Generis" (kendine özgü-herhangi bir kategoriye girmeyen) bir hakkın 1996 yılında yürürlüğe girmesidir. Bu konuda herhangi bir özgün tarafı olmadığı için eser sahibi hakkı (copyright) kapsamında korunmayan verilere, sermaye ve emeğin korunması esas alınarak farklı bir koruma getirilmiş ve bilgi korsanlığı yasaklanmıştır (Nalcı, 2002).

İnanılmaz bir seviyeye gelen bilgi teknolojisi içerisinde haritacılık, başta kentleşme ve savunma sanayiinde olmak üzere birçok bakımdan giderek önem kazanmakta ve buna bağlı olarak da yapılan yatırımlar giderek artmaktadır.

Bu çalışmada; hukukî konulardan daha çok bilhassa haritacılık açısından önemli olan sayısal coğrafi verilerin teknik olarak korunmasına yönelik bilgi sunulmaya çalışılmış ve bunlara ait uygulamalar yapılmıştır. Sayısal verinin her ne kadar teknik olarak korunması ve uygulamaları ele alınsa da öncelikle hukukî konulardan bahsetmek gerekir.

Türkiye'de fikrî haklara ilişkin bazı terimler üzerinde henüz birliğin sağlanamaması nedeniyle, burada bir açıklama yapmak gerekmektedir. Batıda kullanılan terimlere karşılık olarak "Intellectual Property" yerine "Fikrî Haklar/fikri mülkiyet hakları", özgün edebiyat ve sanat eserlerinin korunmasını (izinsiz yayımlanmaması) ifade eden "copyright" yerine, "telif hakkı" değil, FSEK (Fikir ve Sanat Eserleri Kanunu)' de yer alan "eser sahibinin hakları" terimi kullanılmıştır.

2. ESER SAHİBİNİN HAKLARI

2.1 Genel

Teknolojinin, haritanın üretim ve tüketim zincirini değiştirmesi ile haritanın ifade ettiği kavramlar da değişmiştir. Günümüzde bir haritanın üretiminde; başta jeodezik ve fotogrametrik olmak üzere elde edilen coğrafi veriler, bu verilerin belli bir sisteme göre tasnif edildiği veri tabanları desteği ile tematik harita üretimine yönelik CBT (Coğrafi Bilgi Teknolojiler)leri kullanılarak oluşturulan Coğrafi Bilgi Sistemleri pek çok disiplin tarafından kullanılmaktadır. Bu sistemlerin kullanımı kurumlara daha kolay ve hızlı karar verme olanağı sağlamaktadır. Ancak bu sistemi kurabilmek için gerekli yazılım donanım ve özellikle grafik veriler ve bu konuda yetişmiş elemanlar önemli bir yatırım gerektirmektedir. Büyük bir emek ve maliyet ile üretilen haritalar, CBT araçlarını kullanmak CBS yazılımları ve CVT (Coğrafî Veri Tabanları) insan emeği olmaları itibari ile, fikrî hukukun koruma kapsamına girmektedir. Bu sayede haksız rekabete engel olunarak harita üreten müteşebbisin emek ve sermaye harcayarak ortaya çıkardığı ürün korunmakta bu da sektörün ilerlemesine katkı sağlamaktadır (Nalci,2002).

Türkiye'de; haritalar, CBT'de sayısal coğrafi verileri, CBS yazılımları bilim ve edebiyat eseri olarak, içindeki veri hariç olmak üzere CVT'ları ise işleme olarak, 5846 sayılı FSEK ile korunmaktadır. Bu kanun ile eser sahibinin, eseri üzerindeki manevî ve malî hakları belirlenmekte, tanınan bu haklar yasal ve üstün sayılan özel ve genel menfaatlere yön vermek için kısıtlanmakta (Belgesay, 2001), korunma ile bu ürünlerden yararlanma şartları düzenlenmekte, öngörülen esas ve usullere aykırı yararlanma halinde yaptırımlar tespit edilmektedir (FSEK Md. 1).

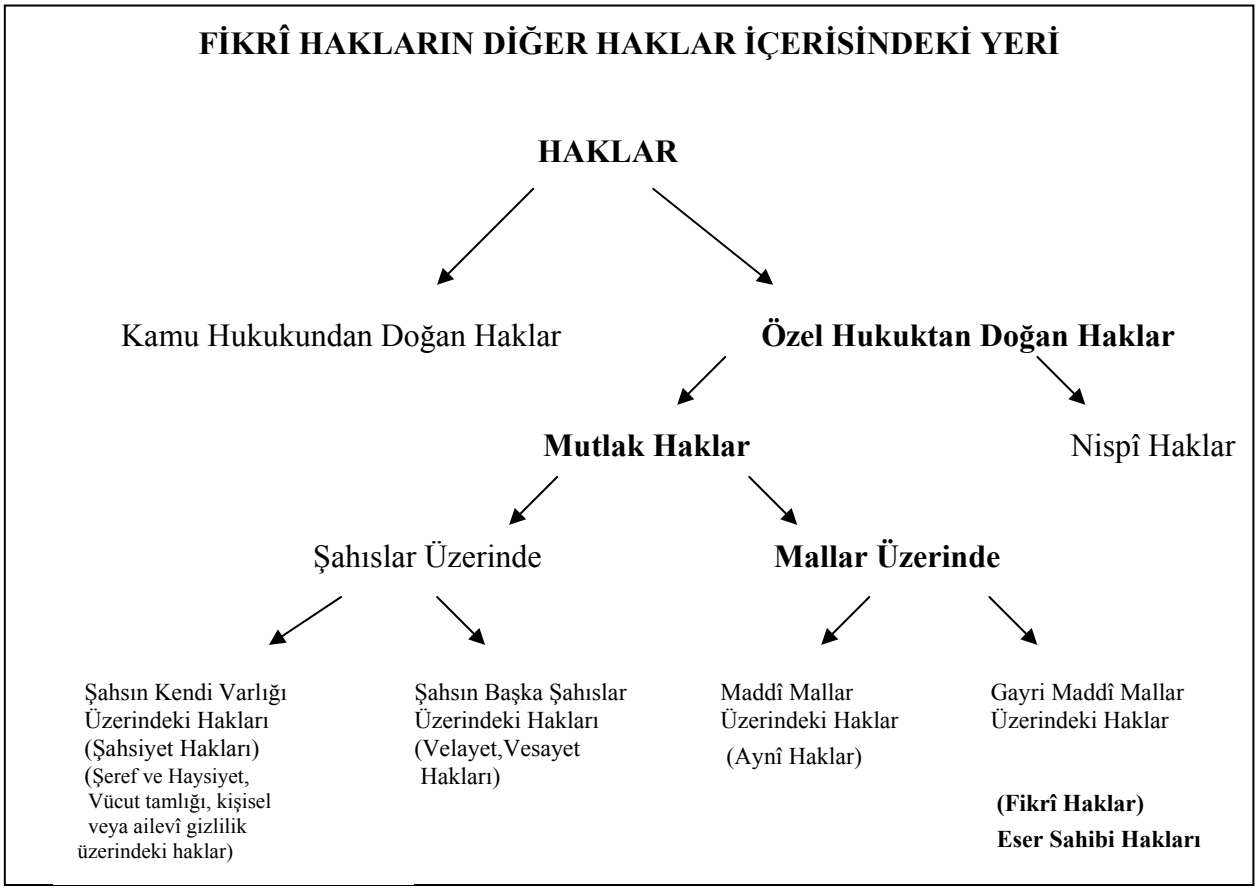
2.2 Eser Sahibi Haklarının Hukuk Sistemindeki Yeri

Harita ve harita üretiminde yer alan CBT' de sayısal coğrafi verileri hukuk düzeni içerisinde fikrî hukuk altındaki eser sahibi hakları (copyright) kapsamında korunmaktadır. Diğer bir ifade ile eser olarak kabul edilen haritaları, bilgisayar programlarını ve veri tabanlarını üretenlerin, bunlar üzerinde eser sahibi hakları mevcuttur.

Eser sahibi haklarının ve fikrî hakların fertlere tanınan haklar içerisindeki yeri Şekil-1 de sunulmuştur (Erel, 1998). Eser sahibi hakkı, hem manevî hem de malî yönü bulunan çift karakterli bir hak niteliğindedir ve bu özelliğiyle karma nitelikli haklar arasında yer alır.

Hukuk düzenindeki kamu ve özel hukuk alanları ayrımına paralel olarak hakları da kamu hukukundan doğan haklar ve özel hukuktan doğan haklar olmak üzere ikiye ayırmak mümkündür. Fikrî hakları ilgilendirmesi nedeniyle özel hukuktan doğan hakları, konuları ve hak sahibine sağladıkları yetkilerin türü ve niteliği bakımından "mutlak haklar" ve "nispî haklar" olarak ikiye ayırmak mümkündür.

Hakları konularına göre sınıflandırdığımızda, mutlak hakları; şahıslar ve mallar üzerindeki haklar olmak üzere ikiye ayırabiliriz. Mallar üzerindeki mutlak haklar da maddî ve gayri maddî olarak ikiye ayrılır. Fikrî haklar, gayri maddî mallar üzerindeki mutlak haklardandır. Gayri maddî mallar, taşınır veya taşınmaz mallar dışında, yaratıcı insan zekâsının ürünü olan, üzerinde cisimlendiği maddî mallardan ayrı bir hukukî varlığa ve ekonomik değere sahip mallardır (Erel, 1998).



Şekil 2.1 Fikrî hakların diğer haklar içersindeki yeri (Erel, 1998).

Türkiye'de fikrî haklar konusundaki ilk düzenlemeler;

- 1857 Hakkı Telif Nizamnamesi (Değişiklik 1910 Hakkı Telif Kanunu ve 1951 Fikir ve Sanat Eserleri Kanunu),
- 1871 Alameti Farika Nizamnamesi (Değişiklik 1965 Markalar Kanunu ve 1995 Markaların Korunması Hakkında Kanun Hükmünde Kararname) ,
- 1879 İhtira Beratı Kanunu (Değişiklik 1995 Patent Haklarının Korunması Hakkında Kanun Hükmünde Kararname) olmuştur.

Koruma, fikrin ifade biçimine göre, değişik yasal düzenlemelerle sağlanmaktadır. Örneğin yeni buluşlar patent ya da faydalı model belgeleri ile endüstriyel tasarımlar (ürünün iki ya da üç boyutlu görünüşleri); FSEK, Endüstriyel Tasarımların Korunması Hakkında Kanun Hükmünde Kararname, Türk Ticaret Kanunu Haksız Rekabet Hükümleri, Markaların Korunması Hakkında Kanun Hükmünde Kararname ile çoklu yasal korumadan yararlanarak, korunmaktadır (Dericioğlu, 2002).

2.3 Eser Sahibi Hakları ve Fikrî Hakların Dünyada Gelişimi

Modern fikir ve sanat eserleri kanununa öncülük eden kanun, 1709 yılında İngiltere'de çıkarılmıştır (Ayiter, 1981). Sadece yazarları koruyan bu kanunun amacı yazarı ekonomik yönden gözetmek ve bilimin teşvik edilmesini sağlamaktır (Gökyayla, 2000). Bunu takiben Fransa'da 1789 İhtilalinden sonra 1791 yılında temsil hakkına, 1793 yılında da eser sahibi haklarına dair iki kanun çıkarılmıştır.

Almanya'da ise siyasi birliğin geç temin edilmesi nedeniyle ilk olarak 1837 yılında Prusya için bir kanun çıkarılmış ve bu kanun 1871 yılında Reich (İmparatorluk) kanunu olarak benimsenmiş, İsviçre'de ise eser sahibinin korunması nispeten geç olarak 1884 yılında gerçekleşmiştir. Osmanlı İmparatorluğunda fikrî haklar konusundaki ilk düzenleme ise; 1857 Hakkı Telif Nizamnamesi ile getirilmiştir (Ayiter, 1981, Erel, 1998).

2.3.1 Uluslararası Alandaki Gelişmeler

İki taraflı anlaşmalar yerine, çok taraflı anlaşmalar yaparak, gelişmemiş ülkeleri taahhüt altına sokacak uluslararası anlaşmaların yapılmıştır (Gökyayla, 2000). Bu noktadan hareketle 1886 yılında, sınaî haklar için "Paris İttihadı Antlaşması" ve "Edebî ve Artistik Eserlerin Himayesi için Bern Sözleşmesi" belgeleri imzalanmıştır.

2.3.1.1 Bern Sözleşmesi

Fikir ve sanat eserleri sahiplerinin haklarını gerek kendi ülkelerinde gerek diğer ülkelerde etkili bir şekilde korumak amacıyla 1886 yılında İsviçre'nin Bern şehrinde 10 devletin katılımıyla toplanan bir uluslararası konferans sonunda "Bern Sözleşmesi" imzalanmış ve tüzel bir kişiliğe sahip "Bern Birliği" kurulmuştur. Bu sözleşme ile üye ülkelerin daha geniş bir koruma tanıma hakları saklı kalmak şartı ile eser sahiplerine bazı asgarî haklar sağlanmıştır (Ayiter, 1981, Erel, 1998). 1886 yılında oluşturulan bu sözleşme 1896'da Paris'te, 1908'de Berlin'de (bu 1914'de Bern'de tamamlanmıştır), 1928'de Roma'da, 1948'de Brüksel'de, 1967'de Stockholm'de ve son olarak da 1971'de Paris'te olmak üzere altı kez tadil edilmiştir. 1971 yılında yapılan tadilatın 1979 yılında tamamlanmasıyla son şeklini almıştır. Bern Sözleşmesine harita kavramı 1908 yılında girmiştir (Beşiroğlu, 2002).

Bern Sözleşmesine göre; birlik üyesi bir ülke vatandaşının, başka bir üye ülkede yayımlanan eseri ile üye ülke vatandaşı olmayanların, üye bir ülkede ilk defa yayımlanmış eseri, bütün diğer üye ülkelerde, kendi vatandaşlarına tanıdıkları ve ileride tanıyacakları haklar da dâhil olmak üzere, korunmaktadır (Madde3/1-Madde5/1). Ancak, Birlik üyesi olmayan bir devlet, üye devletlerin vatandaşlarına daha az koruma sağlıyorsa, onlara sağlanan koruma da karşılıklılık esasına göre azaltılabilecektir (Madde 6/1).

Türkiye ilk olarak 01 Ocak 1952 tarihinde, Sözleşmenin 1948 Brüksel metnine katılmış ancak 10 yıl önce yayımlanan eserlerin Türkçe'ye bedel ödemeden serbestçe çevirisini mümkün kılmak amacıyla Sözleşmenin 8'inci maddesine koyduğu ihtirazî kayıtla 1896 Paris metninin 5'inci maddesini kabul etmiştir. Daha sonra Türkiye 12 Temmuz 1995 tarihinde Bern Sözleşmesinin 24 Temmuz 1971 tarihli Paris metnine de taraf olmuştur.

2.3.1.2 Amerika Kıtasındaki Gelişmeler

Bern sözleşmesi ile Avrupa Kıtasında bir takım gelişmeler yaşanırken, buna paralel olarak Amerika Kıtasında da 1889 yılında 7 Güney Amerika devleti tarafından imzalanan Montevideo sözleşmesi imzalanmıştır. Daha sonra 1946 yılına kadar beş sözleşme daha yapılmış ancak bunlara ABD (Amerika Birleşik Devletleri) taraf olmamıştır. Bunlardan Buenos Aires Sözleşmesi; 17 Amerika Kıta devleti ile birlikte ABD'nin de taraf olması nedeniyle önemli kabul edilmektedir.

2.3.1.3 Evrensel Eser Sahibi Hakları Sözleşmesi (Universal Copyright Convention)

06 Eylül 1952 tarihinde Cenevre'de, UNESCO'nun öncülüğünde Amerika Kıt'a devletleri ile Avrupa devletleri arasındaki sistem farklılıklarını uzlaştırarak düşünce hakları alanındaki düzenlemelerde ulusal farklılıklar bulunan devletleri ortak bir düzeyde bir araya getirmek ve böylece fikir ve sanat eserlerinde kıt'alar arası bir koruma sağlamak amacıyla (Ayiter, 1981, Erel, 1998), Amerika Kıt'asından devletlerin de katılımı ile toplam 35 devlet tarafından Evrensel Düşünce Hakları Sözleşmesi imzalanmıştır (Belgesay, 2001). Bu sözleşmenin sağladığı koruma özellikle koruma süresi açısından Bern Sözleşmesinden daha hafiftir. Katılan devletler, vatandaşlarına tanıdıkları haklar bakımından karşılıklılık (mütekabiliyet) esasını kabul etmişlerdir (Erel, 1998). Sözleşme son olarak 1971 yılında Paris toplantısında gözden geçirilmiştir. Aynı zamanda Paris ve Bern Birliğine de üye olan 96 ülke bu sözleşmeye taraf iken Türkiye taraf bulunmamaktadır. Kültür Bakanlığı yetkilileri ile yapılan görüşmede buna gerekçe olarak, Türkiye'nin Bern ve Ticaretle Bağlantılı Fikri Mülkiyet Hakları (Trade Related Aspects of Intellectual Property Rights -TRIPs) Anlaşması metni imzalamakla bu sözleşmenin gereklerini zaten yapıyor olduğu ifade edilmiştir.

2.3.1.4 Dünya Fikrî Mülkiyet Örgütü (WIPO) Kuruluş Sözleşmesi

14 Temmuz 1967 tarihinde Stockholm'de atılan diğer önemli bir adım da, Dünya Düşünce Mülkiyeti Örgütü-WIPO (World Intellectual Property Organization) adı altında yeni bir kuruluşun oluşturulmasıdır (Beşiroğlu, 1999). Bu örgütün amacı; dünyada fikrî mülkiyet kavramını yerleştirip geliştirmek ve bu doğrultuda devletler ve gerektiğinde uluslararası kuruluşlarla işbirliği yapmaktır. Örgüt, evrensel kültürün korunmasını sağlamak üzere gerekli önlemleri almak, fikrî haklar alanında ülkelerin millî mevzuatlarının birleştirilmesini sağlamak, Bern ve Paris Birliklerinin idarî hizmetlerini görmek, fikrî hakların korunmasını geliştirmek ve bu konuda teknik ve hukukî yardım talep eden devletlere yardımcı olmak, fikrî mülkiyetle ilgili milletler arası siciller tutmak ve bütün bu konularda gerekli bilgileri yayımlamak gibi görevler üstlenmiştir (Erel, 1998). Türkiye bu kuruluşa 14 Ağustos 1975 tarih ve 7/10540 sayılı Bakanlar Kurulu Kararı ile katılmıştır.

Bu kapsamda, uzun yıllar süren tartışmalardan sonra 20 Aralık 1996'da Cenevre'de toplanan uluslararası konferansta WIPO Eser Sahibi Hakları Andlaşması (WIPO Copyright Treaty-WCT) kabul edilmiştir (Beşiroğlu, 1999).

2.3.1.5 Düşünce Mülkiyeti Haklarının Ticarete İlişkin Yönleri Üzerine Anlaşma (TRIPs Anlaşması)

Yaratıcı Düşünce ürünlerinin giderek daha önemli bir oranda ticarete konu oluşturması, ülkeler arasında ürün ve hizmet alışverişi için öngörülen gümrük koşulları uygulanması üzerinde durulmasını zorunlu kılmıştır. Bu konuda gerekli önlemlerin alınmasında, 1967 yılında son şekli verilen GATT (General Agreement on Tarrifs and Trade - Ticaret ve (Gümrük) Tarifeleri Genel Anlaşması), ciddi bir rol oynamıştır. GATT bünyesinde, düşünce ürünü eserlerin ticarî boyutu ve uluslararası akışının düzenlemesi çalışmalarına Uruguay Round adı verilen çalışmalar ile başlanılmış, 15 Nisan 1994 tarihinde Marakeş'te kabul edilen Dünya Ticaret Örgütü Anlaşması (Agreement Establishing the World Trade Organization)'nın IC Ek'inde yer alan Düşünce Mülkiyeti Haklarının Ticarete İlişkin Yönleri Üzerine Anlaşma (Trade-Related Aspects on Intellectual Property Rights-TRIPs) kabul edilmiştir. Türkiye TRIPs Anlaşmasını 31 Aralık 1994 tarihinden geçerli olmak üzere 4067 Sayılı Kanun ile onaylamıştır.

TRIPs Anlaşması, eser sahibinin hakları ve komşu haklar, markalar, coğrafî işaretler, endüstriyel tasarımlar, patentler, entegre devre topografyaları, açıklanmamış bilgilerin korunması ile sözleşmeye bağlı lisanslarda rekabete karşı uygulamaların denetimi konularını kapsamaktadır (Gökçü, 2000).

2.3.2 Fikir ve Sanat Eserleri Kanununun Türkiye'de Gelişimi

2.3.2.1 Türkiye Cumhuriyetinde Fikir ve Sanat Eserleri Kanununun Oluşturulması

Türkiye, 1931 tarihinde Bern Sözleşmesine, çeviri konusunda çekince koymak şartı ile katılmak istemiş ancak sözleşmeye taraf 10 ülkenin itirazı üzerine bu mümkün olmamıştır (Ayiter, 1981, Beşiroğlu, 1999).

Türkiye, 1931 tarihinde Bern Sözleşmesine, çeviri konusunda çekince koymak şartı ile katılmak istemiş ancak sözleşmeye taraf 10 ülkenin itirazı üzerine bu mümkün olmamıştır (Ayiter, 1981, Beşiroğlu, 1999).

10 Mayıs 1939 tarihinde Millî Eğitim Bakanı, İstanbul Üniversitesi Hukuk Fakültesinden, yeni bir düşünce hakları kanun taslağının hazırlamasını istemiş, bunun üzerine Prof.Ernst E.Hircsh tarafından hazırlanan yeni taslak 1941 yılında Millî Eğitim Bakanlığına teslim edilmiş ancak bu taslak yasalaşmamıştır (Beşiroğlu, 1999).

Daha sonra, 1948 Yılında İstanbul Üniversitesi Hukuk Fakültesine aynı teklif Adalet Bakanlığından gelmiş ve aynı yıl taslak hazırlanarak Adalet Bakanlığına gönderilmiştir. Bu taslak 27 Ekim 1950'de Hükümet Tasarısı olarak Parlamentoya sunulmuş, taslağın temel içeriğinde hiçbir nesnel değişiklik yapılmadan 05 Aralık 1951'de kabul edilerek 01 Ocak 1952'de 5846 sayı ile yürürlüğe girmiştir (Beşiroğlu, 1999). 5846 sayılı Fikir ve Sanat Eserleri Kanununu (FSEK) ile Türkiye, çeviri konusunda 1896 Paris Metni esas almak şartı ile Bern Sözleşmesinin 1948 Brüksel Belgesine, 01 Ocak 1952 tarihinde üye olmuştur.

5846 sayılı FSEK'nun uluslararası düşünce hakları alanındaki gelişmelere uyumu amacıyla 1972 yılında hükümet tarafından bir değişiklik girişiminde bulunulmuş ancak hemen sonrasında yapılan hükümet değişikliği nedeniyle bundan bir sonuç alınamamıştır (Beşiroğlu, 1999).

2.3.2.2 1983 Yılında Yapılan Değişiklik

Kanunun etkinlikle kullanılabilmesinin en başta eser sahiplerinden oluşan meslek birliklerinin oluşturulmasına ve çalışabilmelerine bağlı olmasından hareketle, 03 Kasım 1983 tarihinde kabul edilen 2936 sayılı kanun ile, 5846 sayılı FSEK'nda meslek birliklerinin kurulmasına imkân veren eklemeler yapılmıştır (Erel, 1998).

2.3.2.3 1995 Yılında Yapılan Değişiklik

Bu değişiklik 07 Haziran 1995 tarih ve 4110 Sayılı Kanun ile; bilgisayar programları, veri tabanları, koruma süreleri, meslek birlikleri, hakların ihlâllerinde verilen cezalarla ilgili düzenlemeler yapılmıştır.

Ayrıca, 4110 Sayılı Kanunun kabulünü müteakip 12 Temmuz 1995 tarihinde, Türkiye'nin, Bern Sözleşmesinin 1979 Paris Metnine katılmasına ilişkin 4117 sayılı kanun yürürlüğe girmiştir.

2.3.2.4 2001 Yılında Yapılan Değişiklik

Fikir ve Sanat Eserleri Kanununun 44 Maddesinin Değiştirilmesine İlişkin Kanun Tasarısı 21 Şubat 2001 tarihinde Genel Kurulda görüşülmüş ve oy birliği ile kabul edilerek 4630 sayı ile yasalaşmış, 03 Mart 2001 tarihinde de Resmî Gazetede yayımlanarak yürürlüğe girmiştir (Talay, 2001).

Kültür Bakanlığı tarafından yapılan bu son değişikler ile;

- Eser sahiplerinin daha nitelikli eser üretmelerinin sağlanması,
- Eserlerin derlenmesi yoluyla ulusal bir arşiv oluşturulması,
- Ağır para ve hapis cezaları ve kurulacak denetim komisyonları aracılığı ile Avrupa Birliği üyelerinde de organize suç olarak adlandırılan korsan faaliyetlerle mücadelede etkinliğin sağlanması,
- Kayıt dışı faaliyetlerin kayıt altına alınması ve böylece vergi gelirlerinin artması,
- Fikrî yaratımlar sonucu oluşan eserlerin tüketiciye ulaşmasına kadar olan süreç içerisinde malî sorumluluğu üstlenen girişimcilerin haklarının da korunması ve takip edilmesi,
- Yasal açıdan oluşturulacak güvenli bir zemin neticesinde yerli ve yabancı sermayenin fikrî yaratım alanlarına yönlendirilmesi, bilgi ve teknoloji transferinin sağlanması ve istihdam imkânlarının arttırılması,

gibi ekonomik, sosyal ve kültürel açıdan önemli sonuçlar hedeflenmektedir (Baytan, 2001).

2.3.2.5 2001 Yılında Yapılan Değişikliğin Haritacılık Açısından Değerlendirmesi

FSEK'nda yapılan son değişiklikte harita ve harita bilgilerinin giderek etkin bir şekilde kullanıldığı veri tabanlarına dair hükümler, bu konuda uluslararası asgarî hükümleri içeren TRIPS metnine (Md.5) ve ABD'nin fikrî ve sınaî haklara ilişkin gümrük indirimi uygulayacağı ülkeleri belirlemede esas aldığı Trade Omnibus Action, Section 301'e uygun olarak, içindeki veriyi korumamaktadır. Ancak, 11 Mart 1996 tarihli 96/9/EC sayılı Avrupa Parlamentosu ve Konseyinin Direktifinde yer alan ve veri tabanlarındaki verinin de; harcanan emek ve sermayenin gereği olarak korunmasını sağlayan "Sui Generis" (Kendine Özgü) hakkını içermediği görülmektedir. Avrupa Birliğine bütün mevzuatını uyumlu hale getirmeyi taahhüt eden Türkiye'nin, FSEK'de yaptığı son değişikliklere, veri tabanlarındaki verilerin de korunması hükmünü dâhil etmemesinin yapılmış bir hata olduğu, bu hatanın ise en kısa sürede düzeltilmesi gerektiği, aksi takdirde Avrupa Birliğine girmede bu eksikliğin bir engel olacağı değerlendirilmektedir.

Bundan ayrı olarak, 2001 yılında cezalara getirilen artışın büyük caydırıcılık taşıdığı ve bununda Maliye Bakanlığınca belirlenecek yıllık artışlarla caydırıcılığını koruyacağı göz önünde bulundurulduğunda, CBT kullanımında harita, CBS yazılımları, veri tabanlarına ve bunların dâhilinde sayısal coğrafi verilerinde yapılacak tecavüzlerin azalacağı değerlendirilmektedir. Ancak cezaların çok ağır bir şekilde; hem hapis (dört yıldan altı yıla kadar) hem de para cezasını (50 milyar TL.den 150 milyar TL.ye kadar) beraber içermesinin

ise tartışılması gerekir. Zira fikrî haklara tecavüzden çok daha ağır suçlara bile bu cezaların verilmemesinin, hakkaniyetli olmadığı değerlendirilmektedir.

Kurulacak ihtisas mahkemeleri sayesinde de, bu konuda yetişmiş hâkimlerin fikrî haklar konusundaki davaları daha kısa sürede sonuçlandıracağı ve daha etkin bir sistemin oluşturulacağı düşünülmektedir.

2.3.2.6 2004 Yılında Yapılan Son Değişiklik

TBMM (Türkiye Büyük Millet Meclisi)'de kabul edilen bu yasaya göre korsan yayın faaliyetleri "organize suçlar" kapsamına alınıyor.

5846 sayılı Fikir ve Sanat Eserleri Kanunu'nun daha etkin kullanımını hedefleyen değişiklik ile bu kanun kapsamında korunan eser, icra ve yapımların tespit edildiği, kitap, kaset, CD, VCD ve DVD gibi mevcut materyaller ve ileride bulunacak teknik imkânlar ile üretilecek taşıyıcı materyaller, yetkili mercilerden izin alınmış ve işgal harcı ödenmiş olsa bile sokakta satılamayacaktır.

Yasadaki bu değişiklik CBT dâhilinde CBS yazılım sektörünü de yakından ilgilendiriyor. Yasaya göre, resmi mercilerin yetki ve sorumlulukları artırıldı. Buna göre, polis, zabıta, gümrük memurları, korsan yazılım satışı yapan seyyar satıcı gördüklerinde; dağıtım, çoğalma, ithalat gibi durumlarla karşı karşıya kaldıklarında direkt devreye girerek yasal prosedürleri uygulayabilecekler.

Açılacak davalar, artık şahıs değil kamu davası niteliği taşıyacak (71.,72. ve 73. maddeler). Daha önce, telif hakkı ödenmeyen firmanın zarar gördüğü kişi veya kuruma karşı şahsi dava açma zorunluluğu vardı, şimdiyse Sanat Eserleri Hakların İhlali, kamu davası olarak ele alındığından, dava otomatik olarak açılacak. Ancak tarafların kendi aralarında anlaşması sonucu dava düşebilecek.

Suçun niteliğine göre korsan yazılım çoğaltma, organize suç kapsamında değerlendirilerek DGM (Devlet Güvenlik Mahkemesi)nin alanına girebilecek. Yani, korsan CD lerin üretimi veya ithalatı, dağıtımı, son kullanıcıya ulaştırılması, birkaç seri eylemin sonucu olarak ortaya çıktığından organize suç kapsamına alınacak. Bu gibi davalar Devlet Güvenlik Mahkemesi'nde görülecek; böylece korsanlık çok ciddi bir boyut kazanacak.

Yazılım satışı yapan yerlerin Kültür Bakanlığı'ndan sertifika alması gerekecek, sertifika sayesinde Kültür Bakanlığı denetim ve kontrollerini daha etkili yapabilecek, ayrıca kayıt dışı ekonomi önlenecek. Yerli yazılımlar bandrole tabi olurken, yabancı yazılımlar isteğe göre

bandrole tabi olacak. Sertifikalama ve bandrol çerçevesindeki prosedürler en sade şekilde yapılacak.

Yeniden düzenlenen cezalar ise şöyle: korsan yayını satan ve dağıtanlar için, 3 aydan 2 yıla kadar hapis veya 10-50 milyar ağır para cezası; hak sahibinin izni olmadan bir eseri işleyen, çoğaltan, yayan, topluma açık yerlerde gösterimini düzenleyenler için 2-4 yıla kadar hapis veya 50 ile 150 milyar arası ağır para cezası; bandrol alma hakkı olmadığı halde sahte evrak veya dokümanla bakanlık veya yetkilileri yanıltarak bandrol alanlar, bandrolü amacı dışında kullananlar için 2-4 yıl arası hapis veya 20 ile 200 milyar lira ağır para cezası; sahte bandrol yapanlar ve kullananlar için 3 ile 6 yıl arası hapis cezası veya 50 ile 250 milyara kadar ağır para cezası uygulanacak.

3. COĞRAFÎ BİLGİ TEKNOLOJİLERİNDE COĞRAFÎ BİLGİ SİSTEMİ YAZILIMLARI VE SAYISAL COĞRAFÎ VERİLERİN ESER OLARAK İNCELENMESİ

3.1 Eser Kavramı

Fikrî hukuk kapsamında ancak eser sayılabilen fikrî emek ürünleri üzerindeki hakların korunabilmesi nedeniyle eser tanımının ne olduğunu belirtmek gerekir. Eser biçimlenmiş, maddî bir varlık kazanmış olan bir fikirdir. Dolayısıyla fikir ürününün dışarı aksettirilmesi için bir araca ihtiyaç vardır (Ayiter, 1981). Aksi takdirde yalın olarak düşünce ya da düşünceler, ne kadar dâhiyane olurlarsa olsunlar, koruma kurallarından yararlanamazlar. Bir eserin özelliği, düşünce yönünden değil, düşüncelerin ifade biçiminin farklılığında ortaya koyulmaktadır. Eser sahipleri, eserlerinde ortaya koydukları düşünceler üzerinde değil, düşüncelerin anlatım biçimi üzerinde hak sahibidir (Beşiroğlu, 1999).

Koruma sadece toplumun kültürünü zenginleştiren ve ona katkıda bulunan fikrî ürünler için sağlanmalıdır. Aksi takdirde bu nitelikte olmayan ürünler için üçüncü şahısların hürriyet alanın kısıtlamak haksız ve gereksizdir (Erel, 1998).

Belirli tarih, coğrafya matematik vb. bilgileri gibi düşüncelerin ortak ürünü olan bilgiler yasal koruma alanının dışında kalırken, olaylar, durumlar ya da bilgilerin sunuşunda ya da yorumlanmasında yapılan çalışma ve emek için koruma söz konusudur (Beşiroğlu, 1999). Bir eserin özelliği, herkesin malı olan içindeki fikirde değil ifade şekli diğerlerinden farklı bulunmasında olabilir (Belgesay, 2001).

Haritalar, lügat ve rehberler gibi, özellikleri nedeniyle aynı konudaki diğer eserlere ister istemez benzerler. Bu nedenle, bu gibi eser sahipleri, eserlerinde verdikleri bilgiler için özgün kaynaklara başvurulduğunu ve alınan sonucun bir kopya ürünü olmadığını belirtmek zorundadırlar (Beşiroğlu, 1999).

3.2 FSEK'de CBS Yazılımları ve Sayısal Coğrafî Veriler Konusunda Yer Alan Hükümler

FSEK'te CBT'ye ilişkin CBS yazılımları; bir tür bilgisayar programı olarak, sayısal coğrafi veriler ise; veri tabanının bir türü olarak, yer aldığı hükümler şunlardır:

3.2.1 Bilim ve Edebiyat Eserleri Kapsamında

FSEK Madde-2, Paragraf-3'de,

“Bedii vasfı bulunmayan her nevi teknik ve ilmi mahiyette fotoğraf eserleriyle her nevi haritalar, plânlar, projeler, krokiler, resimler, coğrafya ve topografyaya ait maket ve benzerleri, her çeşit mimarlık ve şehircilik tasarım ve projeleri, mimarî maketler, endüstri, çevre ve sahne tasarım projeleri”,

FSEK Madde-2, Paragraf 1'de,

“Herhangi bir şekilde dil ve yazı ile ifade olunan eserler ve her biçim altında ifade edilen bilgisayar programları ve bir sonraki aşamada program sonucu doğurması koşuluyla bunların hazırlık tasarımları”,

3.2.2 İşlenmeler ve Derlemeler Kapsamında

FSEK Madde-6, Paragraf 10'da,

“Bir bilgisayar programının uyarlanması, düzenlenmesi veya herhangi bir değişim yapılması”,

FSEK Madde-6, Paragraf 11'de,

“Belli bir maksada göre ve hususi bir plân dâhilinde verilerin ve materyallerin seçilip derlenmesi sonucu ortaya çıkan ve bir araç ile okunabilir veya diğer biçimdeki veri tabanları (Ancak burada sağlanan koruma, veri tabanı içinde bulunan veri ve materyalin korunması için genişletilemez)”.

Sonuç olarak,

- Haritalar, kabartma haritalar, hava fotoğrafları, uydu görüntüleri, CBS yazılımları, ilim ve edebiyat eserleri kapsamında,

- CBS yazılımlarının uyarlama, derleme, düzenleme veya herhangi bir şekilde değiştirilmesi ve içindeki veri hariç olmak şartıyla Coğrafî Veri Tabanları ise işlenmeler ve derlemeler kapsamında, FSEK ile korunmaktadır.

Ancak harita üzerindeki bilgiler, Coğrafî Veri Tabanlarındaki koordinat, manyetik, gravite vb. değerler ise veri oldukları ve sahibinin hususiyetini taşıyan herhangi bir unsuru üzerlerinde bulundurmadıkları için eser sayılmamakta ve FSEK kapsamında korunmamaktadır.

26 Eylül 2004 tarihinde 5237 sayılı kanun olarak yürürlüğe giren Yeni Türk Ceza

Kanunu'nda İkinci kitap Üçüncü Kısım Onuncu Bölüm'de 243-246'ncı maddeler ile Bilişim Alanında Suçlar tarif edilmiştir.

Türk Ceza Kanunu'nda İkinci kitap Üçüncü Kısım Onuncu Bölüm Madde 243'de;

- Bilişim sistemine girme
  - "Bir bilişim sisteminin bütününe veya bir kısmına, hukuka aykırı olarak giren ve orada kalmaya devam eden kimseye bir yıla kadar hapis veya adli para cezası verilir".
  - "Yukarıdaki fıkrada tanımlanan fiillerin bedeli karşılığı yararlanılabilen sistemler hakkında işlenmesi halinde, verilecek ceza yarı oranına kadar indirilir".
  - "Bu fiil nedeniyle sistemin içerdiği veriler yok olur veya değişirse, altı aydan iki yıla kadar hapis cezasına hükmolunur".

Türk Ceza Kanunu'nda İkinci kitap Üçüncü Kısım Onuncu Bölüm Madde 244'te

- Sistemi engelleme, bozma, verileri yok etme veya değiştirme
  - "Bir bilişim sisteminin işleyişini engelleyen veya bozan kişi, bir yıldan beş yıla kadar hapis cezası ile cezalandırılır".
  - "Bir bilişim sistemindeki verileri bozan, yok eden, değiştiren veya erişilmez kılan, sisteme veri yerleştiren, var olan verileri başka bir yere gönderen kişi, altı aydan üç yıla kadar hapis cezası ile cezalandırılır".
  - "Bu fiillerin bir banka veya kredi kurumuna ya da bir kamu kurum veya kuruluşuna ait bilişim sistemi üzerinde işlenmesi halinde, verilecek ceza yarı oranında artırılır".
  - "Yukarıdaki fıkralarda tanımlanan fiillerin işlenmesi suretiyle kişinin kendisinin veya başkasının yararına haksız bir çıkar sağlamasının başka bir suç oluşturmaması halinde, iki yıldan altı yıla kadar hapis ve beş bin güne kadar adli para cezasına hükmolunur".

Türkiye'de e-devlet kapsamında oluşturulan projelere ait sayısal coğrafi verilerin paylaşım ihlali ve hırsızlığı yukarıda belirtilen maddeler ile korunmaktadır. Yine e-devlet kapsamında kurumlar arası sayısal coğrafi veri akışının güvenliğini sağlamak maksadıyla çeşitli yaptırımlar söz konusudur.

3.3 Sayısal Coğrafî Verilerin FSEK Kapsamında Korunması

Teknolojik gelişmelerin sonucunda, veri ve materyallerin toplanıp veri tabanı oluşturulması ve ticarî kullanıma sunulması, dünyada olduğu gibi Türkiye'de de yaygınlaşmaktadır. Bilgi toplumunun gereklerinden birisi de belli bir plâna göre derlenmiş, toplanmış verilerin ve bilgilerin ticarî meta olarak dolaşıma sunulması, alınıp satılabilmesidir. Bu, büyük ölçüde, veri tabanları ile mümkün olmaktadır. Veri tabanlarını oluşturmak belli bir fikrî yaratımı gerektirmektedir. Veri tabanını oluşturan veri ve materyaller, kendileri eser olarak korunmaya hak kazanmasalar da, bu veri ve materyallerin derlenip toplanmasından oluşan veri tabanı bir bütün olarak eser sayılmakta ve koruma altına alınmaktadır. Bu kapsamda FSEK'de 1995 yılında yapılan değişiklikle veri tabanları işleme olarak koruma altına alınmıştır. Daha sonra 2001 yılında yapılan değişiklikle, TRIPS Metni Madde 10/2 nin gerektirdiği şekilde "bir araç ile okunabilir ve diğer biçimdeki" ibareleri eklenmiş ve böylece derleme sonucu ortaya çıkan veri tabanlarının diğer seçme ve toplama eserlerden ayırt edilmesi sağlanmıştır (2001 yılında 4630 Sayılı Kanunla FSEK'de yapılan değişiklik hakkında gerekçe).

Veri tabanlarının korunması konusunda iki farklı model ortaya çıkmıştır.

- Birinci model, herhangi bir orijinallik veya yaratıcılık unsuru bulunmayan veri tabanlarını korumayı reddetmektedir. Bu modeli savunanlara göre, koruma, veri tabanı içinde bulunan olguların seçimi, koordinasyonu veya düzenlenmesinden doğan orijinal "ifade"ye sağlanmalıdır, ama olguların kendisine değil. Veri tabanıyla derlenen isimler, adresler, coğrafî detaylar, koordinatlar vb. miktar, nitelik ve niceliğe yönelik bilgiler sırf veri tabanına konu oluşturmaları nedeniyle ayrıca koruma kapsamına girmemelidir.
- İkinci model ise "Alın teri" veya "zahmetli iş" doktrinidir. Buna göre, herhangi bir orijinallik taşımasa bile veri tabanları ve olgusal derlemelere, bunları derlemek için gereken zahmetli ve uzun süreli çalışmayı ve yatırımı ödüllendirmek açısından koruma sağlanmalıdır. Bu modeli savunanlara göre, mevcut fikrî mülkiyet rejimleri (Eser Sahibi Hakları, ticarî sırlar, ticarî markalar, sözleşmeler) ve teknolojik koruma metotlarının kombinasyonu veri tabanlarına yatırım yapmak için yeteri kadar teşvik edici değildir. Bu modelde koruma, şimdiye kadar ki uygulamalarda koruma kapsamı dışında tutulan olgulara da genişletilmektedir.

Veri tabanları uluslararası arenada da ilgi konusu olmuştur. Veri tabanlarının eser sahibi haklarına konu statüleri, Edebiyat ve Sanat Eserlerinin Korunmasına İlişkin Bern Sözleşmesi ve Dünya Ticaret Örgütü Kuruluş Anlaşması ve GATT - TRIPs Metni tarafından garanti altına alınmıştır. TRIPs Anlaşması, Dünya Ticaret Örgütü'ne üye ülkelerin, "ister elektronik

isterse diğer formlarda olsun, muhtevanın seçim ve düzenlenmesi dolayısıyla düşünce ürünü niteliğini kazanan veri veya diğer materyal derlemeleri"ni korumalarını gerektirmektedir (Acun, 2000).

3.4 Türkiye'de Veri Tabanlarının Korunması

Türkiye'de veri tabanları 1995 yılında, taraf olduğumuz uluslararası anlaşmaların bir gereği olarak, FSEK md. 6'ya yapılan bir ilave ile işlenme olarak korunma altına alınmıştır. Söz konusu madde şöyle düzenlenmiştir: "Belli bir maksada göre ve hususi bir plân dâhilinde verilerin ve materyallerin seçilip derlenmesi soncu ortaya çıkan veri tabanları. (Ancak, burada sağlanan koruma, veri tabanı içinde bulunan veri ve materyalin korunması için genişletilmez.) istifade edilen eserin sahibinin haklarına zarar getirmemek şartıyla oluşturulan ve işleyenin hususiyetini taşıyan işlenmeler, bu Kanuna göre eser sayılır. "

Burada açıkça görüldüğü üzere, FSEK'de veri tabanları eser değil de işlenme olarak kabul edilmiş ve daha da önemlisi, veri tabanı içinde bulunan veri ve materyal tamamen koruma kapsamı dışında tutulmuştur.

Fakat FSEK'de veri tabanlarındaki verilerin korunması mümkün olmaması nedeniyle, yalnızca bilgileri otomatik olarak işleme tabi tutmuş bir sistemdeki verilerin korunması konusunda Türk Ceza Kanununun 1991 yılında yürürlüğe giren "Bilişim Alanında Suçlar" başlıklı on birinci Bab'ı işletilebilir. Ancak bu kanun maddelerinde hedeflenen amaç; eser sahibi haklarını korumak değil, bilgileri otomatik olarak işleme tabi tutulmuş sistemlerden program ve verilerin çalınmasının cezaî yaptırıma bağlı kalmasıdır.

Kanunlarda yer alan hükümler, arz talep dengesi içinde, bir ihtiyaca cevap vermek üzere düzenlenir. Türkiye'de kapsamlı veri tabanlarının yok denecek kadar az olmasının doğal bir sonucu olarak bu konudaki hukukî alt yapı da yeterli değildir. Türkiye'de Temel verilerin derlenmesi bile henüz tamamlanamamıştır. Mesela, Türkiye'de coğrafî detayların yer aldığı ulusal coğrafi veri tabanı henüz mevcut değildir.

AB'de yer alan sui generis korumanın Türkiye'de de kanunlaşması, gerek bilgi sunumuna yatırım yapan yerli ve yabancı sermayenin Türkiye'de gelişmesi ve gerek AB'ye giriş şartlarından birinin yerine getirilmiş olması açılarından bir zorunluluk olduğu değerlendirilmektedir. Bu korumanın olmamasından en çok zarar görecek sektörlerden birisi de hiç kuşkusuz, haritacılık sektörüdür.

Veri tabanlarındaki verinin korunmasının şu an için Avrupa Birliğinde uygulandığı, ABD'de de kısa bir süre sonra bu konuda bir kanunun kabulünü müteakip, bu ülkelerin uluslararası yaptırımı ile bu korumanın bir dünya standardı olacağı göz önünde bulundurulmalıdır. Ancak bu konudaki korumada, Türkiye'de bu işle uğraşan firmaların kâr etme isteği ile, kamunun veriyi paylaşma ve öğrenme isteğini bir denge içerisinde düzenlemesi gerekir.

4. CBT'DE SAYISAL COĞRAFİ VERİ KORUMA YÖNTEMLERİ

4.1 Yasal Önlemler

Fikir ve sanat eserleri kanununa göre, bir eserin (örneğin coğrafi veri tabanı veya sayısal her nevi sayısal harita içeren bir CD'nin) eser sahibinden izinsiz olarak çoğaltılması, satılması, dağıtılması, kiralanması, ödünç verilmesi veya herhangi bir şekilde ticaret konusu yapılması yasak olup, ihlali halinde 4 yıldan 6 yıla kadar ağır para cezasına hükmolunur.

Bu kanun kapsamına alınacak eserlerin korunmasına yönelik olarak, eser sahibinin adını belirtme, bandrol kullanımı, kayıt ve tescil ettirme gibi yöntemlerin yanı sıra: bu kanun kapsamı dışında üretici ve kullanıcı arasında yapılan ve yasal yaptırımı olan protokoller de yasal önlemler arasında yer alır (Taştan, 2003).

4.1.1 Eser Sahibini Belirtme

FSEK 11'nci maddesi ile; eserin aslında, o eserin sahibi olarak adını kullanan kimse, aksi sabit oluncaya kadar o eserin sahibi sayılır. Böylece, FSEK kapsamında belirtilen tüm mali ve fikri haklara sahip olur(Taştan, 2003). Coğrafi veriyi içeren materyal (örneğin CD) üzerine, üreticinin adı ile telif haklarına ilişkin bilgiler kaydedilerek eser sahibi belirtilmiş olur.

4.1.2 Bandrol

FSEK 81 inci maddesine göre "kolay kopyalanmaya müsait eserlerin çoğaltılmış nüshalarına da eser ya da hak sahibinin talebi üzerine bandrol yapıştırılması zorunludur". Bu maddeye dayanarak, eser olarak nitelenen ve bu kanun ile hakları korunmak istenen CBS verilerini içeren CD'lere eser sahibinin talebi halinde bandrol yapıştırılması zorunludur. Bu bandroller Kültür Bakanlığınca bastırılmakta ve satılmaktadır(Taştan, 2003). Kültür Bakanlığı, bandrol satışını meslek birlikleri (örneğin HKMO (Harita ve Kadastro Mühendisler Odası)) aracılığı ile de yapılabilir.

4.1.3 Kayıt ve Tescil

FSEK 13'üncü maddesi (Ek: 21.02.2001-4630/7) ile eser sahipleri, sahip oldukları mali ve manevi hakların ihlal edilmemesi, sahipliklerinin belirlenmesinde ispat kolaylığı sağlanması ve mali haklara ilişkin yararlanma yetkilerinin takip edilmesi maksadıyla eserlerin kayıt ve tescilini yaptırırlar. Böylece hangi coğrafi ürünün sahibinin kim olduğu resmi olarak belli olur. Kayıt ve tescil usul ve esasları, Türkiye'de Kültür Bakanlığınca çıkarılan yönetmelikle belirlenir.

4.1.4 Protokol

Veri üreticisi ve kullanıcı arasında imzalanan protokol çerçevesinde, verilerin üçüncü şahıslara verilmeyeceği, protokol kapsamı dışındaki uygulama alanlarında kullanılamayacağı belirtilir. Protokole uymama durumunda izlenecek yasal işlemler protokolle belirtilir. Harita Genel Komutanlığınca yaygın olarak uygulanan bir yöntemdir.

4.2 Teknik Önlemler

Teknik önlemler yasal önlemlere delil teşkil edecek şekilde "eserin sahibini kanıtlamaya yönelik teknik yöntemler" ile yasal önlemlerin yetersiz kaldığı veya uygulanamadığı durumlarda başvurulmak üzere geliştirilmiş "yetkisiz kullanımı önlemeye yönelik teknik yöntemler" dir (Taştan, 2003).

4.3 Eser Sahibini Kanıtlamaya Yönelik Teknik Yöntemler

Bu yöntemler, mühürleme (watermarking) ve işaretleme (fingerprintig) olarak bilinir. Her iki yöntem de kısmen steganografya tekniğine dayanır.

4.3.1 Steganografya

Steganografya sözcüğü Yunanca örtülü çatılı anlamına gelen "steganos" ve yazmak anlamına gelen "graphy" sözcüklerinden oluşur**.** (Huber 2002, Johnson ve Jajodia 1998). Gönderilecek bilginin veya haberin bir ses ya da görüntü kaydının içine şifrelenerek yerleştirilmesi ve alıcı tarafta şifrenin çözülerek bilgiye veya habere ulaşılması sayılabilir.

Gizli mesajın verici ve tasarlanan alıcı gibi medyatik araçlar tarafından ortaya çıkarılamadığı gizili mesajları saklama tekniğidir (Thoen, 2004).

Steganografya tekniğinde, gizli mesajlar, mesaj içine saklanır ve gizlenen bu mesajlar sadece gönderici tarafından bilinir. steganografya, kriptoğrafya (crytography) tekniğinden farklıdır. Kriptoğrafyada kriptolanmış bir mesajın varlığı açıktır: fakat steganografyada, mesajın gizlendiği bilgisi açık değildir. Örneğin, mısraların ikinci harfi ile birleştirilmesi ile gizli bir mesaj elde edilen şiir veya belli aralıklardaki harflerin birleştirilmesiyle gizli bir mesajın ileten yazı steganografya tekniğine birer örnektir.

Ayrıca, eski Yunan tarihçisi Herodot, stenografiyi şöyle anlatır: Milet'li Histiaus, bir kölenin saçını tıraş eder ve gizli bir mesajı dövme halinde kafasına işler. Kölenin saçı uzadığında,

Histiaus onu Atina'ya yollar ve kafası yine tıraş edilerek mesajın ne olduğu öğrenilir. İkinci Dünya Savaşı'nda görünmez mürekkep kullanılırken, Almanlar mikrodot sistemini geliştirmişti. Böylece, bir sayfalık yazım bir nokta haline getirilirken, alıcı aldığı mesajı yine büyütebiliyordu.

11 Eylülün planlanmasından uygulanmasına kadar geçen aşamalarda ileri teknolojik olanakların kullanıldığı görülmektedir. Bu eylem sürecinde Dünya Ticaret Merkezi, Amerikan Havayolları, Pentagonûn ve diğer dünya ülkelerinin bilgi/yönetim organizasyonunu sağlayan bilgisayar sistemlerine sızılma olasılığı göz ardı edilmemelidir. Amerikan istihbarat birimleri saldırganların e-mail ve benzeri iletişimlerinde gelişmiş şifreleme yöntemleri kullandıklarını açıkladılar. Elektronik ortamda gelişmiş steganografya teknolojisi son derece popüler olmaya başlamıştır. Geleneksel olarak şifrelenmiş yazılar kolayca fark edilirken, stegonografi, iletilecek mesajı ses veya resim dosyalarının içine saklayarak tespitini güçleştirmektedir (Büke, 2002). Örneğin Adana'dan kalkan bir uçağın kaçta Paris'te olacağı ile ilgili bir mesaj Çukurova üniversitesinin göl manzaralı bir fotoğrafının içerisine yerleştirilerek gönderilebilmektedir.

Bu tekniğin uygulanması, kullanılması ve daha iyi anlaşılması maksadıyla bu çalışmada steganografya vektör ve raster olarak iki alt bölüme ayrılmıştır. Günümüzün teknolojisinde her iki tekniği de geliştirmek ve kullanılması kolaydır. Buna rağmen kullanım alanları açısından bu tekniklere kısıtlamalar getirilmektedir.

4.3.2 Vektör Steganografya

Görüntü yardımıyla mesajları saklamanın birçok yolu vardır. Bir görüntü piksel dizininden oluşması ve gereğinden fazla detaylı bilgilerin bir bölümünü içermesi nedeniyle bir mesajı görüntü içerisine saklamak oldukça kolaydır.

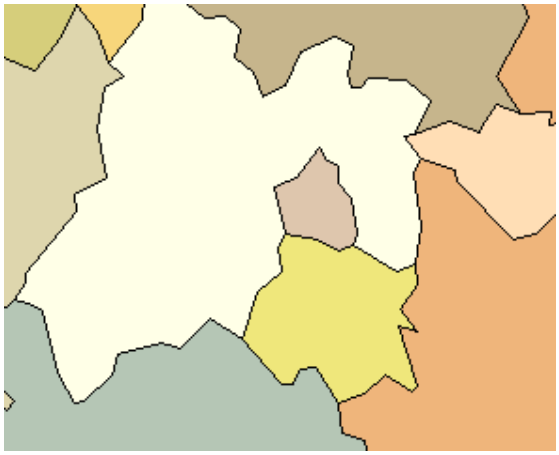
Bitmap ve diğer tüm görüntü dosyaları raster formattadır: renkli noktaların dizilişi. Bu konuda bir vektör veri içerisine gizli bir mesajın saklanması ile ilgilenilmiştir. CBS'de kullanılan veri tipi genellikle vektör yapıdadır. Vektör veriler CBS'de nokta, çizgilerin ve alan sınırlarının bulundukları konumlarını belirlemek amacıyla kullanılır.

Vektör veriye gizli bir mesaj saklamak raster veriye mesaj saklamaktan daha kolaydır. Zor şartlar içerisinde elde edilmiş coğrafi verileriyle sayısal ortamda ortaya bir ürün çıkarılır. Verinin sayısal olması kötü niyetli kişiler tarafından ürünü kullanma ve kopyalama imkânı sağlar. Vektör veriye 'watermarking (mühürleme)' tekniğini uygulayarak ürünü yapan kişi ya

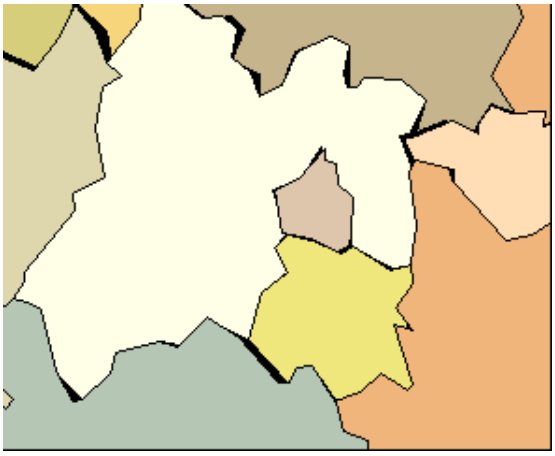
da kişileri belirlenmektedir. Kötü niyetli kişiler tarafından kopyalandığında veya kullanıldığında, bu teknik ile ürünü üreten kişi ve kişiler ispat edilebilir (Huber 2004).

Çeşitli steganografya teknikleri vardır, fakat bu çalışmada sadece **jittering** ve **embedding** teknikleri açıklanmıştır.

Jittering vektör koordinat hanelerinde anlamsız küçük değişikler içerir ve koordinat hanelerinin yuvarlanmasıyla ortaya çıkartılabilir. Örneğin bir sayı kümesi 3.142, 2.783, -1.000 olarak devam ederken birden 5.926**3125952115** sayısını görebiliriz. Bu verinin gereğinden fazla sayılardan meydana geldiği apaçıktır. Sayılar anlamsız olduğundan vektör veri üzerinde herhangi bir değişiklik olmaz. Çünkü 0.001'den küçük sayılar vektör veri için anlamsızdır.



Şekil 4.1 Meksika şehirlerinin sınır çizgileri (Huber 2004)



Şekil 4.2 Meksika şehirlerinin sınır çizgileri verteks jittering gösterimi (Huber 2004)

Şekil 4.1' de gösterilen Meksika şehirlerinin sınır çizgilerinin sıklığıdır. Şekil 4.2'de ise vertekslerin nasıl hareket ettiğini gösteren bir jittering gösterimi bulunmaktadır.

Çizgi boyunca yalancı köşe noktaları arasındaki mesafelerin kullanımı, **embedding** olarak tanımlanır. Genellikle vektör formatlı şekillerde fazladan noktalar kullanılır. Bu noktalar şeklin kendisini oluşturduğundan, görünüşü değiştirmezler. Sadece içerisindeki değişimi gösterirler. Burada bulunan iç içe noktalar, birçok gizli mesaj iletimi veya ürünün kime ait olduğunu belirten mesajlar sağlar (Huber 2004).

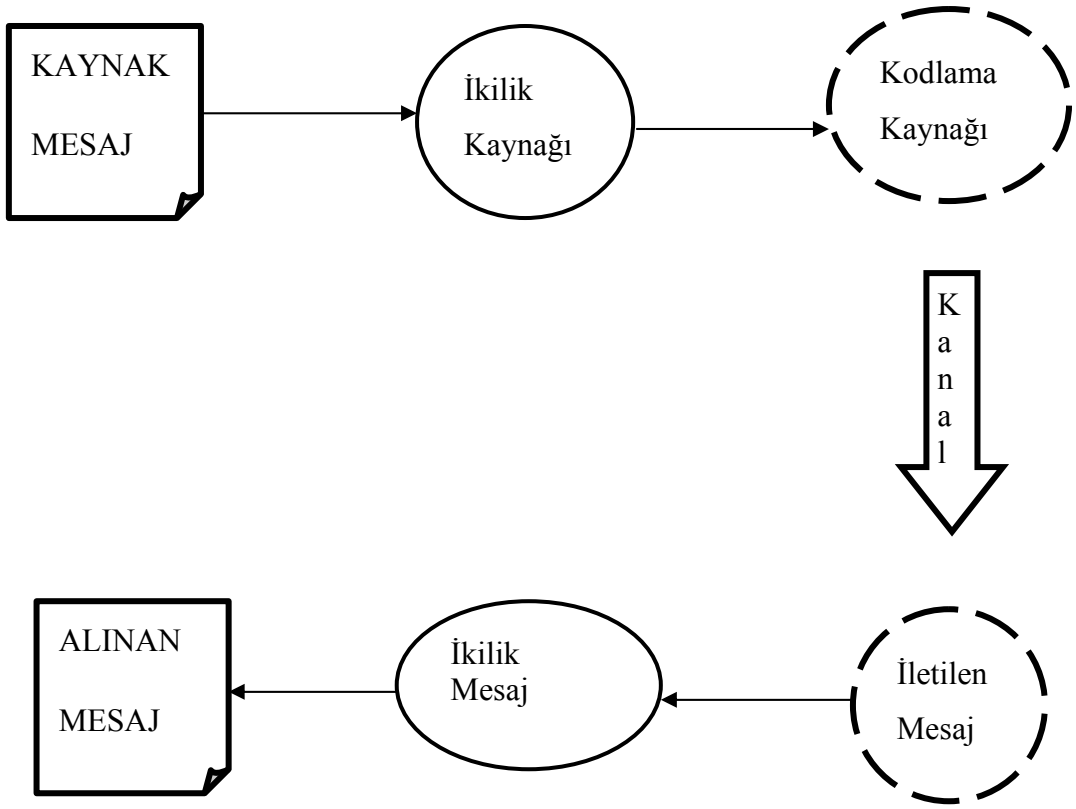
CBS uygulamalarında, vektör Steganografya için en büyük tehdit alışagelmiş çalışmaların etkileri ile uğraşmaktır. Vektör veriyi gerçek dünya özniteliğine dönüştürmek için bir CBS gösterimi olan 'georeference' (coğrafik düzlem) kullanılır. Georeference işlemi; şekil etrafındaki hareketi, onları döndürmesi, ölçeklerini değiştirmesi, şekillerin iz düşürülmesi (yeryüzü yüzeyinden harita düzlemine) ve tekrar harita düzleminden yeryüzü düzeyine iz düşürülmesidir. Bir CBS'de, şekilleri topolojik olarak tutarlı ve temiz yapmak için onları aynı zamanda değiştirebilirler. Örneğin, vertekslerin yönü ters çevrilebilir. Bütün bu çalışmalar, genellikle koordinatlarda büyük değişiklikleri ortaya çıkartırlar, bundan dolayı herhangi bir bilgiyi kaldırmak en az anlamlı sayılarda yer alır (Huber 2004).

Steganografya tekniği bir başka görüşe göre; kaynaktan alınan mesajın yoluna devam edebilmesi için kullanılan 'kanal' olarak belirtilir (Şekil-4.3). Herhangi bir kaynak alfabeden oluşan harf dizimi olabilir. Bilgisayar teknolojisinde düşünürsek 0 ve 1 den oluşan alfabeden söz edebiliriz. İki harften ibaret olduğundan dolayı bu teknik için kullanılabilecek en kolay alfabedir. Bu harfler kaynak üzerinden gönderilirse değişiklikler tahmin edilebilir. Bu işte gerekli olan işlem, kaynak mesajı iletim yoluna göndermeden önce kodlamak, hedefe ulaştığında bu kodu çözmektir. Böylelikle mesajın hedefe ulaşıncaya kadar üzerinde bir değişiklik olmadan özel bir koruma sağlanır.

Kanal hatalarını saptamak ve düzeltme yeteneği için bir bedel ödemeyi bekleyebiliriz: Kodlanan kaynak fazla olduğundan kapladığı alan da artacaktır. Bu raster Steganografya için sorun değildir, çünkü raster görüntü kaynağı büyüktür. Yüklenen bilgilerin boşluğu vektör kanal için sınırlı olduğundan öncelikle sıklaştırılmış kaynaklara ihtiyaç vardır. Ama birçok kaynak zaten iyi bir teknik kanala sahip olması için uygundur.

Birçok uygulamalarla herhangi birinin CBS verilerine ulaşabileceği gibi vektör kanal da genel amaçlı olacaktır. Mesajlar güvenli bir şekilde tutulmak istenirse, kanalın içerisindekiler ortaya çıkarılsa bile anlaşılamamalıdır. Belgelerin sahibine ait olduğu gösterilmek istenirse doğru alıcıların olduğu saptanabilmelidir. Ayrıca, güvenlik için kriptolama, belgelemek için de sayısal imza gibi bilinen, zor olmayan birçok teknik vardır. Bunun için sayısal olarak

belirtilmiş, kriptolanmış olan kaynak mesaj çözülerek alıcıya ulaşmak zorundadır.



Şekil 4.3 Kaynak kodlama (Huber 2004)

Birçok uygulamalarla herhangi birinin CBS verilerine ulaşabileceği gibi vektör kanal da genel amaçlı olacaktır. Mesajlar güvenli bir şekilde tutulmak istenirse, kanalın içerisindekiler ortaya çıkarılsa bile anlaşılamamalıdır. Belgelerin sahibine ait olduğu gösterilmek istenirse doğru alıcıların olduğu saptanabilmelidir. Ayrıca, güvenlik için kriptolama, belgelemek için de sayısal imza gibi bilinen, zor olmayan birçok teknik vardır. Bunun için sayısal olarak belirtilmiş, kriptolanmış olan kaynak mesaj çözülerek alıcıya ulaşmak zorundadır.

Vektör kanal için artık bir tane karmaşık durum kalır. İlk olarak kanal gizlenmiş iletişimi destekleseydi yapılan değişikler küçük olsa bile gizlenen görüntü değiştirilecektir. Rastgele gözükecek bir çalışma hazırlanır. İlk başta, problem değildir; çünkü herhangi iyi kriptolanmış bir kaynağı, zaten çok rasgele görünecek ve ikiliğe çevrildiğinde dahi rasgele erişimli olarak kalacaktır. Bu bağlamda, rasgele olma durumu, hata düzeltme kodlaması tarafından kaybedilecek. Bir mesajın hazırlanış işlemi gereksiz birçok yapı sinyal içerisine ilk kez

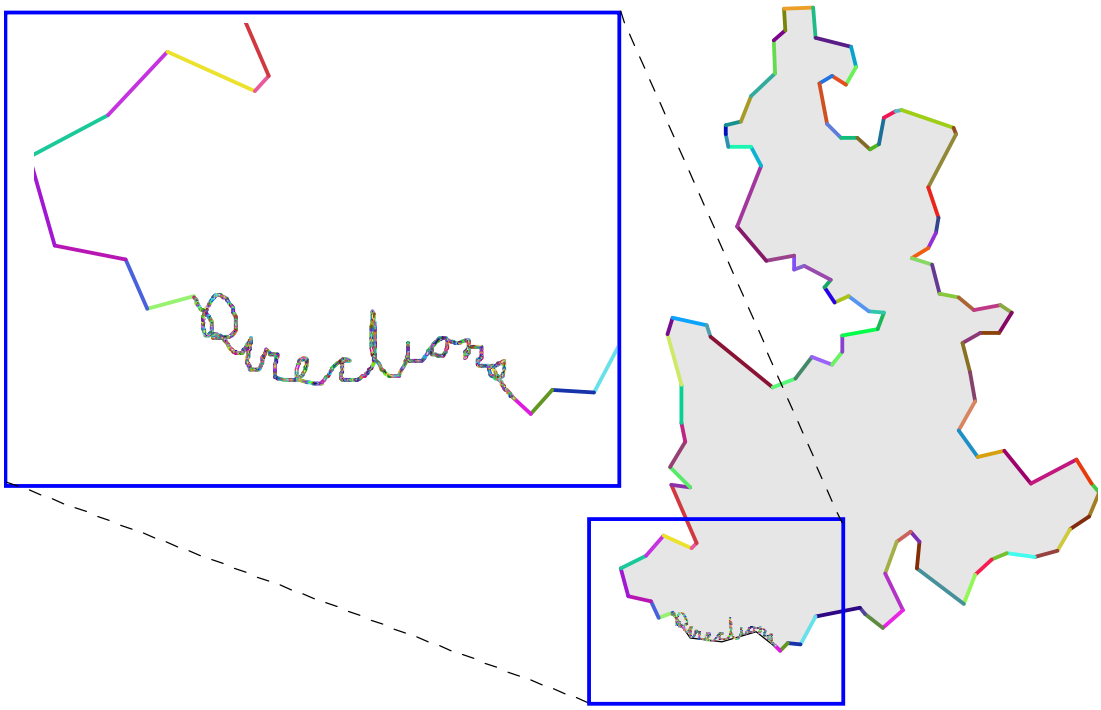
ulaşacaktır. Bu işlem, olanaklı saklı mesajlar için vektör verisi araştırma yapan bir yazılım yoluyla saptanması kolay olabilir. Bunun için, sinyalin kanala girmeden önce rastlantısal hale getirme olanağının sağlanması gerekir.

İkincisi, en zor olanıdır. Bu çok zor bir bölümüdür. Vektör şekilde yer alan mesajda olabilecek değişikliklerin çeşitleri ile uğraşmak o iletişim teorisinin uzmanlıklarından farklı olduğudur. Birçok iletişim kanalları, bazı çeşitli (telefon telleri, ağ bağlantıları, radyo dalgaları vb.) borular olabilir, bundan dolayı mesajı bit olarak gönderir. Yollar boyunca, bu yerinde duramayan parça, gürültü, kozmik ışınlar gibi, elektrik sinyallerin hangisini yakalayıp tanımanın ötesinde bazen değiştirmek ve yok etmelidir. Genellikle birçok değişikliklerin rastlantısalca olması ya da rasgele oluşması olabilecek en kötü şeydir.

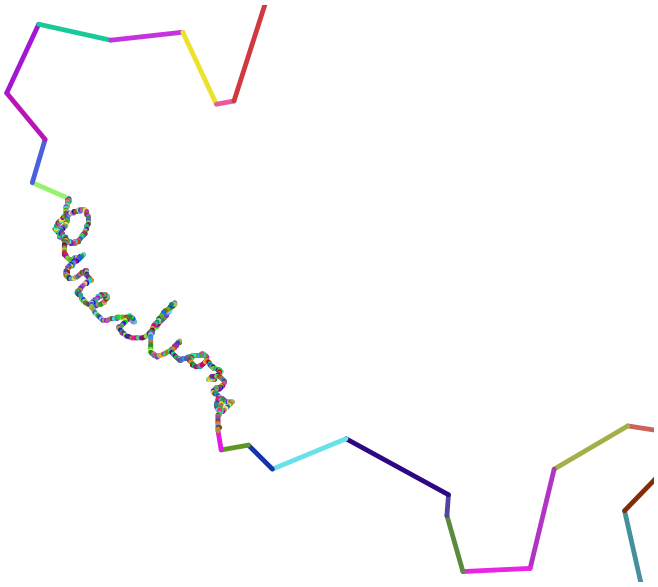
Diğer taraftan, bir vektör şekil hareket ettirilebilir, yeniden izdüşürülebilir, parçalara ayrılabilir, başka bir şekille birleştirilebilir, bulunduğu durumda çevrilir ya da eklenilen ve kaldırılan vertekse bile sahip olabilir. O zaman şeklin korunmasının zorluğu tartışılır. Eğer biri şeklin dışından bir mesaj almaya çalışıp ve onu bulup silerse, en azından değişikliği ortaya çıkartırız. Fakat diğer uygulamalarda, fikri mülkiyetin korunması gibi, belki de “yeni eser” de olan küçük ve rutin değişikler önemsenmeyecektir. Yol ve boru hatları gibi çizgi detaylar haritalarda eksiksiz olarak ölçülmek isteniyorsa, şeklin ve hassasiyetinin kurallara uygun olarak korunmalı ve projeksiyon sistemini haritaya uygun olarak seçilmelidir. Bundan daha önemlisi çizgilerin tekil parçalarını korumaktır.

Çizgi boyunca yalancı köşe noktaları arasındaki mesafelerin kullanımı **(embedding),** konumun ve uzaklığın değişmesine, açıların ve alanların değişmesine rağmen tip (shape) olarak her zaman aynı kalır. Bir vektör figürünün içinde bir mesajı yerleştirmenin diğer bir hayali yolu ise ; "El yazısı" **(Handwriting)** tekniğidir (Huber 2004).

Şekil 4.4’te gösterilen harita hangi projeksiyonda olursa olsun olsa bile mesaj tanımlanır. Burada farklı renkler içerisindeki verteksler sınırın her bir parçasını göstermektedir. Sınır çizgilerine ait vertekslerin nerede olduğu görülmektedir.



Şekil 4.4 El yazısı tekniği kullanılan bir vektör harita (Huber 2004)



Şekil 4.5 El yazısı tekniği sınır çizgisinin büyütülmüş görüntüsü (Huber 2004)

Şekil 4.5 ile gösterilen görüntüdeki renk farklılıkları ile belirtilen her bir parça renklendirildiği için köşelerin bulunduğu alan görülebilmektedir. Orijinal şekilde 112 parça içeriyordu, ancak 10 harflik bir mesaj yerleştirildiği için 853 parçalık bir vektör harita oluşmasına neden olmuştur. Bu işlem sonucu harita sınır çizgilerinde çok iyi görünmeyen ve yapılamayan kesişmeler meydana gelir.

El yazısı tekniği çok kullanışlı olmasa da karakteristik özellik olarak bir vektör steganografya gibi özelliklere sahiptir.

- Mesajı kodlayıp kanal göndermek ve tekrar çözmek kolaydır. Örneğin; mesajın(el yazısının) kanal içerisinde yer değiştirilmesi, yeniden ölçeklendirmesi gibi,
- Yeniden izdüşürülse ve bazı vertekslerin rastlantısal olarak hareket ettirilirse veya vertekslerin eklenmesiyle çok küçük parçalara ayrılsa bile kendini bu durumlara karşı korur,
- Mesajlar diğer şekillere nazaran çok küçük kıyaslamalarla gizlenebilir.

Buna rağmen el yazısının dezavantajları da vardır [3]**:**

- **Etkisizdir**: Yeni vertekslerin büyük bir kısmı karakterlerin her birisine iletmek için uydurulmalıdır.
- **Saptanması ve silmesi kolaydır**: Şeklin kıvrımlarını yumuşatma işlemi yapan herhangi bir program bütün el yazısını temizler.
- **Çizgi detayın özelliği bozulursa:** Herhangi bir yazılımda işlenen bir veri için sonradan yapılan değişiklikler coğrafi analiz için sorun olabilir.

Çizgi boyunca yalancı köşe noktaları arasındaki mesafelerin kullanımı **(embedding),** hatta çok karmaşık formda ("splined embedding") olması fark edilemez.

4.3.3 Raster Steganografya

Bu yöntemler gözle görülmeyen fakat ısı veya kimyasal yöntemlerle belli olan mürekkepler, karakter yerleştirme, sayısal imza, gizli iletişim kanalları ve örtülü spektrumla haberleşmedir.

Steganografya mesajı sakladığı için görüntüde fark edilmez. Örneğin, şifre halindeki bir yazı mesajı, eğer steganografya yöntemi ile yapılan “görünmez “ bir mesaj konmazsa alıcı verilere kolaylıkla ulaşabilir (Johnson, Jajodia, 1998).

Bu bölümde görüntü dosyalarından ve bu dosyaların içerisine bilgi saklama yollarından söz edilecek.

4.3.3.1 Image (Görüntü) Dosyaları

Bir bilgisayarda, görüntü dosyaları çeşitli noktalarda (pixels-en küçük birim eleman) en düşük yoğunluktaki sayıların dizinini temsil eder. Bu pikseller görüntünün raster verisini oluşturur. Genel olarak bir görüntü boyutu 640*480 ebatta piksel ve 256 renktir (her pikselde 8 bit). Yaklaşık olarak bir görüntü 300 kilobits veri kapsar (Johnson, Jajodia, 1998).

Sayısal görüntüler tipik olarak 24 bitlik ve 8 bitlik dosyaların birinde depolanırlar. Bir 24 bitlik bir görüntü bilgi saklamak için en fazla boyutu sağlar. Ancak, bu büyüklük olabilir. (JPEG (Joint Photographic Experts Group) görüntüleri hariç tutulursa). Tüm renk değişimleri üç birincil renk olan kırmızı (red), yeşil (green) ve mavi (blue) renklerinden türetilir. Basit bir sayısal görüntüyü ele alırsak, her temel bir renk 1 bayt ile gösterilir ve 24 bitlik bir görüntüde her pikselin için renk değerini taşıyan 3 byte'lık değerine karşılık gelir. Bu 3 byte'lar onaltılık, onluk, ikilik sistem olarak temsil edilirler. Birçok Web sayfalarında zemin renkleri altı haneli (six digit) onaltılık sayılar aslında oluşan kırmızı, yeşil, mavi renklerini temsil eder. Beyaz zemin değeri ise FFFFFF olmalıdır: (FF) %100 kırmızı, (FF) %100 yeşil, (FF) %100 mavidir. Bunların onluk sistemdeki değeri sırasıyla 255, 255, 255 ve ikilik sistemdeki değeri sırasıyla 11111111, 11111111, 11111111 olur. Üç rengin birleşiminden beyaz renk oluşur.

Beyaz zeminin bu tanımlaması, bir görüntüde tek bir pikselin renk tanımlamasıyla benzerdir. Piksellerle temsil edilmek, dosya büyüklüğüne dâhil edilir. Örneğin, yüksek çözünürlük için yaygın olan çözünürlük boyutları bir 24 bitlik görüntü, genişliğinin 1.024 piksele boyunun 768 piksel olduğu düşünülür. Bazı görüntüler 2 milyondan daha fazla piksele sahiptir ve bu şekilde tanımlanır. Buradan bir dosya içeriği 2 Mbyte'lık yer kaplar. Çünkü 24-bitlik görüntüler nispeten internet üzerinde yaygın değildir. Herhangi bir dosyayı iletmek gerekli değilse, dosya sıklaştırmak yararlı olabilir (Johnson, Jajodia, 1998).

4.3.3.2 Dosya Sıkıştırma

Kayıplı ve kayıpsız olarak iki çeşit sıkıştırma vardır. Her iki yöntem de dosya büyüklüğünü azaltır ancak gömülü bilginin etkilenmesi açısından farklı sonuçlar verirler. Bilgi kaybı olmayan sıkıştırmada orijinal mesajı tam olarak yeniden yapılandırmamıza izin verir. Bu nedenle orijinal mesaj bozulmadan olduğu gibi kaldığından bu tip sıkıştırma tercih edilir (Steganografya görüntüde olduğu gibi). Bilgi kaybı olmayan sıkıştırmada görüntü tipi GIF (Graphic Interchange Format) ve 8 bitlik BMP (a Microsoft Windows and OS/2 bitmap dosyası) dir.

Diğer taraftan, bilgi kaybını oldukça azaltır ancak, orijinal görüntünün bütünlüğünü korumaz.

Bu yöntemde JPEG (Joint Photographic Experts Group) tipi görüntüleri kaydeder. J Kullanılan kayıplı sıkıştırma algoritmasına bağlı olarak JPEG formatı, yüksek kaliteli dijital resimlere yakın sonuç verir. Bu sebepten dolayı tercih edilmektedir(Johnson, Jajodia, 1998).

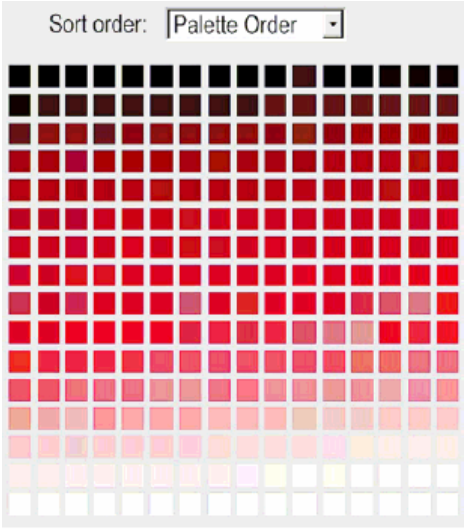
4.3.3.3 İçine Yerleştirilmiş (Embedding) Veriler

Saklanmış olan ve yerleştirilmiş bilgidir. Birincisi, örtülü görüntü olarak adlandırılan, gizli bilgileri tutan normal – gözüken- görüntülerdir. İkinci dosyalar gizlenmiş olan bilgi mesajlarıdır. Bir mesaj düz bir metin, şifre-metin ve diğer görüntüler ya da bir bit dizini içerisine yerleştirilmiş herhangi bir şey olabilir. Örtülü görüntü ve yerleştirilen mesaj birleştiğinde stego görüntüyü oluştururlar. Bir stego-anahtar (bir şifre tipi) mesajı gizlemek için kullanılır ve daha sonra mesajın şifresini çözer (Huber, 2002).

Birçok steganografya yazılımı JPEG formatını ya desteklemez veya kullanımını tavsiye etmezken, 24 bit BMP resimlerin kullanılmasını tercih eder. Diğer alternatifler ise gri tonlamalı ve 256 renk resimlerdir. Söz edilen 256 renk resimlerin en yaygın kullanılanı GIF formatıdır (Huber, 2002).

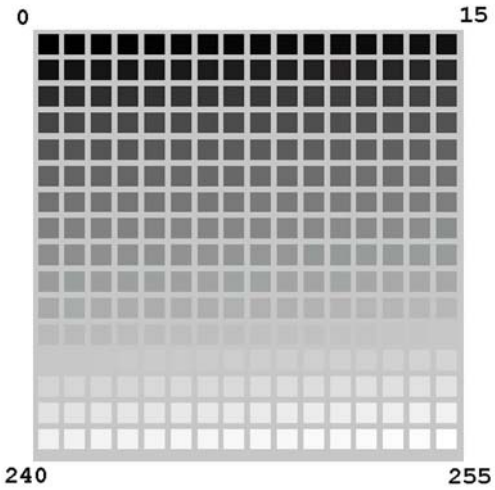
GIF formatlı resim dosyaları ve 8 bit BMP resimlerde her piksel bir baytla gösterilir. Bu tip resimler resimde kullanılan renkleri içeren 256 renkli bir palet taşırlar. Bir pikselin değeri 0 ile 255 arasındadır. Bu yazılımda seçilen rengi basit bir şekilde gösterir. Şekil 4.6'da ki kırmızı palette renk varyasyonundaki ince değişiklikleri belirtmekte olup bu renklerin çoğunun birbirleri arasındaki farklılıkları gözle görebilmek zordur. Şekil 4.7'de ise ince renk değişiklikleri gözü zorladığını görülmektedir.

Steganografi uzmanları 256 gri tonlamalı resimlerin kullanımını önermektedir. Gri tonlamalı resimlerin tercih edilme sebebi koyuluğun her değer için çok küçük farklarla artmasıdır. Şekil 4.8'de 256 tonunun gri cetvel paletini gösteriyor. Palet değerlerindeki küçük değişimler gözün fark edemeyeceği kadar azdır. Bazı gri tonlamalı resimler 4 bitliktir ve 16 farklı gri ton içermektedirler. Bu yapıdaki resimlerde değişimler daha belirgin olmaktadır.



Şekil 4.6 Kırmızı palet (Johnson, Jajodia, 1998).

Şekil 4.7 Hassas renk değişiklikleri(Johnson, Jajodia, 1998).



Şekil 4.8 Gri Ton Cetveli (Johnson, Jajodia, 1998).

Şekil 4.6 ve Şekil 4.7 gri cetvelli görüntüler Steganografya için en iyi sonucu verirken; hassas renk varyasyonu dahi çok etkili olduğunu gösteriyor (Huber, 2002).

Gri tonlamalı resimler, Steganografya için en iyi sonucu verdiğine göre ince renk değişimlerini çok miktarda içeren resimler de oldukça efektiftir. Düz renkli büyük kısımlar içeren bir resim ise iyi bir seçenek değildir. Bu düz renkli kısımlarda gömülü mesajın oluşturacağı değişimler dikkat çekici olabilir.

4.3.3.4 Sayısal Görüntülerde Gizleme

Bilgiler görüntülere birçok farklı yolla saklanabilir. Bilgileri gizlemek için, doğru mesajı araya konmalı, görüntü içerisinde bilgilerin her biti kodlanmalı ya da daha az dikkat gerektiren "gürültülü" alanlar içerisine seçici olarak mesajı yerleştirmelidir. Bunlar doğal renk varyasyonların bir hayli çok olduğu alanlardır. Mesaj görüntünün başından sonuna kadar rastgele olarak dağıtılmıştır.

Bir örtülü görüntüyü ayırmak istediğimizde yerleştirmek istediğimiz bilgiyi saklamak için bir teknik üzerinde mutlaka karar vermelidir. Gereğinden fazla olan desenler mesaj ile örtülü görüntülü arasında "wallpapers" duvar kâğıdı gibi kodlanır.

Sayısal görüntüde bilgi saklamanın birkaç yolu vardır. Genel yaklaşım olarak içeriği;

- en küçük ağırlıklı bit yerleştirme (Least significant bit insertion – LSB),
- maskeleme ve filtreleme (Masking and filtering) ve
- algoritmalar ve dönüşümler (Algorithms and transformations).

Her bir teknik, farklı görüntü dosyalarında başarılı değişken derecesi ile uygulanabilmektedir.

4.3.3.5 En Az Ağırlıklı Bit Yerleştirme (LSB)

En az ağırlıklı bit yerleştirme (LSB) örtülü dosyalara içerisine bilgi yerleştirmek için genel ve basit yaklaşımdır. Ne yazık ki, önemsiz görüntü işlemesinde bile kolayca zarar görebilir. Bir görüntüyü JPEG gibi bilgi kaybı olan sıklaştırma değil, orijinal mesajı koruyan (bilgi kaybı olmayan sıklaştırma) GIF ya da BMP gibi formatlardan çevirme yapılabilir ve geri dönüşten sonra LSB'nin içinde saklanmış olan veri yok olabilir. "LSB (Least Significant Bit) Insertion" yöntemi, örtü verisine ait segmentlerde her byte'ın en az anlamlı biti yerine gizlenecek verinin bitleri sırasıyla verinin başlangıcından itibaren birer birer yerleştirilir. Burada her sekiz bitin en fazla bir biti değişikliğe uğratıldığından ve eğer değişiklik olmuşsa da değişiklik yapılan

bitin byte'ın en az anlamlı biti olmasından dolayı, ortaya çıkan stego verisindeki (= örtü verisi + gömülü veri) modifikasyonlar insan tarafından algılanamaz boyuttadır.

4.3.3.6 24-Bitlik Görüntüler

Bir 24-bit görüntünün her bir byte LSB'nin içerisinde bir görüntüyü gizlemek için her bir piksel için 3 bit yer depolamak gerekir. "A " 1024*768 görüntü bilginin toplam 2.359.296 bit (284.912 byte) saklar. Herhangi bir görüntüye yerleştirmeden önce gizlenmesi için bir sıkıştırma yaparsak, bu bilgi büyük yer kaplayabilir. İnsan gözü sonuçta oluşan stego-görüntüyü aynen örtülü görüntüymüş gibi algılayacaktır.

Örneğin; A harfi üç pikselin içine saklanmış olabilir (sıkıştırılma yapılmadan). 3 piksel (9 byte) olan orijinal raster görüntü için

(00100111 11101001 11001000)

(00100111 11001000 11101001)

(11001000 00100111 11101001)

olabilir.

A için ikilik değeri 10000011 (bit değerleri). 3 piksel içerisine A için ikilik değer yerleştirilmesiyle şöyle bir sonuç elde edilir.

(00100111 11101000 11001000)

(00100110 11001000 11101000)

(11001000 00100111 11101001)

Şunu belirtmek gerekir ki; bitler 8 byte içerisinde kullanıldığında sadece üç gerçek değişiklik vardır. Ortalama olarak, LSB görüntü içerisindeki bitlerin yarısını değiştirmesini gerektirir. Sondaki bitin 1 veya sıfır olması sayının değerini çok fazla değiştirmeyecektir. Sondaki bit değerimiz 1 yerine 0 olsaydı bu, renk üzerinde gözle görülecek büyük bir değişikliğe neden olmayacaktı. İşte bu sondaki bitimiz LSB olarak adlandırılır. Bu bitler yerine bizim gireceğimiz verileri girilirse gizlenmiş olabilir. Orijinal resimle içerisine veri sakladığımız resim arasında gözle görülür bir fark yoktur.

4.3.3.7 LSB uygulaması

Steganografya yazılımları saklanmış bilgileri algılanmaz hale getirmek için LSB yerleştirme

işlemine tabi tutulur. Bu yaklaşım oldukça iyi bir gri tonlamalı bir görüntü sunar ve görüntü içerisinde renklerle ilişki kurmaya çalışır.

S-tools diğer bir steganografya aracıdır. Örtülü görüntülerde değişik bir yaklaşım vardır. Bu görüntüler ortalama radikal renk değişimleridir. 24-bit görüntü ile pikselinde değişiklikler yaparak yeni renkler yaratılabilir (Bu oluşan yeni renkler 8-bit görüntüye eklenmez çünkü palet sınırı vardır). S-Tools görüntü kalitesini korumaya devam ederken renk sayısını azaltır. Bundan dolayı LSB değişiklikleri renk değerlerini değiştirmesinde zorlayıcı değildir.

Örneğin; Sekiz renk değeri her bir renk değeri için 000 değeri eğer 111 olarak depolanması gerekiyorsa, tek renk değerini 32 için kesinleştirmek ya da bunu kullanmak renk sayısı olan 256 (256/8=8) sayısını aşmayacaktır. Paletteki 32 tek renklerin her biri 000'dan 111 'e dizili RGB renklerine sahip olan sekiz renge genişletebilir. Bu sonuç aynı görüntüyü verir fakat bir bit tarafından değişebilir. Bu araçlar gri tonlu görüntülerle aynı yaklaşımı içerir. Örneğin; normal gri tonlu bir görüntü içerisinde beyaz RGB ile siyah renge kadar hareket ettirilecek

(255 255 255), (254 254 254), ...

(1 1 1), (0 0 0)

S-Tools ile işleme sokulduktan sonra beyaz için değer 8 renge yükselerek,

(255 255 255), (255 255 254) ve (255 254 255)

gibi olacaktır.

4.3.3.8 Maskeleme ve Filtreleme

Maskeleme ve filtreleme tekniği gri tonlu ve 24-bit görüntüleri genel olarak sınırlandırır. Küçük farklılıklarla mühürleme yöntemine benzer, bir görüntüye iz bırakarak bilgiyi saklar. Mühürleme teknikleri, bilgi kaybı olan sıkıştırma yüzünden onların daha çok, görüntü ile bütünleştirildiği için görüntünün kaybolma korkusu olmadan uygulanabilir.

Görülebilir mühürleme steganografya tanımlaması değildir. Birinci farklılık amaçlarıdır. Geleneksel steganografya bilgileri gizli tutar: mühürleme bilgileri kapsamını büyütür ve örtülü görüntü özelliğini getirir. Sayısal mühürleme eser sahibinin hakları, mülkiyet hakları ya da lisans gibi bilgileri kapsar. Steganografyada iletişim nesnesi saklanılan mesajdır. Sayısal mühürlemede iletişim nesnesi ise örtüdür.

Sayısal görüntü parlaklığında küçük oynamalar yaparak bu görüntü içerisinde düz bir metin

ve kodlanmış bilgi kullanılabilir (Şekil 4.9). Parlaklığın %15'ini göstermez. Maskeleme LSB yerleştirmesinden sıkıştırma, kısaltma ve görüntü işlemlerinde daha duyarlıdır.

Şekil 4.9 Mühürleme ile tasvir edilmiş görüntü

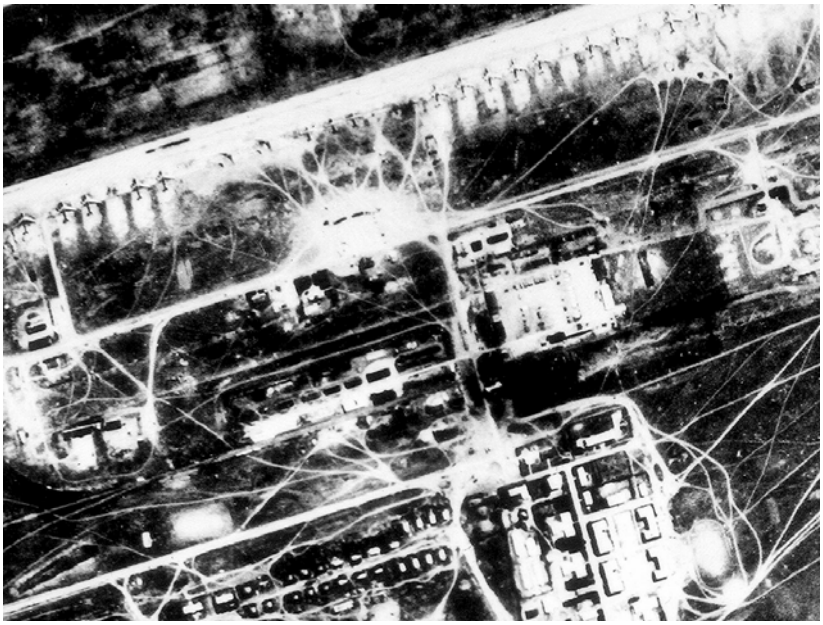
4.3.3.9 Algoritmalar ve Dönüşümler

LSB işlemesi bilgi saklanması hızlı ve kolaydır. Fakat bu işlemin sonucunda görüntüde küçük değişiklikler ya da sıklaştırma esnasında bilgi kaybı meydana gelir. JPEG görüntüler diğer formatlara göre daha avantajlıdır. JPEG kullanarak sıklaştırma yapılması yüksek kalitede verilerin toplanmasını sağlar. JPEG görüntüler internet üzerinde çok tercih edilen formatlardır. Örtülü mesajları ve mesajların birleştirildiği yazılımlar JPEG algoritmalarını kullanarak bilgi kaybolan JPEG stego-görüntü yaratırlar.

Diğer bir teknik ise saklanmış bir veriyi görüntü içerisinde şifrelemek ve dağıtıp gözden kaybolma teknikleridir. Bu dağıtmayla mesajlar bir gürültü gibi ortaya çıkar. Bu yaklaşımı öneren kişi varsayım olarak; mesaj parçası seçilmiş ise algoritma ve stego-anahtar (şifre anahtarı) kullanmaksızın bu parçaları kodlayabilir. Örneğin belirli frekansları kapsayan gürültülü ses (White Noise Storm-WNS) aracı spektrum teknoloji ve frekans beklentisine dayanır. WNS içerisinde rasgele sayılar olan sekiz kanallı bir önceki pencere büyüklüğünü ve veri kanal tarafından üretilmiştir (anlaşılmıyor). Her bir kanal 1 bit büyüklüğündedir, bundan dolayı her bir görüntü penceresi 1 bytelık bilgiyi ve birçok kullanışsız parçayı tutar. Bu parçalar çeşitli bit permütasyonlarında bulunabilir.

Örneğin; 1 bit, 7 bit ile yer değiştirebilir ya da her ikisi de sıra ile pozisyonlarını değiştirebilir. Yer değiştirmenin kuralı stego-anahtarı ve bir önceki pencerenin rastgele olan veriyi kabul ettirmektir.

İkinci bir mesaj dosyası uydu görüntüleri olabilir. Şekil 4.10'da uydu görüntüsü görülmektedir.



Şekil 4.10 Uydu görüntüsü

Şekil 4.11 Renior örtülü dosya örneği

4.3.4 Değerlendirme Örnekleri

Bu bölümde değişik steganoğrafik paketler değerlendirilmiştir. Paketler:

- StegoDos
- White Noise Storm (belirli frekansları kapsayan gürültülü ses)
- S-Tools for Windows (Windows steganografik araçları)

4.3.4.1 StegoDos

StegoDos herkesin kullanabileceği halka açık bir yazılımdır. Sadece 256 renkli 320*200 piksel görüntüler için geliştirilmiştir. Mesaj şifreleme ve şifre çözme gibi birçok aşamayı kapsar, bundan dolayı orijinal dosyalar taranır ve dosyalar değiştirilir. İstenilen büyüklükte olmayan görüntüleri içerisine metin mesajını gizlemek için 320*200 piksel görüntülere uygun hale getirmek zorunludur (Johnson, N.F., Jajodia, S., 1998).

StegoDos'ta mesajı saklamak için LSB yöntemi kullanılır. Bu kullanım ise diğer araçlardan daha başarılı değildir. StegoDos dosya sonundaki karakteri mesajın sonuna ekler. Fakat EOF (dosya sonu) karakteri bile mesajı dosya sonunda oluşan artığı kapsaması gibi değiştirilen görüntülerden tekrar geri düzeltir.

4.3.4.2 Belirli Frekansları Kapsayan Gürültülü Ses (White Noise Storm)

White Noise Storm, DOS için çok etkili bir Steganografya uygulamasıdır. Kolayca örtülü görüntülerin içerisine metin mesaj yerleştirilebilir ve bozulma olmayan yerler saptanabilir. White Noise Storm Renior örtülü görüntü içerisine havalanı yerleştirildi. Ancak, şekil 4-13'te görüldüğü gibi çeşitli yeri değiştirilmiş palet görüntünün, görüntü bütünlüğüne gürültü karışması gibi birçok sorun vardır (Johnson, N.F., Jajodia, S., 1998).

Şekil 4.12 WNS İle havaalanı yerleştirilmiş renior örtülü görüntüsü

Şekil 4.13 S-Tools ile havaalanı yerleştirilmiş renior görüntüsü

Şekil 4.14 S-Tools ile 248 den 32 tek renge düşen örtülü görüntü

White Noise Storm görüntü içerisindeki parçalar rastgele şifreler. Yazılım LSB yaklaşımı ile kullanılır ve bu metot IBM (International Business Machines) paintbrush (PCX) dosyalarına uygular. Yazılım örtülü görüntüden LSB'leri seçer ve onları bir dosyada depolar. Mesaj şifrelenir ve yeni bir LSBs kurumu yaratmak için bu parçalar uygulanır. Düzeltilmiş parçalar yeni bir stego-image yaratmak için örtülü görüntü içerisine enjekte edilir. Bu yöntemin en önemli dezavantajı bilgiyi tutmak için kullanılan birçok parça kaybı olur. Bu ise Steganografya için istenilen durum değildir.

4.3.4.3 S-Tools

Windows için S-Tools kullanılan Steganografya araçları arasında çok yönlü olanıdır. GIF ve BMP görüntü ve ses WAV (Waveform) dosyalarında işlem yapılabilir. S-tools bilgiyi diskte kullanılmamış alana dahi saklayabilir (Johnson, N.F., Jajodia, S., 1998).

S-Tools LSB metodu, hem görüntü hem de ses dosyalarında kullanılmasına rağmen haritacılık için görünü dosyalar önemlidir. Kullanıcı mesajı istenilen mesajı sakladıktan sonra yazılım yeni bir stego-image gösterir ve kullanıcı yeni oluşan görüntü ile orijinal görüntü arasında bağlantı yapabilir. Bu durumda görüntü kötüleşir. Ancak stego-image kaydedildikten sonra yaklaşık olarak orijinal görüntüsüne ulaşır. Bu bozulmuş görüntüler hafıza sınırından

kaynaklanır ya da S-Tools'da bir hata vardır. Ara sıra kaydedilen görüntü hata ve düzeltmelerle bozulmuş olur veya okunmayabilir.

S-Tools veriyi şifrelemek ve saklamak için birçok alternatif sağlar. Bu işlemi sağlayan en iyi görüntü 24-bit görüntülerdir. Buna benzer örnek şekilde mevcuttur. Orijinal görüntü 195.891 tekil renge sahipti, ancak sonuç olarak stego-image 312.340 tekil renk içermektedir. Fakat çıplak gözle bakıldığında bu görüntüler aynı görünmektedir [1].

S-Tools işleyicileri GIF dosyaları gibi 8-bit görüntülerde sadece bir bit farklıdır. İki seçenek vardır: 24-bitlik görüntü ile kuvvetlendirmek ya da renk azaltması. 24-bitlik görüntü ile kuvvetlendirmek örtülü görüntüyü 8-bit görüntüyü 24-bitlik görüntüye dönüştürmektir. Sonuç olarak aynı görüntüyü verir.

5. MÜHÜRLEME, İŞARETLEME VE SAYISAL İMZA

Mühürleme, işaretleme ve sayısal imza ile yaratılan teknolojilerin özelliklerinin ve yeteneklerinin ve dolayısıyla sayısal bilgi kaynaklarının sanat eserleri haklarının korunması sağlanacaktır.

Mühürleme ve işaretleme sayısal nesne içerisinde yerleştirilmiş güvenlik bilgilerini içerir. Bunlar; mülkiyet ve lisanslı kullanıcının kimliğinin belirlemesini sağlar. Bu bilgi belki anlaşılabilir (arka plan görüntü gibi) ya da daha konvansiyonel olarak görülemez. Bu teknoloji sanat eserleri sahipleri için çekiciliğe sahipken, güvenlik mülkiyeti için sınırlıdır.

'Sayısal imza' kamu anahtar gizli sistemin yeteneğinin (capabilities of public key cryptosystems-PKCS) biri için kullanılan terimdir. İmza görevi sağlar (asıl kimliğini temsil etme), bu teknoloji güvenlik ve dürüstlük hizmeti sunar. Bu hizmet güvenilirdir ('sağlam' kriptoğrafya teriminde), fakat bu teknoloji veri nesnelerini düzeltme ortamı için tasarlanmamıştır. Bu bölümde eser sahibi haklarının korunması ve bu hakların bilimsel kullanımı içinde yer alan diğer konular ele alınmıştır (Sandy, 1998).

5.1 Mühürleme, İşaretleme ve Sayısal İmza Tekniklerine Genel Bakış

Web teknolojilerinin kullanımında önemli gelişmelerle birlikte ve özellikle e-devlet kapsamında sayısal dokümanlara kolayca erişilmesi ve işlenmesi söz konusu olmaktadır. Bu nedenle üretilen sayısal kaynakların akademik ve kurumlar arası paylaşımı sırasında sayısal veri sahibinin haklarının korunması (veri mülkiyet sahibinin) için bazı yasal ve teknik tedbirler alması gerekmektedir. Bu bölümde bu tedbirler teknik olarak incelenmiştir.

Yeni bilgi teknolojisinin sayısal bilgiye girişini kolaylaştırması, sanat eserleri haklarının korunmasına yönelik yasanın varlığı (yasal olmayan kopyalama ve kullanma) sayısal coğrafi veriler için de bu tür tedbirlerin alınmasına ön ayak olmuştur. Asıl mal sahiplerin eserlerinin bir ağ üzerinde kullanımın güvenliği de belli yöntemlerle sağlanmalıdır (Sandy, 1998).

Mühürleme ve işaretleme gibi bazı teknolojiler eser sahibine görünürde korumayı sağlar. Ancak yasa ise veri korsanlığının önlenmesinde caydırıcılık sağlar. Kriptografi ve sayısal imza veri sahibinin kimliğinin belirlenmesini sağlar [6].

5.1.1 Mühürleme (Watermarking)

Mühürleme yönteminde, telif hakkına ilişkin olarak eser sahibine ait bilgiler, sayısal veri içerisine yerleştirilir. Bu bilgiler gizli olarak yerleştirileceği gibi, raster haritalarda, raster haritanın kalitesini, okunabilirliğini bozmayacak nitelikte saydam fakat anlaşılabilir nitelikte geri plan görüntüsü şeklinde de olabilir (Sandy, 1998). Buna benzer olarak televizyonlarda ilk kez gösterilen. Filmlerde televizyon kanalının logosunun belli belirsiz eklenmesi şeklinde de uygulanmaktadır.

Mühürleme yöntemi ile sahibi belirlenmiş bir veri seti yetkisiz kullanıcılar tarafından ele geçirildiğinde; eser sahibini koruma haklarına ilişkin bilgilerin veri seti içinde saklanması yöntemi ile sahibinin adı ispatlanabilmektedir.

Damgalama yöntemlerinin geliştirilmesinde, sayısal çalışmalara damgalanan bilginin çeşitli saldırılara karşı dayanıklı olması öncelikli amaç olarak göz önünde tutulur. Ancak steganografya uygulamalarında böyle bir beklenti yoktur.

5.1.2 İşaretleme

Mühürlemenin bir başka şeklidir. Sahibine ait eserin üzerine seri numarası yazılması ve bu şekilde kullanıma sunulması (veya satılması) yasal olmayan kullanımı veya satışı önlemektedir. Bir sayısal çalışmanın belli bir müşteriye dağıtılma öncesinde, telif haklarının korunması amacıyla, yalnızca o müşteriyi temsil eden bilginin çalışmaya görünmez bir şekilde damgalanması işlemidir. İşaretleme parmak izi ve etiketleme olarak ikiye ayırabiliriz. Etiketleme için kullanılan yöntemde bilgi, dışardan yapılan çeşitli saldırılara karşı dayanıklıdır. Böylece her müşteriye, içinde kendisine özel bir bilginin saklandığı bir ürün verilir (ARNOLD ve ark, 2003). Parmak izi ekleme, amaç bakımından sayısal damgalamadan farklı ancak yöntem olarak sayısal damgalama ile aynı özellikler gösterir.

5.1.3 Sayısal İmzalar

Elektronik imza; bir bilginin üçüncü tarafların erişimine kapalı bir ortamda, bütünlüğü bozulmadan (bilgiyi ileten tarafın oluşturduğu orijinal haliyle) ve tarafların kimlikleri doğrulanarak iletildiğini elektronik veya benzeri araçlarla garanti eden harf, karakter veya sembollerden oluşur.

Mühürleme ve işaretleme teknikleri ‘veri saklama’ tekniği olan steganografya ile yakın ilişkisi vardır. Sayısal imza tekniği mülkiyet içeriği nedeniyle kriptoğrafya alanına aittir. Sayısal imzalama, kişisel ve kamusal anahtarın kullanıldığı damgalama olarak tanımlanabilir. Bir

kişisel anahtar ile imzalanan doküman, sahibi hakkında bilgi de birlikte taşımış olur. Bazı otoritelerin, sayısal damgalama ile sayısal imzalamanın eş anlamlı olduğuna dair görüşlerine karşın bunları birbirinden ayrı tutan görüşler de vardır (MOHANTY, 1999).

Uygulamada sayısal dokümanların imzalanması için çeşitli yazılımlar mevcuttur. Her kişi için oluşturulan kamusal ve kişisel imzalar, kendisine elektronik kartlarda verilir. Bu konuda, birçok yerde yasal düzenlemelerin ve teknik altyapının henüz sağlanmamış olmasından dolayı kullanımı yaygın değildir. Sayısal imza kullanılarak, gönderilecek dokümanın bütünlüğü sağlanır, göndericinin kişisel imzası kullanılarak şifrelendiğinden gönderici tarafından inkâr edilemez ve göndericinin imzası taklit edilemeyeceğinden belirtilen göndericiden geldiği kesindir. Alıcı kendisine ait kamusal anahtarı kullanarak bu dokümanı açar, ancak göndericinin kişisel anahtarı olmadan üzerinde değişiklik yapamaz (TOPALSAN, 2004).

5.2 Mühürleme ve İşaretleme Tekniklerinin Kapasiteleri

5.2.1 Yaratıcının Kimliğinin Belirtilmesi (Mühürleme)

Bu hizmet orijinal verileri yaratana verinin mülkiyet iddiası için delil sağlar. Ancak bu iddia yeterli değildir. Mülkiyetin yetkili bir kurum (ya da kişi) tarafından doğrulanması gerekmektedir (Buke, 2004, Cotex all 1996).

5.2.2 Alıcı Kimliğinin Belirtilmesi (İşaretleme)

Veri sahibinin gönderdiği alıcının da belirlenmesi gerekir. Aksi halde kimliği belli olmayan alıcı veriyi üçüncü şahıslara verebilir.

Mühürlemede güvenlik bilgisi sayısal nesnenin her yerine görünümü bozmayacak şekilde yerleştirilir. Taşınabilen güvenlik bilgisini maksimize ederek, yerleştirme yaklaşımı mühürlemenin belirtilmesine izin verir ve orijinal nesnenin izole edilmiş örneğinin nerede kullanıldığını belirtir. Birçok uygulamada mühürleme tekniğinin amacına ulaşması için tamamlanması güçtür (sıkıştırma). Mühürleme tekniği kolayca zarar görebilir, bu da eser sahibin haklarını korumada sınırlı destek sağlar.

- **Asıl kimlik denetimi:** Orijinal veri alıcıya tanıtılırsa doğruluk ispatlanmış olur.
- **Memnun gizlilik:** Üreticiye kolaylık sağlayan bir uygulamadır. Üreticinin sunduğu hizmette malın kendisine ait olduğunu belirten bir mühür bulunmaktadır. Kullanıcı sunulan hizmetin sahibini görmesini ve bilmesini sağlar.

- **Bütünlük hacmi:** Ürünün elde edilmesinde kullanılan verilerin kimlik doğrulamasını sağlar. Böylece alıcı ürünü kullanırken elde ettiği verilerle ürün sahibinin haklarının bütünlüğünün korunmasını sağlar.

- **Kaynak olan ret olmayan:** Verilerin bütünlüğü korunur, yaratıcının belirlenmesinde bir mesajla veya işaretle alıcıya önemli bir delil sunar.

5.3 Sayısal Mühürleme Uygulamaları

Birçok mühürleme teknikleri sadece teknik bakış olarak ele alınmış olarak literatürde geçmiştir. Çoğu kez, teknolojinin gerçek amacı gözden kaçırılmıştır. Mühürleme tekniği aşağıda açıklanan uygulama alanlarıyla ilgilidir [4].

5.3.1 Mülkiyeti İspat Etmeyi Sağlayan Uygulamalar

Mühürlemenin başlıca kullanımı sayısal verilerin korunması adına, nesnenin sanat eserleri haklarının mülkiyetine yetkili kurumla yardımcı olunmasıdır.

5.3.2 Müşterek Olarak Çalışan Kopya Koruması Uygulamaları

Bazı verileri korumaya yönelik uygulamalar çok karmaşıktır. Buna örnek olarak seri kopya yönetim sistemidir. 1980'li yıllarda ortaya çıkmıştır. Satmış olduğu kayıtların tek sayısal ses bandı hazırlamak için bir kullanıcı seçildi.

Yakın geçmişte üretilen elektronik ve sayısal verilerin çok yönlü sayısal disk (Digital Versatile Disc-DVD) için kopya yönetim planı düzenlenmiş, ancak kısa sürede bunların kopyalanması ve üretilmesi de kolaylaşmıştır.

5.3.3 Uygulamalar İçin Veri Bütünlüğünün Kontrolü

Bu uygulamaların verilerin orijinliğini gösterebilen ve bütünlüğünü ispatlayan güvenceye sahip olması gerekir. Örneğin bir sayısal görüntü değiştirilmediği sürece mahkeme için delil sağlayabilir.

Mühürleme veri bütünlüğü içerisinde verinin orijinalliğini ispatlamada etkin değildir. Veriler içinde başkaları tarafından esnek küçük değişiklikler yapılabilir (tonlama düzeltmesi, kırpma gibi). Ya da daha büyük değişiklikler yapılarak mühürleme iptal edilebilir. (görüntüden bir şeklin çıkarılması gibi).

5.3.4 Notlarla Açıklama Uygulamaları

Bu uygulama alanlarında, mühürleme belirli nesne bilgileri (“detay kodu” ya da “tipi”) nesne kullanıcılarına devredilir. Örneğin, görüntü içerisindeki detay etiketlenebilir ya da bütün görüntünün tipi belirlenebilir. Önemli ve gerekli bir görüntünün içinde bu teknik kullanılabilir.

Farklı teknikler görüntü tiplerine göre şifreleme formatının kullanımını gerektirir. Örneğin, algoritma sıklaştırması dönüşüm tipindedir.

5.4 Görünmez Mühürleme İçin Genel Çerçeve

“Görünmez mühürleme ” terimi insan algılamasında anlaşılabilir. İçerisine numaralar saklanmış renk körlüğü teşhisinde kullanılan test kartlarını örnek verebiliriz. Dolu renk görüşü olarak algılanabilir, fakat renk körü olan bir kişi için görünmez.

İnsan algılama sisteminin çeşitli özelliklerinden yararlanarak şifreleme yöntemi ile görüntü belirsiz hale getirilir. Mesele insanın algılayabileceği görüntüye bazı işaretler yerleştirilebilir. (Buke, 2004, Cotex all 1996)

5.5 Sayısal Mühürleme Kullanımın Faydaları ve Zararları

Sayısal mühürleme basılı nesneler üzerinde geleneksel mühürleme görüşüne benzer sayısal nesne özelliklerini uygulanmasını sağlar. Kâğıt mühürleme; kâğıt bulamaç nem çıkarması için çerçeveler arasında basıldıktan sonra kalıbından ayrılarak üretim sürecine girmesiyle ilk olarak üretilmiştir. Bunlar çeşitli zamanlarda üretici ticari marka kaydı ve kâğıt niteliğinin onaylanmasında kullanıldı. Bugün, birçok ülke nakit para kâğıdı mühürlemesinde sahtekârlığa karşı kullanıyor. Bununla kusursuz bir korunma sağlanamazken, sahtekârlık yapılması da oldukça zordur.

Mühürlemenin silinmesi zordur. Yeni bir mühürleme eklemek zordur. Mühürleme filtreleme, sıkıştırma, tekrar örnekleme, kırpma, gürültülü kanal, sayısal/ analog dönüşüm ve insan yapılarını işleme tabi tutulan diğer sinyallere benzer rutin dönüşümleri daha uzun ömürlü tutar. Saldırı olan ünlü formlara karşı delil olur (gizli antlaşmalara saldırı, aynı içerikli birçok sürümün nerede olduğu, farklı mühürlemelerle damgalananların karşılaştırılması).

Mühürleme göze çarpmaz ve nesnenin uygun kullanımına engel olmaz. Mühürleme orijinal veriyi belli bir kısmını kapsar. Mühürleme görülemediği için bir hırsız yasadışı kopyalamanın varlığından haberdar olamayacaktır. Mühürleme görülebilmesiyle anlaşılabilir, böylece

çalınan veri setinin ticari değeri azalır.

Görünen ve gelişen teknolojiyle birlikte her alana ve farklı veri nesnelerine değişik tekniklerde mühürleme uygulanabilir. Hangi nesneyi ele alıyorsak ona ilişkin analiz ve araçlar kullanılır, çeşitli teknolojik çözümler getirilir.

5.6 Temel bilgi saklama

Uluslararası şirketler veri saklama (güvenliği) üzerinde bazı terminolojileri kabul ederek basit kavramları açıklamışlardır (Belgesay, 2001). Açık ve kesin veri girişi ya da "örtülü" bilgiyi gizlemek için birleştirilmiş nesne (ses, görüntü, video ya da metin), "gömülü" nesne (mühürleme ya da işaretleme), bir "stego" nesne üretmek. Veri yerleştirme işleminde veri sahibinin bilmiş olduğu bir gizli "anahtar" kullanılır ya da bir kişi tarafından diğer kullanıcılara paylaştırılır (detektör fonksiyonu gibi).

Veri saklamanın kullanımı ve kullanma şeklinde değişiklikler içermesinden (askeri şartlar ve suçlarla ilgili) (Bender, 1996), dolayı asıl önemli olan, sayısal ürünlerin telif haklarının korunması için uygulama yapmaktır. Mühürleme tekniği veri sahibinin işareti ile bir veri setinin bütün kopyalarını işaretleyerek, mülkiyeti ve telif hakkının mülkiyetini ispat etmeye yarayan bir mekanizma sağlar. İşaretlemede ise, veri setini satın alan her bir müşteri için tek, kendine özgü bir işaret yerleştirilir. Bu kanunlarda; gizlenmiş bir seri numarası konulabilir ya da nesnenin kopyalanmasından sorumlu üçüncü kişinin kimliğinin tanımlanması sağlayan ve veri setinin mülkiyetini belirten bir işaret yer alabilir.

Yerleştirilmiş (gömülü) veri hacmi, mühürlemenin sağlamlığı ile yer değiştirilerek elden çıkarılabilir. Verilen bir veri saklama metodu ya yerleştirilmiş yüksek veri hacmi ya da sinyal dönüşümüne ya da sıkıştırılmasına yüksek direnç sağlar. Uygulamanın şartlarına göre, istenilen bir ya da bu özelliklerden diğer bir teknik seçilebilmektedir.

Mühürleme tasarısının işlemlerinin temel faktör, fazlalıktır. Yerleştirilen işaret bit olarak kodlanır. İhlal eden kişi bu değişiklikleri fark edemez ve göremez. Başka bir deyişle, yerleştirilen veri aynı bitlerle kaplanır yararlı sıkıştırma algoritmaları ile uzaklaştırılır. Sıklaştırma tekniğinden sonra yer değiştirme yapılarak elden çıkarılanların arasında dengeleme yapılarak sayısal değerler ve sıkıştırma oranı elde edilir.

5.7 Basit Mühürleme Metotları

Basit sistemler görüntü düzleminin LSB'leri (Least significant bit insertion), yerleştirilmiş nesnenin bitlerinin basitçe yer değiştirmesiyle hareket ederler. Bu metot hesaplanmayla kolay fark edilir ve aynı şekilde kaldırılması da kolaydır.

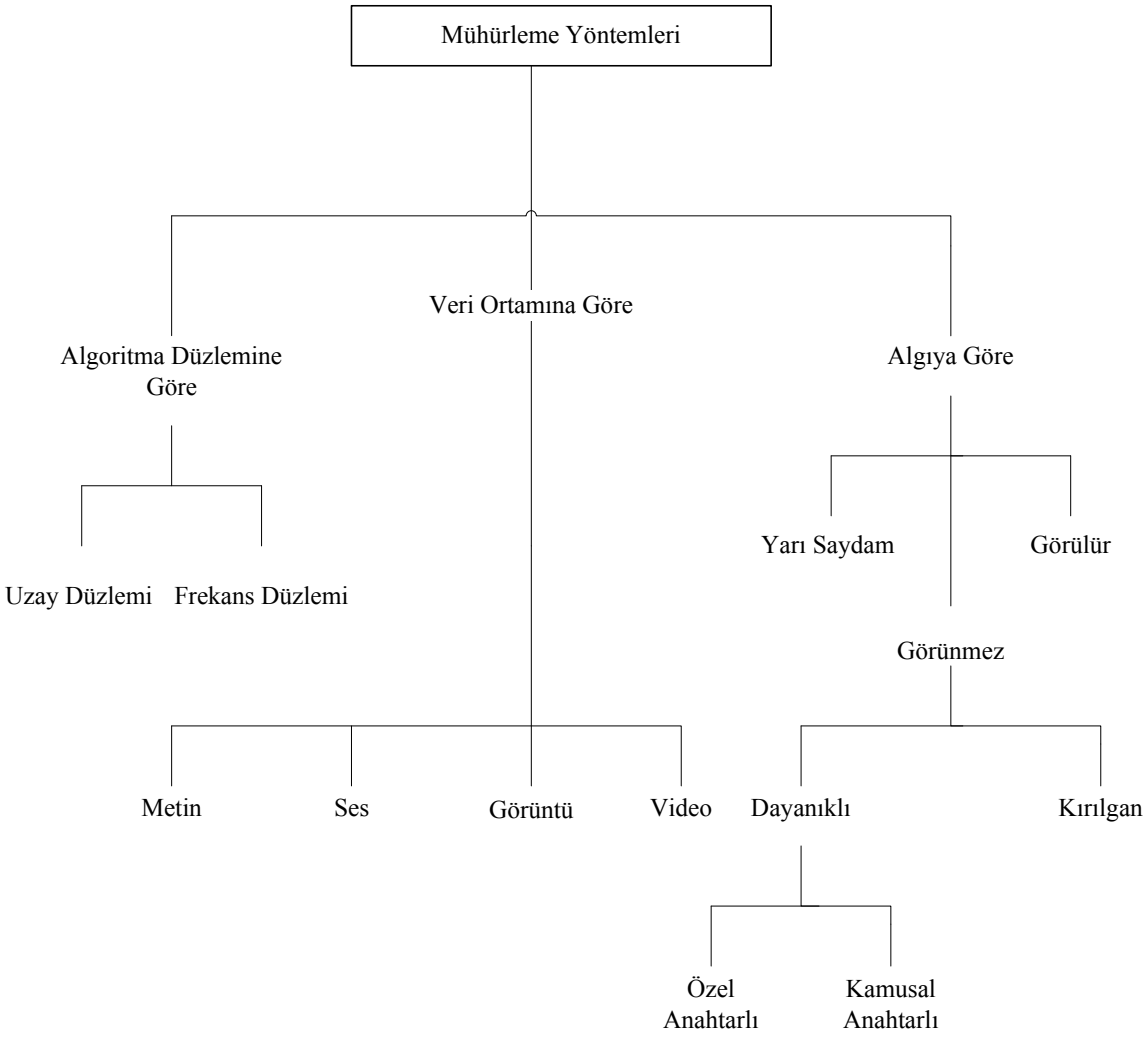
Bir gizli anahtar kullanımı için gelişmedir, alıcı ve gönderici tarafından paylaşılır. (bu bağlamda, gönderici telif hakkı sahibi olabilir ve alıcı mühürleme yapan mekanizma olabilir). Anahtar, sıra ile yerleştirilmiş işaret taşıyacak, seçilmiş piksellere uyumlu, yalancı rasgele şifre yayımı üretmek için kullanılır (Beşiroğlu, 2000). Asla pikseller bazı görünür izlerden ayırmaksızın değiştirilemez. Tek renkli alanları ya da yüksek kontrastlı sınırlar örnek verilebilir. Bu işlem, algoritma kullanımı sayılabilir, komşu piksele göre karşılaştırılarak uygun pikselin kontrol edilmesini sağlar ve sadece testten geçirilen pikseller değiştirilir.

Bu metot LSBs değerlerinin değişikliklerine karşı duyarlıdır. Bazı korumalar mühürleme ve yerleştirme tekniklerinin büyüklüğünü azaltır. Bazı uygulamalar hariçtir; veri nesnesine karıştırma yapıldığında koruma içim bu metot yeterli değildir ve görüntü içerisine veri saklama tekniklerini gerektirir.

Görünebilir mühürleme tekniği tasarlanan veri saklama projelerinden ve bir örtülü mühürleme görüntü katmanını ekleme işlemi farklıdır. Saldırılara kolayca duyarlıdır. Örneğin insan gözü tarafından fark edilebilir, tekrarlı saldırılara elverişlidir ve fırsat verir. Küçük değişimler, mühürleme düzlemi okunaksız hale getirilinceye kadar defalarca uygulanır.

5.8 Mühürleme Yöntemleri Çeşitleri

Bilgisayar ortamındaki verilerin damgalanması için birçok yöntem geliştirilmiştir. Damgalama yöntemleri, algoritma düzlemine göre, çalışmanın türüne göre ve algıya göre olmak üzere öncelikle üç ana başlıkta incelenebilir. Bunlar da kendi içerisinde alt gruplara ayrılır. Buna göre Şekil 5.1'de sayısal damgalamanın çeşitleri görülmektedir (MOHANTY, 1999).



Şekil 5.1 Mühürleme yöntemi çeşitleri (MOHANTY, 1999).

Damgalama algoritmaları, üzerinde çalışılan düzleme göre ikiye ayrılır. Uzay düzleminde yapılan damgalama işlemlerinde doğrudan damgalanacak çalışmanın bilgisi üzerinde değişiklik yapılır. Frekans düzleminde yapılan damgalama işlemlerinde, damgalanacak çalışma öncelikle frekans bileşenlerine ayrılır. Bu amaçla DCT (Discrete Cosine Transform), DWT (Discrete Wavelet Transform), DFT (Discrete Fourier Transform), FFT (Fast Fourier Transform) gibi dönüştürme araçları kullanılarak, çalışma frekans düzlemine taşınır. Burada, elde edilen frekanslar ve katsayıları üzerinde değişiklik yapıldıktan sonra ters dönüştürme uygulanarak damgalanmış ürün elde edilir.

Damgalanacak çalışmanın türüne göre, damgalama yöntemleri dört alt başlıkta incelenebilir. Bunlar yazı, ses, görüntü ve videodur.

Algıya göre damgalama algoritmaları üç grupta incelenebilir. Damgalanacak mesajın, görüntünün bir yerine gözle görülebilecek bir şekilde yerleştirilmesine "görünür damgalama" adı verilir. Görünür damgalamaya örnek olarak televizyon ekranında bulunan kanal logosu ya da Internet'te yayınlanan görüntülerin altında bulunan yayıncı sitenin adresi verilebilir. Bu yöntemde her ne kadar logo görüntünün üzerinde belirgin bir şekilde yerleştirilse de, kırpma (cropping) yoluyla görüntüden kolaylıkla ayrılabilir ve hatta yerine başkası yerleştirilebilir (MOHANTY, 1999).

Görüntü içine gözle algılanamayacak bir şekilde mesajı yerleştirme işlemine "görünmez damgalama" adı verilir. Bu yöntem ile damgalanan görüntülerde mesaj, görüntü içine yetkili kişi tarafından bilinen bir algoritma ile dağıtılır ve başka bir algoritma ile görüntüden geri elde edilir. Mesajın görüntü içindeki yeri belli olmadığından kırpma işlemi ile görüntüden ayrılamaz. Damgalama ve geri elde etme algoritmaları sadece yetkili kişi tarafından bilindiğinden yetkisi olmayan kişilerin görüntüdeki mesaja ulaşmaları neredeyse imkânsızdır.

Görünür ya da görünmez damgalamanın yanında sayılabilecek üçüncü bir yöntem ise, logonun görüntünün büyük bir bölümü üzerine yarı saydam olarak eklenmesidir. Bu yolla eklenen logonun görüntüden ayrılması, görüntüyü anlamsız kılacağından avantajlıdır. Ancak görüntüyü kullanıcıya bu şekilde sunmak bir dezavantajdır.

Görünmez damgalama yöntemleri kendi içinde "dayanıklı" ve "kırılgan" olmak üzere ikiye ayrılır. Dayanıklı damgalama yöntemleriyle yapılan damgalamada, taşıyıcı görüntüye gizli bir şekilde damgalanan bilginin, görüntünün kalitesinde ciddi bir bozulmaya neden olmayan çeşitli görüntü işleme saldırılarına karşı dayanıklı ve geri çıkarıldığında tanınabilir nitelikte olması amaçlanır. Kırılgan damgalama yöntemlerinin amacı görüntünün gerçekliği ya da doğruluğunun tespiti olduğundan, görüntüde yapılacak en küçük bir değişikliğin damgalanan bilgiyi yok etmesi istenir.

Dayanıklı görünmez damgalama algoritmaları kendi içlerinde iki grupta incelenebilir. Bunlar "kişisel anahtarlı" ve "kamusal anahtarlı" olarak adlandırılır. Bu tür damgalama yöntemlerinin

temel prensibi, damgalama ve geri elde etme sırasında kullanılan anahtarlara bağlıdır. Eğer taşıyıcı görüntüden mesajın çıkarılması için gerekli anahtar herkes tarafından biliniyorsa, bu yöntem "kamusal anahtarlı görünmez dayanıklı damgalama" olarak adlandırılır. Diğer taraftan, kullanılan anahtar sadece görüntünün sahibi tarafından biliniyorsa, yani gizli tutuluyorsa, bu "kişisel anahtarlı görünmez dayanıklı damgalama" olarak adlandırılır (ARNOLD ve ark., 2003).

Sayısal görüntülere gizli mesaj damgalama yöntemlerinin sınıflandırılmasında kullanılan bir diğer kriter ise geri elde algoritmasında görüntünün aslının kullanılıp kullanılmamasıdır. Mesajın geri elde edilmesinde eğer görüntünün ya da mesajın aslı kullanılmıyorsa, bu tür yöntemlere "kör damgalama" adı verilir. Eğer görüntünün ya da mesajın aslından biri kullanılıyorsa, bu tür yöntemlere "kör olmayan damgalama" denir.

5.9 Mesaj Damgalama Yöntemlerinde Dikkat Edilmesi Gereken Hususlar

Sayısal görüntülerde telif haklarının korunması ve güvenlik için mesaj damgalanması üzerine birçok çalışma yapılmıştır. Kullanılan algoritmalar ve düzlemler birbirinden farklı olsa da, temelde belli başlı amaçlar etrafında toplanmıştır. Mesajın algılanmaması ve dayanıklılığı göz önünde bulundurularak damgalama algoritmalarından beklenen özellikler aşağıdaki gibi sıralanabilir (MOHANTY, 1999).

5.9.1 Görünür Mesaj Damgalamanın Özellikleri

- Görünür bir şekilde damgalanan mesaj hem renkli hem de monokrom görüntülerde açıkça belli olmalıdır.
- Mesajı resim kırpma işlemine karşı korumak için, görüntüde geniş bir alana yayılmalı ya da görüntünün önemli bir bölümü üzerine yerleştirilmelidir.
- Mesaj yarı saydam olarak görüntü üzerine eklenecekse görünebilecek seviyede saydam olmalı fakat orijinal görüntünün ayrıntıları korunmalıdır.

5.9.2 Görünmez Dayanıklı Mesaj Damgalamanın Özellikleri

- Görünmez bir şekilde görüntüye damgalanmış mesaj, ne görüntüde tespit edilebilmeli ne de

görüntü içeriğinin kalitesini düşürmelidir.

- Görünmez bir şekilde görüntüye damgalanmış mesaj, görüntü kalitesinde gözle görülür bir bozulmaya sebep olmayan çeşitli işlemlere karşı dayanıklı olmalıdır.
- Yüksek kaliteli görüntülerin ve sanat çalışmaların damgalanmasında en az sayıda piksel değiştirilmelidir.
- Mesaj damgalanması ve geri görüntüden elde edilmesi işlemi kolay ve hızlı bir şekilde yapılabilmelidir.
- Görüntüye damgalanan mesajın geri çıkarılmasında kullanılacak yazılım bilgisayar ve işletim sistemlerinden bağımsız çalışabilmelidir.
- Görüntü içindeki mesaj, JPEG gibi çeşitli kayıplı sıkıştırma işlemlerine karşı dayanıklı olmalıdır.

5.9.3 Görünmez Kırılgan Mesaj Damgalamanın Özellikleri

- Görünmez bir şekilde görüntüye damgalanmış mesaj, ne görüntüde tespit edilebilmeli ne de görüntü içeriğinin kalitesini düşürmelidir.
- Görüntü pikselleri üzerinde yapılacak bir değişiklik mesajın kolayca bozulmasına neden olmalıdır.
- Mesaj güvenli olmalıdır. Bunun anlamı, sık kullanılan görüntü işlemleri ile görüntü üzerinde yapılacak herhangi bir değişiklik sonucu bozulan mesaj, tekrar düzeltilebilecek niteliğe sahip olmamalı ve tanınabilir bir düzeyde geri elde edilmesi mümkün olmamalıdır.
- Mesaj damgalanması ve geri görüntüden elde edilmesi işlemi kolay ve hızlı bir şekilde yapılmalıdır.

5.10 Sayısal Coğrafi Veri İzin Dışı Kullanımı Tespit Eden Yöntemler

Sayısal coğrafi verilerin izin dışı ve yasa dışı kullanımını tespit eden yöntemleri aşağıda belirtilmiştir.

5.10.1 Görüntüden Sayısallaştırma İşlemi ve Tespit Yöntemleri

Görüntüden sayısallaştırma olarak bilinen bir yöntemle, basılı haritaların bir tarayıcı ile tarandıktan sonra, bilgisayar ortamında yeniden koordinatlandırılması ile elde edilen ekran görüntüsünden, vektör veri toplama işlemi sayısal haritacılık alanında çok yaygın olarak kullanılan bir yöntemdir. Böyle bir yöntemle yapılan sayısallaştırma durumunda kaçınılmaz hatalar meydana gelmektedir. Hata yayılım ilkesi gereği yapılan her işlem yeni bir hata meydana getirir ve bu hata bir sonraki işlemdeki hataya eklenerek artar. Sonuçta oluşan hata birikimi, eğer kabul edilebilir sınırlarda ise, bir sonraki işleme devam edilebilir. Görüntüden yapılan sayısallaştırma işlemi sonucunda elde edilen ürün orijinalinin birebir aynısı olamaz ve onun kadar hassas da değildir. Bu tür bir sayısallaştırma işlemi aşağıdaki adımları içerir;

- Basılı haritanın taranarak bilgisayar ortamına aktarılması.
- Elde edilen görüntünün, referans noktaları yardımıyla (bu noktalar genellikle pafta köşe noktalarıdır) dünya koordinatlarına göre yeniden konumlandırılması.
- Bu görüntünün vektör sayısallaştırma yapılabilmesi için bir CAD (Computer-aided design) veya CBS yazılımına yüklenmesi.
- Bu görüntü üzerinden etkileşimli, otomatik veya elle olarak sayısallaştırma işleminin yapılması.

Yukarıdaki işlem adımlarının her birisinde bir miktar hata meydana gelmektedir. Bu hatalar birikimli olarak artar. Ancak asıl önemli hata kaynağı, dördüncü adımda ortaya çıkmaktadır. Bu işlem sırasında operatörler tarafından yapılan sayısallaştırma sırasında, bu güne kadar elde edilen tecrübeler ışığında, herhangi bir nokta, çizgi veya alanın aynı operatör ile arka arkaya iki defa sayısallaştırması sonucunda dahi birebir aynı detaylar elde edilememektedir. Bu tür bir işlem sonrasında oluşan verilerden yararlanarak üretilen haritalar orijinalinin aynısı olmasa bile hemen hemen aynı görüntüyü sağlayabilirler.

Elde edilen vektörel ürün yardımıyla istenildiği kadar yeni ve çeşitli ürün veya basılı harita üretmek mümkündür. Bu yöntemin kullanılması sayısal haritacılıkta sıkça kullanılır. Ancak bazı ürünlerin bu yöntem ile dahi olsa çoğaltılarak yeniden üretilmesi, yayınlanması veya ticari amaçlarla kullanılması esasları, telif ve iktibas hakları ile ilgili kanun, yönetmelik ve kararnameler ile belirlenmiştir. Bazı haritalar ise bu kapsamın dışındadır ve kanunlarla belirlenmiş gizlilik çerçevesinde üretilmesi ve kullanımı sınırlandırılmıştır. Bazı ürünler ise

herkese açıktır ve istendiği şekilde, birebir kopyası olmadığı sürece, bu yöntemle üretimi gerçekleştirilebilir.

Görüntüden yapılan sayısallaştırma işlemi sonucunda elde edilen ürünler ile orijinal ürünün karşılaştırılması ve aynı kaynaktan geldiklerini göstermek için aşağıdaki ipuçları aranmalıdır.

- Her iki üründe mevcut ortak bölgeler tespit edilmelidir.
- Bu bölgelerde bulunan nokta, çizgi ve poligon detaylarının birbirleri ile aynı karakterde olup olmadığı incelenmelidir.
- Haritaların üzerine konulan ve bilgi iletimi için kullanılan yazı, işaret ve karakterlerden ortak olanlar bulunmalıdır.
- Sonradan yapılan sayısallaştırma ile orijinalde bulunan özel işaretlerin yönleri birbirlerine göre konumları, yazıların yön, kıvrım ve yerleşimleri incelenmelidir.
- Harita üzerinde aktarılan bilgilerden orijinal haritaya özgü olabileceği değerlendirilen işretler aranmalıdır.
- Bu ve diğer bulgular bir verinin diğerinden, görüntüden sayısallaştırma yapılarak elde edildiği sonuçlarını gösterir deliller olarak mütalaa edilebilir.

5.10.2 Aynı Kaynaktan Türetilmiş Vektör Verilerin Tespit Yöntemleri

Sayısal haritacılık alanında vektör ve raster adı verilen iki tip veri formatı vardır. Bu formatlar yapılacak haritanın niteliğine göre seçilir. Raster formatlar ile üretilen haritalar daha çok ortofoto olarak adlandırılan yersel veya göksel tekniklerle elde edilmiş fotoğrafların koordinatlandırılarak belirli bir ölçekte hazırlanması ile elde edilir ve görüntü kalitesi ve çözünürlülük gibi parametrelerle ifade edilir. Bu tür haritalar belirli bir amaca hizmet etmek için kullanılır ve üzerinde fazla bir değişiklik yapılması mümkün değildir. Tam tersi olarak vektör haritalar defalarca yeniden kullanılabilen ve sınırsız sayıda kullanım alanı bulunan formatlardır. Bu tür haritalar genellikle raster haritalardan yararlanarak veya yersel ölçümler yapılarak üretilirler.

Vektör verilerin aynı kaynaktan geldiğini tespit etmek için çok fazla yöntem kullanılabilir. Öncelikle her iki veri kümesinde birbirinin aynı görüntüye ve konuma sahip nokta, çizgi ve alan

detaylar gözle aranır. Bu tarama işlemi verilerin üst üste bir CAD veya CBS yazılımının görüntüleme modülü aracılığıyla kolaylıkla gerçekleştirilebilir. Her iki veri kümesinin üst üste bir CAD veya GIS yazılımı aracılığıyla görüntülenebilmesi için aynı projeksiyon sistemine dönüştürülmesi gerekmektedir. Ancak bu işlem sonucunda iki veri kümesi birbirleri ile karşılaştırılıp değerlendirilmesi yapılabilir. Yeryüzünün farklı bölgelerinin bir düzleme aktarılması işlemi yansıtma veya izdüşüm (projeksiyon) olarak adlandırılır. Projeksiyon bilgileri bir vektör veya raster veri kümesinin yeryüzü üzerinde konumlandırılması yardımcı olur.

Aynı projeksiyona dönüştürülmüş veri setleri görüntülendikten sonra aynı kaynaktan türetilmiş olan veriler birbirini tam olarak örtecek, farklı olanlar ise ayrık görünecektir. Görüntüde üst üste örtüştüğü tespit edilen detaylar üzerinde detaylara ait karakteristik özelliklerin karşılaştırılması gerekir. Coğrafi Bilgi Sistemlerinin temel yapı taşı olan nokta, çizgi ve alan nesneleri bir vektör veri kümesini oluşturan geometrik elemanlardır. Bir nokta tek anlamlı olarak yeryüzünde konumlandırılabilen ve [X,Y] gibi en az iki parametreden oluşan bir geometrik nesnedir. Bir çizgi birbirini takip eden noktaları birleştiren doğru parçalarından oluşur. Bir alan ise başlangıç ve bitiş noktası aynı olan bir tür kapalı çizgi olarak tanımlanabilir. Bu geometrik elemanlara ait koordinat çiftlerinin değerleri, CAD veya CBS yazılımı imkânları aracılığıyla elde edilebilir. Vektör verilerde koordinat bilgileri hassas şekilde kaydedilebildiğinden, ekrandan yaklaşarak işaretçi konumunu okuma yoluyla yapılan işlemden farklı olarak kesin sayısal değerlere ulaşılabilir. Bir başka deyişle bir noktanın koordinat bilgisi tam olarak elde edilebilir.

İki farklı veri kümesinin görüntüde örtüşmesi verilerin aynı kaynaktan geldiği anlamına gelmez. Görüntü kalitesi, gözün algılama düzeyi, kullanılan bilgisayarın ekran çözünürlülüğü ve diğer etkenler nedeniyle ekrandan yapılan koordinat okumalarında yanılmalar olabilmektedir. Ancak vektör veriler üzerinde bir takım işlemler sonucunda bu koordinat bilgileri, biraz önce anlatılan etkenlerden arındırılmış olarak tespit edilebilir. Her iki veri kümesinde örtüşen nokta, çizgi ve alan detayları oluşturan koordinat çiftleri bu işlemler aracılığıyla karşılaştırılabilir. Böyle bir işlem sonucu aşağıdaki iki durum ortaya çıkabilir;

Bir detaya ait koordinat çiftlerinin her iki veri kümesinde de aynı ondalık hassasiyetine sahip olması,

Bir detaya ait koordinat çiftlerinin her iki veri kümesinde de birbirine yakın çok yakın değerlere sahip olması,

İlk durumda vektör verilerin birbirinin kopyası olduğuna kolaylıkla karar verilebilir. Bir verinin, diğer verinin içerisinden kesme işlemi ile türetilmiş olduğu sonucuna hemen varılabilir. Ancak ikinci durum biraz daha inceleme gerektirmektedir. Bir coğrafi detaya ait iki farklı koordinat çifti kümesinin birebir aynı değerlere sahip olmamaları bu değerlerin farklı kaynaklardan türetildiği anlamına gelmez.

İzdüşüm bilimi yeryüzünün bir düzleme aktarılması için gerekli dönüşüm parametrelerini ve algoritmalarını araştırmakla uğraşan bir bilimdir. Yeryüzünün geometrik özelliklerinin matematiksel olarak modellenebilmesi için zaman içerisinde birçok bilim adamı tarafından çeşitli algoritmalar ve matematiksel fonksiyonlar geliştirilmiştir. Bu fonksiyonlarda kullanılan ve yersel ölçümlere dayanan bazı parametreler vardır. Bu parametreler uluslararası projeler ve çalışmalar ile araştırılıp güncellenmektedir. Coğrafi Bilgi Sistemleri yazılımları genellikle bu algoritmalar ve parametreleri esas alarak geliştirilirler. Yeryüzünün tamamının tek bir izdüşüm algoritması ile düzleme tam doğru olarak yansıtılmasının imkânı olmadığından, haritası yapılacak olan ilgili bölgeye uyan izdüşüm sistemi ve parametreleri kullanılmak zorundadır. CBS yazılımı geliştiren firmalar ise bu izdüşüm parametreleri ve algoritmalarını, kendi politikalarına uygun şekilde sistemlerine aktarırlar. Aynı izdüşüm sistemine ait farklı algoritma ve parametreler kullanabilirler.

Yukarıda bahsedilen nedenlerden dolayı farklı yazılımların, farklı izdüşüm algoritmaları, parametreleri veya fonksiyonları kullanması nedeniyle aynı kaynaktan olan bir veri kümesine uygulanacak farklı işlemlerin, farklı koordinat çiftlerinden oluşmuş verilere dönüşebileceği bir gerçektir. Ayrıca veri kümesi için tanımlanan sayısal duyarlılık, yani ondalık hassasiyeti de bu duruma neden olan etkenlerden birisidir. Bundan dolayı aynı veriler üzerinde uygulanan farklı işlemler sonucunda verinin konumsal duyarlılığında bazı bozulmalar, değişmeler olabileceği bir gerçektir. Sayısal analiz tekniklerinin de doğruladığı bu durumun sonucu olarak koordinat çiftlerinin değerlerinde küçük farklılıkların olması kaçınılmazdır. Eğer aynı veri kümesine aynı sırayla bu tür dönüşüm işlemleri uygulanırsa, bu farklılıkların da ortadan kalkacağı görülebilir.

Koordinat çiftlerinin çok yakın değerlere sahip olmasının yanında verinin karakteristiği olarak değerlendirilebilecek diğer ipuçlarının da bulguları desteklemesinde fayda vardır. Bunlar arasında;

- Çizgi detayları oluşturan doğru parçalarının kırıklık yaptığı noktalardaki açıları,
- Bir çizgi veya alanı oluşturan noktaların sayısı ve birbirine yakınlığı
- Bir alan detayın alanı
- Bir alanın ağırlık merkezini gösteren referans noktası
- Bir çizginin uzunluğu
- Bir coğrafi nesnenin diğerine olan göreceli uzaklığı
- Bir nokta detayın kuzeye veya bir başlangıç istikametine göre açısı
- Bir çizgi veya alanı oluşturan doğru parçası sayısı
- Yükseklik bilgisi içeren nokta detayların değerleri.
- Gibi çeşitli kriterler, bulguları güçlendirici ipuçları olarak değerlendirilebilir.

5.10.3 Veri Formatları ve Öznitelik Karşılaştırması

Coğrafi vektör veriler, temsil ettikleri gerçek dünya nesnesine ait çeşitli tanımlayıcı öznitelik bilgilerini bünyelerinde barındırabilen bir yapıya sahiptirler. Bir nesneye ait sınırsız sayıda bilgi tutabilirler. Ancak bu bilgilerin sayısı ekonomik kaygılar nedeniyle genellikle sınırlandırılmaktadır. Bilgisayar ortamında bir coğrafi nesnenin modellenebilmesi için CBS yazılımları bu tür öznitelik bilgilerine ihtiyaç duyar. Gerçek dünyaya ait nesneler, öncelikle ortak karakteristikleri ile belirli sınıflandırmaya tabi tutulurlar. Sınıflandırma sonucunda her bir sınıfa özgü olacak ve ilgili nesneyi tek anlamlı olarak tanımlayabilecek bir detay kodu üretilir. Bu detay kodu, birkaç karakter ve numaradan oluşan tek bir kod olabileceği gibi birkaç koddan oluşan karmaşık bir değerde olabilmektedir. Veri formatları arasında dönüşüm ve veri sayısallaştırmada standartlığı sağlamak maksadıyla bu tür kodların kullanılması oldukça yararlıdır ve bu durum uluslararası standardizasyonun bir gereğidir. Bunun yanında bazı yazılımların doğası gereği, kodlama tekniği ve kod değerleri arasında farklılıklar bulunabilmektedir. Yazılımların kendine özgü karakteristikleri veriyi işleme yöntemlerine, şirketlerin ticari ve politik kaygılarına göre değişir. Bu da çok çeşitli veri formatlarının ortaya çıkmasına neden olmaktadır. Ancak

uluslararası organizasyonlar bu farklılıkların ortadan kaldırılması ve sistemler arasında veri dönüşümünün gerçekleştirilebilmesi için bazı standart formatlar geliştirmişler. Ticari olan bir çok yazılım, kendi formatlarından bu ortak formatlara dönüşüme imkân tanıyacak araçlar içermektedir. Ancak her sistemin kendine özgü karakteristiklerinin bu formatlarda doğrudan karşılığı bulunmamaktadır. Bunun sonucu olarak veri dönüştürme sırasında bazı verilerin veya özelliklerin dönüşümü gerçekleşememekte ve veri kaybı meydana gelebilmektedir.

Bir yazılım sisteminde tanımlanmış olan öznitelik bilgilerinin diğer bir sisteme dönüşümü ise her iki sistemde de tanımlanmış olan dönüşüm tabloları aracılığı ile gerçekleştirilebilir. Eğer dönüşüm tablosu tanımlanmamışsa öznitelik kaybı veya kod değişimi meydana gelebilir.

Aynı öznitelik bilgilerine ve detay kodlarına sahip veriler bir çok farklı veri kümesinde bulunabilir. Ancak bir veri aynı öznitelik bilgilerine sahipte olsa hiçbir şekilde aynı koordinatlara sahip nokta çiftlerinden oluşması mümkün değildir.

5.10.4 Vektör Veri ve Kâğıt Haritaların Karşılaştırma Yöntemleri

Sayısal haritacılık alanında vektör veri formatları çok geniş kullanım alanı bulan bir format türüdür. Dünyada birçok haritacılık kuruluşu bu formatlar aracılığı ile haritalarını üretmektedir. Günümüzde haritalar bilgisayar ortamında veri toplama arabirimleri sayesinde vektör formatlara dönüştürülmekte ve sonra da kâğıt harita üretimine esas teşkil eden EPS, PDF, RTL, PS, PRN veya TIF gibi ara formatlara dönüştürülmektedir. Bu ara formatlar matbaacılık ve baskı teknolojilerinin kolaylıkla kullanabildiği ve sayısal verilerin kâğıda basılabilmesi için gerekli bilgileri bünyesinde bulundururlar. Bu sayede baskı ve çizim makineleri verinin kâğıt üzerinde hangi şekilde basılacağı bilgisine sahip olurlar. Sayısal haritaların bu tür ara formatlardan birine dönüştürülmesinden sonra elde edilen kâğıt haritalar vektör verinin karakteristiklerini taşımakla beraber, kâğıt haritaların hassasiyeti çok daha düşüktür. Bilgisayar ortamında elde edilen sonuçlar, kâğıt haritalarda elde edilemez. Fakat bu durum bir harita kullanıcısı açısından bir fark yaratmayacak seviyelerdedir.

Bir sayısal harita ile herhangi bir kâğıt haritanın karşılaştırılabilmesi için aşağıdaki işlemlerin uygulanması yeterlidir.

- Sayısal harita bir CAD veya CBS yazılımında açılarak, kâğıt haritanın üzerindeki sembollerin

aynısı kullanılarak tekrar sembolleştirilir.

- Kâğıt haritanın ölçeği ile aynı ölçek değeri programda ayarlanır.
- Sayısal haritanın ilgili alanı, bir çizici veya yazıcıdan çıktı olarak alınır.
- Kâğıt harita ile bu çıktının gözle karşılaştırılmasının yapılması.
- Kâğıt harita ile yapılan karşılaştırmada aşağıdaki hususlar incelenmelidir.
    - Çizgilerin karakteristik özelliklerinden olan kırıklık noktaları.
    - Nokta sembollerin açıları.
    - Alan detayların şekilleri ve köşe yaptığı yerler.
    - Yazı karakterlerinin yerleşimi ve tipleri.
    - Açılı nokta detayların bir istikamete göre açı değerleri.
    - Detayların birbirine göre göreceli konumları.
    - Yazıların detaylara göre konumları ve yazı istikametleri.

Benzerliklerin olduğu belirlenen bölgeler ve detaylar her iki kâğıt üzerinde de işaretlenmeli ve sonra da bu işaretlerin bulunduğu yerler bilgisayar ekranından tekrar gözle teyit edilmelidir. Tespit edilen bulgular, bu haritanın tamamının veya bir kısmının bu veriler kullanılarak çıktısının alındığını gösterir deliller olarak değerlendirilebilir.

6. UYGULAMA

6.1 Amaç

Bu uygulamanın konusu herhangi bir kurum veya firma tarafından üretilen sayısal coğrafi ürünlerin ve verilerin yasadışı kullanımını önlemek, bu verilerin güvenliği ve eser sahibi hakların korunması amacıyla kullanılan yöntemlerin geliştirilmesi ve gerçekleştirilmesidir.

Coğrafi Bilgi Teknolojilerinin temelini, sayısal coğrafi bilgi oluşturmaktadır. Yoğun emek, zaman ve maliyet ile üretilen sayısal coğrafi ürünler, bilgisayar teknolojisinin sağladığı olanaklarla tamamen ya da kısmen üreticinin izni olmaksızın kopyalanabilmekte, çoğaltılabilmekte, çevrimdışı yöntemle (CD, DVD, smart disk, harici disk üzerinde) veya çevrimiçi yöntemle (internet, iç ağ üzerinden) dağıtılabilmekte ve bu şekilde yasadışı olarak kullanılabilmektedir. Ayrıca, üreticinin sayısal coğrafi ürünleri üzerinde başka yazılımlar kullanılarak kazanç elde edilmektedir.

Coğrafi veri oluşturmak ve kullanıma hazır hale getirmek çok pahalı, kopyalama işlemi ise çok kolaydır. Bu verilerin eser sahibi hakları korunması ve izin dışı kullanımı önlemek amacıyla caydırıcı yöntemler geliştirmek gerekir. Sayısal coğrafi verilerin korunma ve caydırıcı yöntemlerinin olamayışı korsan sektörünü teşvik edebilir ve verileri yasa dışı olarak topluma sunulabilir. Bu uygulamada belirtilen yöntemler kullanılarak sayısal coğrafi ürünlerin izin dışı kullanımı tespit edilebilir ve caydırıcı olabilir.

Uygulamada üretilen raster haritaların yasa dışı kullanımını önlemeye ve caydırmaya yönelik var olan yöntemler gerçekleştirilmiştir. Üretilen haritalarda mevcut yasal sorunlar yasal sorunlar maddesinde belirtilmiştir.

6.2 Yasal Sorunlar

Kurum ve firmalarca üretilen raster haritalar üzerinde 5846 Sayılı Fikir ve Sanat Eserleri Kanununa (Fikir ve Sanat Eserleri Kanunun Bazı Maddelerinin Değiştirilmesine İlişkin Kanun, Kabul; Tarihi ve Sayısı: 21.02.2001/4630, Resmi Gazete Tarih ve Sayısı: 03.03.2001/24335 (mükerrer)) dayalı olarak yasal hak talep etmeye yönelik olarak üzerlerinde, üretimi yapan kuruma ait olduğunu, her hakkının saklı olduğunu ispat eden her hangi bir ibare yoktur. Bu

nedenle, bu raster haritalar, yasal bir engel olmaksızın yetkisiz kişiler tarafından kullanıma, kopyalanmaya, dağıtıma ve satılmaya açıktır.

Raster haritaları içeren veri CD ve DVD'leri ya da medyaları 5846 Sayılı Fikir ve Sanat Eserleri Kanunun (Fikir ve Sanat Eserleri Kanunun Bazı Maddelerinin Değiştirilmesine İlişkin Kanun, Kabul ;Tarihi ve Sayısı: 21.02.2001/4630, Resmi Gazete Tarih ve Sayısı: 03.03.2001/24335 (mükerrer)) gerektirdiği bir bandrol taşımadığından, yasal bir engel olmaksızın yetkisiz kişiler tarafından kullanıma, kopyalanmaya, dağıtıma ve satılmaya açıktır.

Raster haritalardan ve görüntülerden elde edilen vektör ürün yardımıyla istenildiği kadar yeni ve çeşitli ürün veya basılı harita üretmek mümkündür. Bu yöntemin kullanılması sayısal haritacılıkta sıkça kullanılır. Ancak bazı ürünlerin bu yöntem ile dahi olsa çoğaltılarak yeniden üretilmesi, yayınlanması veya ticari amaçlarla kullanılması esasları, telif ve iktibas hakları ile ilgili kanun, yönetmelik ve kararnameler ile belirlenmiştir. Bazı haritalar ise bu kapsamın dışındadır ve kanunlarla belirlenmiş gizlilik çerçevesinde üretilmesi ve kullanımı sınırlandırılmıştır. Bazı ürünler ise herkese açıktır ve istendiği şekilde, birebir kopyası olmadığı sürece, bu yöntemle üretimi gerçekleştirilebilir (Taştan 2002).

6.3 Görünür Mühürleme Yöntemi Uygulaması

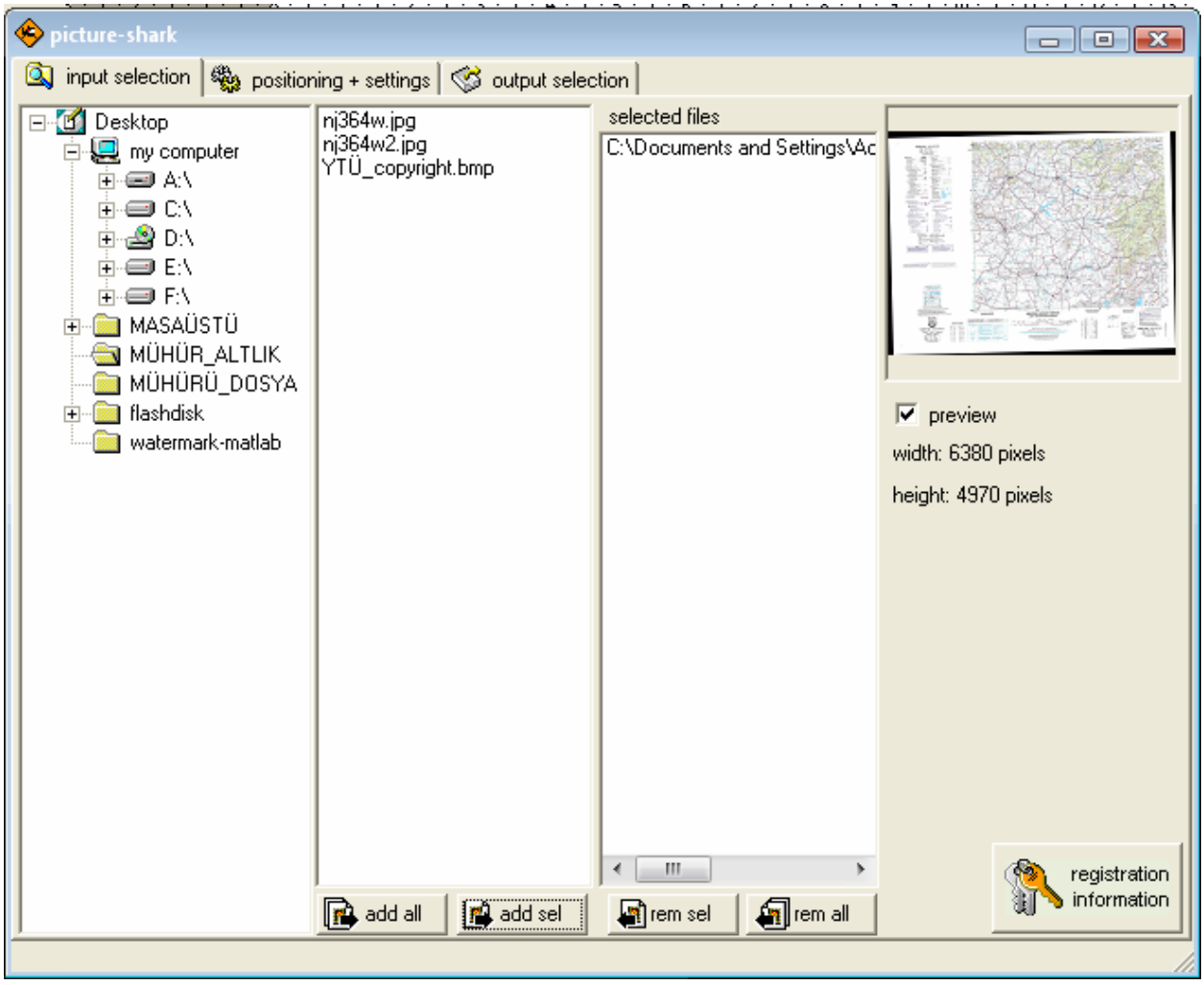
Damgalanacak mesajın, görüntünün bir yerine gözle görülebilecek bir şekilde yerleştirilmesine "görünür mühürleme" adı verilir. Bu yöntemle; üretici adı, üretici amblemi ve yetkili kullanıcı mühürleme uygulaması gerçekleştirilecektir. Uygulama aşamasında kullanıcılara kullanım kolaylığı sağlamak amacıyla yapılan işlemler detaylı olarak anlatıldı.

Bu çalışmada bilgisayar ortamına aktarılan haritalara sayısal mühürleme yöntemi uygulamak amacıyla internet ortamında belirtilen şirkete ait "Picture Shark" yazılımı kullanılmıştır. Yazılımın kurulduğu ve uygulamanın yapıldığı bilgisayar Pentium Dual 3.0 Ghz. işlemcili, üzerinde 1 GB RAM ve 256 MB ekran kartı özelliklerine sahiptir.

Uygulama için kullanılan sayısal mühürler, değişik boyutlardaki BMP uzantılı dosyalardır. Bu dosyalar 6380X4970 piksel boyutundaki JPEG formatlı raster haritaya mühürlenmiştir. Sayısal Mühürlemede kullanılan tüm görüntüler renkli bitmap formatındadır.

6.3.1 Mühürleme Yapılacak Altlık Dosyanın Seçimi

Yazılımı kullanarak mühürlenecek dosyanın seçimi Şekil 6.1'de gösterilmektedir. Bu şekilde seçilen altlık dosyanın ön izlemesi boyutları ile birlikte gözükmektedir. Çalışmada kullanılan dosyanın ismi nj364w.jpg paftası olarak seçildi ve "add sel" düğmesine basıldı. Eğer birden fazla görüntü seçmek istenirse tüm dosyalar da seçilebilmektedir.



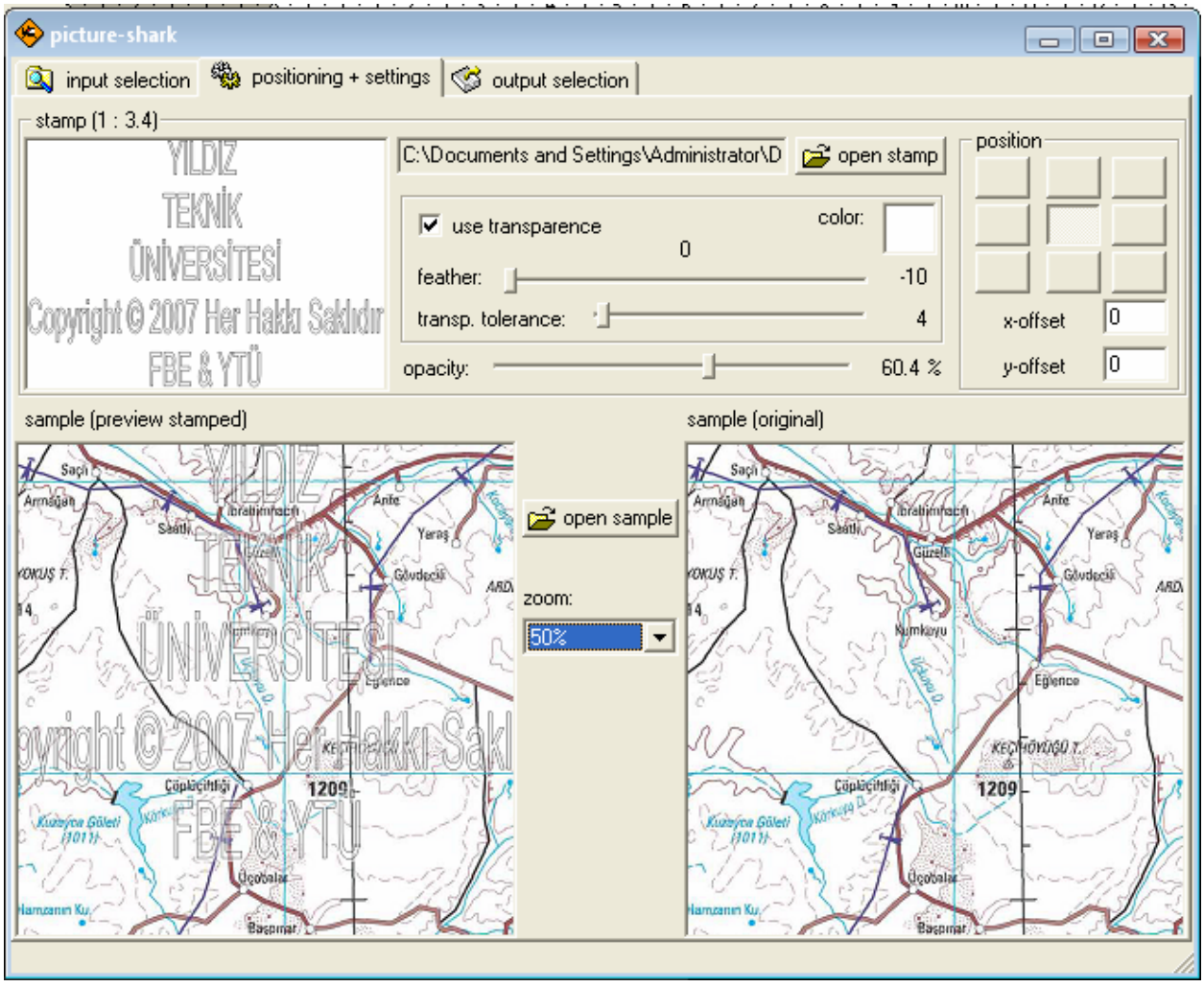
Şekil 6.1 Mühürleme yapılacak altlık dosyanın seçimi

6.3.2 Mührün Seçilmesi ve Mühürleme Uygulamasında İstenilen Ayarların Yapılması

Bu aşamada mühürlenen altlık dosya üzerinde değişik ayarlar test edilerek önceden görme olanağı sağlanmaktadır. "open stamp" tıklanarak istenilen mühür seçilir. Yapılan çalışmada daha önceden hazırlanan YTÜ_copyright.bmp dosyası seçilmiştir (Verinin orijinali Harita Genel

Komutanlığına aittir. Ancak, örnek uygulama olarak mühürleme işlemini gösterebilmek maksadıyla farklı bir mühür seçilmiştir). Dosya seçildikten sonra mühür ara yüzde gözükür. Şekilde sadece bir görüntüde yapılan ayarlar ve değişiklikler görülmektedir. “select sample “ düğmesine tıklanarak nj364w.jpg paftası seçilir. Dosya açıldıktan sonra ikiz bir görüntü ortaya çıkar; bir “sample original” başlıklı kutuda biri de “sample preview stamped ” başlıklı kutuda görünür. Sağdaki görüntü her zaman orijinal görüntüyü temsil eder. Soldaki ise üzerinde ayarlar yapıldığı mühürlü görüntüdür (Şekil 6.2).

Mührün yerini belirmek için “position” kutularından birisine tıklanarak mührün yerini görebiliriz. Mührün görüntüde belirtilen pozisyon dışında olması isteniliyorsa “x-offset” ve “y-offset” özelliği kullanılarak mühür görüntü üzerindeki yeri değiştirilebilinir.



Şekil 6.2 Mühürleme yapılacak altlık dosyanın seçimi

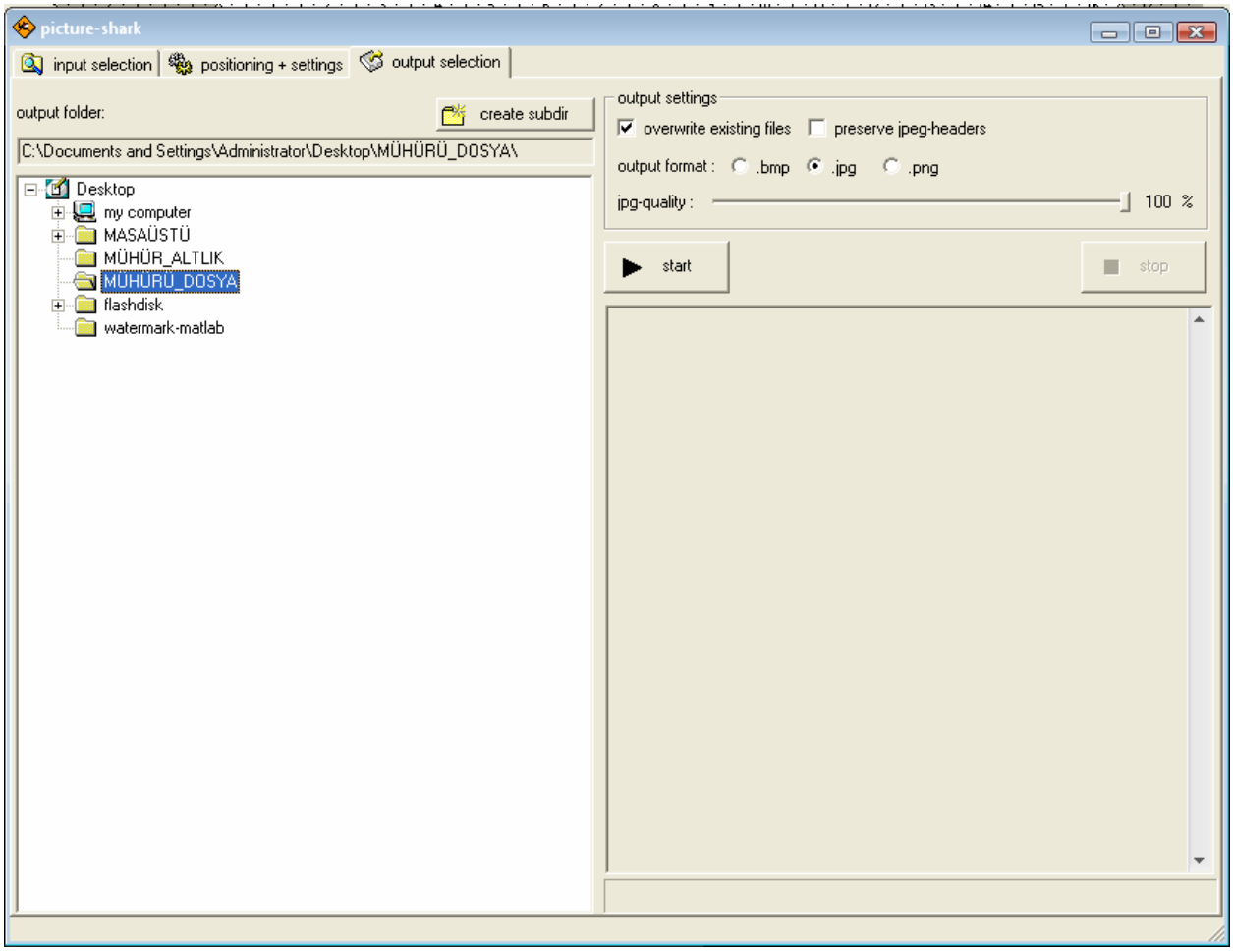
6.3.2.1 Mührün Görüntü Üzerindeki Uygunluk Ayarları

Şekil 6.2'de görülen "use tarnspance" ile "opacity" kayan bar araçları denerek mührün görüntü üzerindeki etkileri görülebilir. "Use transpance" işaretleyerek fare ile mühür üzerine gelinir. Farenin imleci pipet haline dönüşecektir. Bu durumda iken istenilen renge tıklanarak saydam özelliği kazandırılabilir. Seçilen renk "color" kutusunda gözükecektir.

Mühre saydamlık toleransı verilmek istenirse "transparance tolerance" kayan barı kullanılabilir. Bu tolerans görüntüyü oluşturan renklerden fazla uzak kalmaması gerekir aksi halde mühür gözükmez.

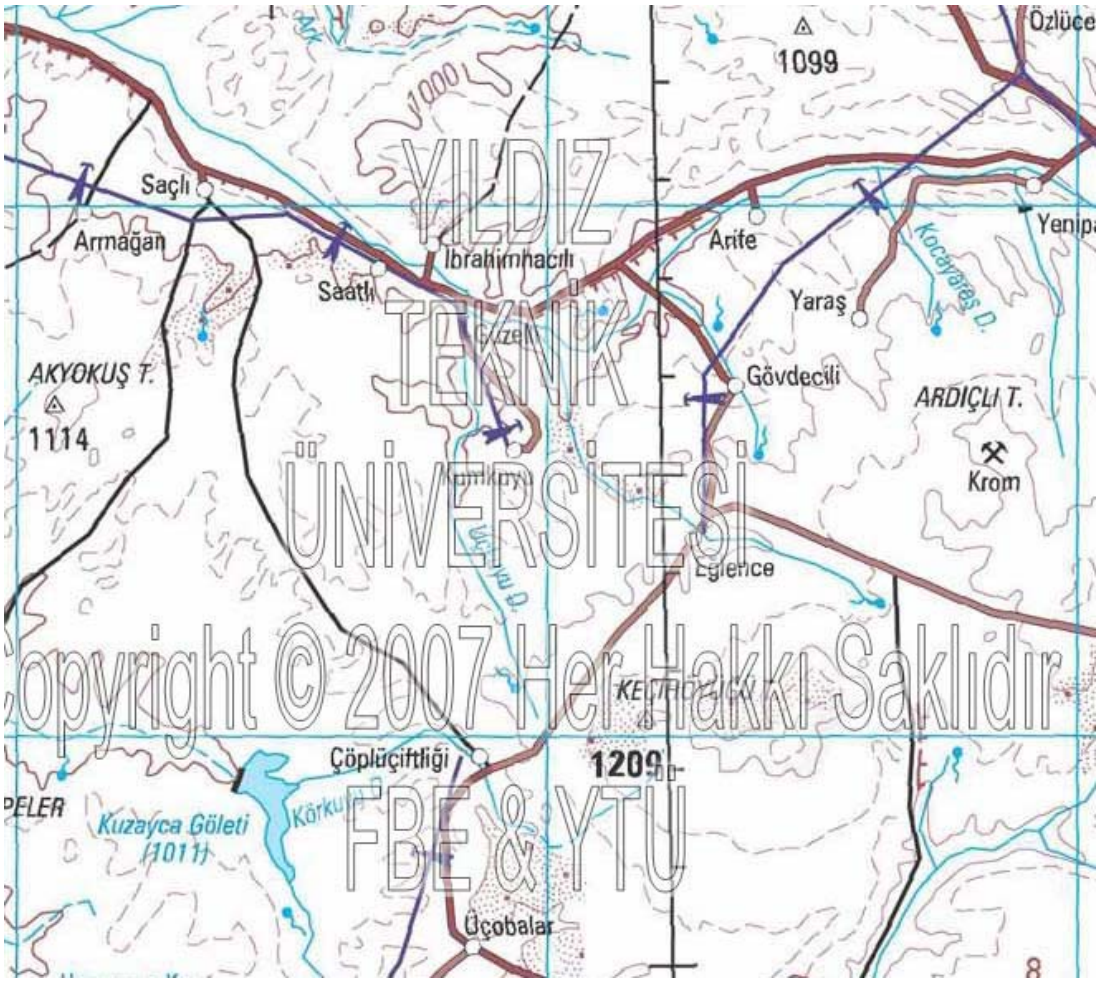
6.3.3 Çıktı Dosyasının Seçilmesi ve Mühürleme işlemi

Bu aşamada mühürlenecek altlığın dosya klasörü seçilir. "output selections" ile varolan bir dosya üzerine yaratılabilir ya da yeni klasör oluşturulabilir. Uygulama dosya formatı JPG veya BMP olabilir. Daha önce de belirtildiği bu uygulamada JPEG seçilmiştir. Dosya formatının JPEG olması görüntünün boyutunu artırmaktadır (Şekil 6.3).



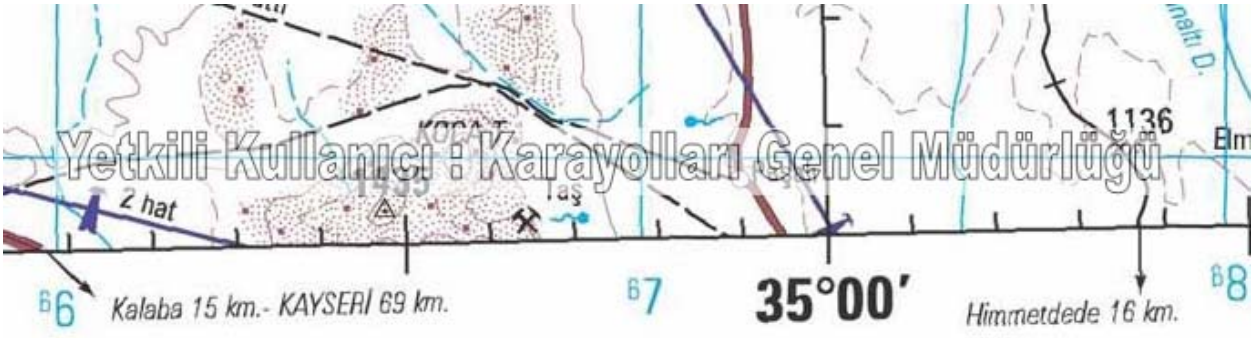
Şekil 6.3 Mührün çıktı dosyasının seçilmesi ve mühürleme işlemi

Bu yöntemle üretici adı, üretici amblemi ve yetkili kullanıcı mühürleme uygulaması gerçekleştirilen haritalar gösterilmektedir. Üretici adı uygulaması Şekil 6.4, üretici amblemi uygulaması Şekil 6.6 ve yetkili kullanıcı uygulaması Şekil 6.8'de gösterilmektedir.

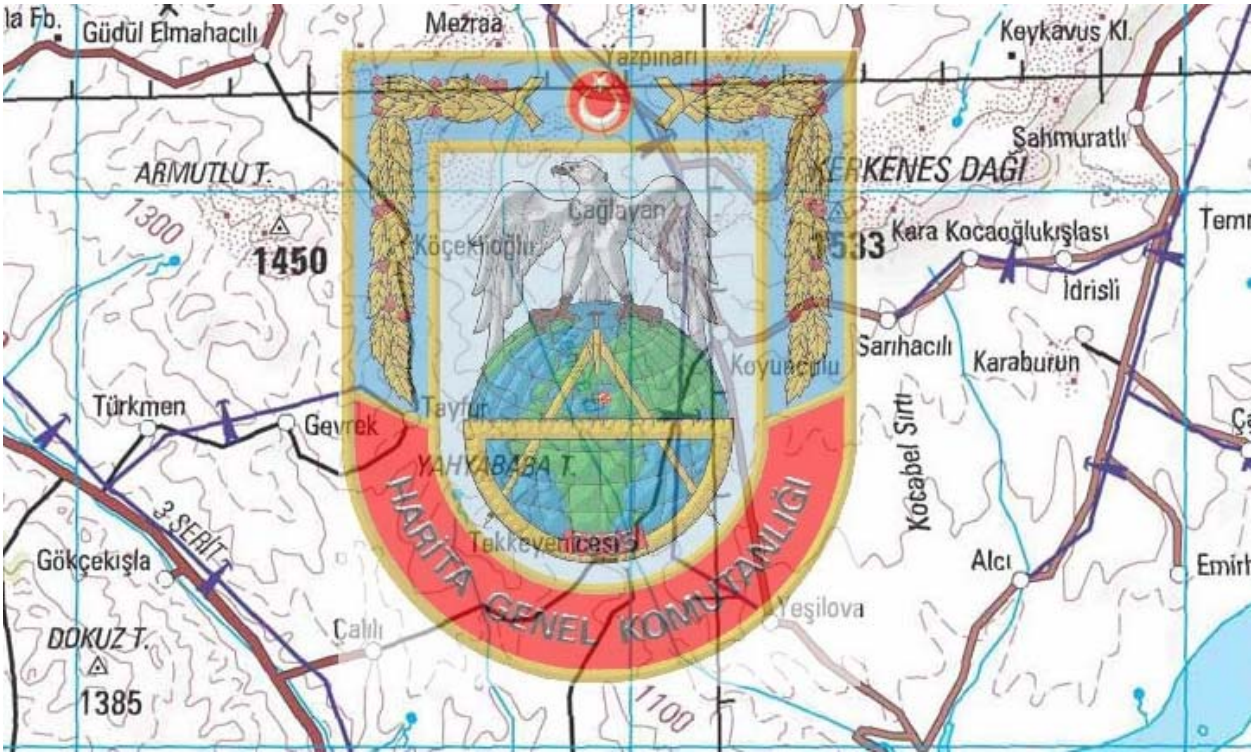


Şekil 6.4 Üretici adı ile mühürlenmiş raster harita uygulanması örneği (mühürlü)

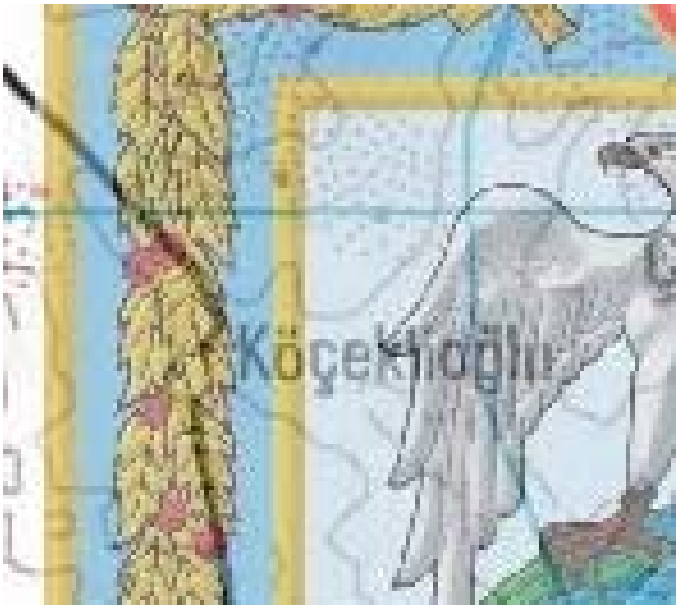
Şekil 6.5 Üretici adı ile mühürlenmiş raster harita uygulanması örneği (mühürlü büyütülmüş)



Şekil 6.6 Yetkili kullanıcı (mühürlü)



Şekil 6.7 Üretici amblemi ile mühürlenmiş raster harita uygulaması örneği



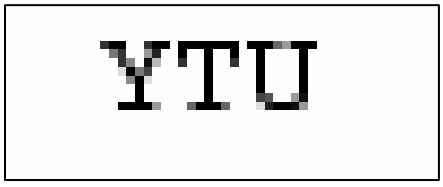
Şekil 6.8 Üretici amblemi ile mühürlenmiş raster harita uygulaması örneği-büyütülmüş

6.4 Görünmez Mühürleme Yöntemi Uygulaması

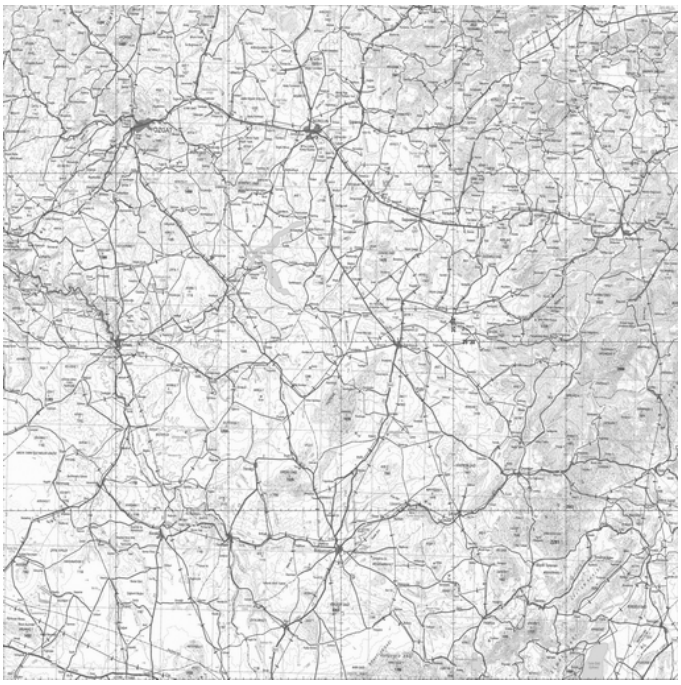
Bu damgalama yöntemleriyle yapılan damgalamada, taşıyıcı görüntüye gizli bir şekilde damgalanan bilginin, görüntünün kalitesinde ciddi bir bozulmaya neden olmayan çeşitli görüntü işleme saldırılarına karşı dayanıklı ve geri çıkarıldığında tanınabilir nitelikte olması amaçlanır.

Bu çalışmamda bilgisayar ortamına aktarılan görüntülere mühürleme işlemi ve mührün geri elde edilmesi amacıyla geliştirilen yöntem için bir bilgisayar programı hazırlanmıştır. Bu program için MATLAB kullanılmıştır. Programın hazırlandığı ve testlerin yapıldığı bilgisayar, Pentium Dual 3.0 Ghz. işlemcili, üzerinde 1 GB RAM ve 256 MB ekran kartı özelliklerine sahiptir.

Testler için kullanılan mühür mesaj, Şekil 6.9.'da görülen piksel boyutlarındaki siyah–beyaz bir mesajdır. Bu mesaj, 512x512 boyutundaki haritaya damgalanmıştır (Şekil 6.10.). Testlerde kullanılan görüntüler gri seviyede Bitmap formatındadır.



Şekil 6.9 Taşıyıcı görüntüye damgalanacak 128×128 piksel boyutlarındaki mesaj



Şekil 6.10 Taşıyıcı için seçilen 512×512 piksel boyutlarındaki görüntü

6.4.1 Yöntem

Sayısal görüntülere gizli bir bilginin damgalanması için önerilen yüzlerce farklı algoritma vardır. Bu algoritmaların yapılarına göre sınıflandırılması Şekil 5.1.'de görülmektedir. Bu çalışma ile; sayısal görüntülere görünmez ve dayanıklı bir şekilde damgalama işlemi için mesaj saklayan geri elde edilebilen yöntem önerilmiştir.

Literatürde uzay ve frekans düzlemlerinin bir arada kullanıldığı damgalama yöntemleri (SHIH ve WU, 2003) olmakta beraber, bu metotlarda damgalama işlemi her iki düzleme ayrı ayrı yapılmıştır. Mesajın bir kısmı frekans düzlemine damgalanırken, diğer bir kısmı da uzay düzlemine doğrudan damgalanmıştır. Bu çalışma ile önerilen bu düzlemde oluşan frekans bantlarından orta bantta bulunan katsayıların seçilerek mühürleme işlemini gerçekleştirmektir.

Önerilen yöntemin ayrıntıları 6.4.1.1 ve 6.4.1.2 bölümlerinde açıklanacaktır. Mühürleme için görüntü ile mesaj üzerinde yapılan ön işlemler, damgalama algoritması ve damgalanmış görüntünün oluşturulması yöntemin ilk aşamasını oluşturmaktadır. İkinci aşamada ise saklanan mesajın geri elde edilmesi için sırasıyla ön işlemlerin yapılmasının ardından geri elde etme algoritmasının çalıştırılması ve son olarak mesajın oluşturulması hakkında bilgi verilecektir.

6.4.2 Mühürleme İşlemi

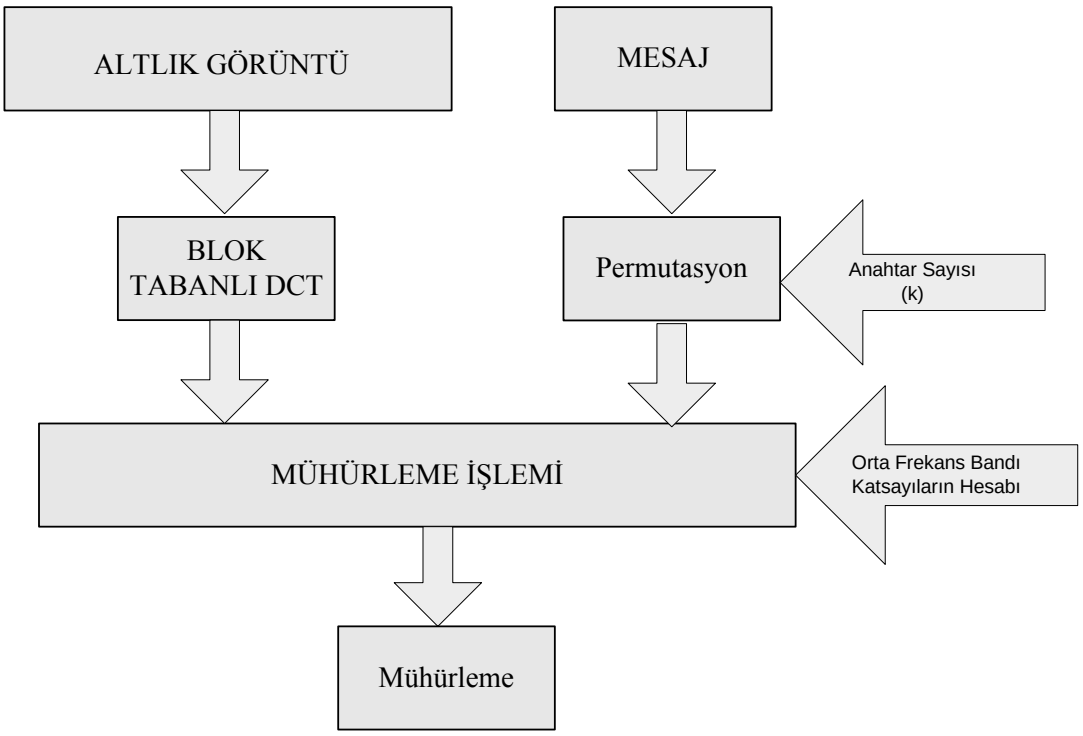
Mühürlenmiş bir görüntüye yapılan saldırıların türleri düşünüldüğünde, saldırılara karşı algoritmaların frekans düzlemini sıklıkla kullandıkları görülmektedir (HARTUNG ve KUTTER, 1999). Bu amaçla, Discrete Fourier Transform (DFT), Discrete Wavelet Transform (DWT) ve Discrete Cosine Transform (DCT) en çok kullanılan dönüştürme araçlarıdır. JPEG kayıplı sıkıştırma algoritmasında da kullanılan DCT, yaygın bir kullanım sağlamış ve pek çok çalışmada damgalama için DCT katsayıları üzerinde değişiklik yapılmıştır. Bu nedenle, çalışmamda, taşıyıcı görüntü ilk olarak JPEG sıkıştırma algoritmasında kullanıldığı gibi, 8×8 piksel boyutlarında bloklara ayrılmıştır. Ardından, DCT dönüştürme aracı ile orta band frekans (orta blok) bileşenlerinden rastgele katsayılar seçilmiştir. Damgalama işlemi, DCT ile elde edilen band frekans katsayılarında yapılan değişiklikle gerçekleştirilmiştir. Taşıyıcı görüntüye damgalanacak mesajın dayanıklılığının ve görünmezliğinin arttırılması amacıyla, damgalama öncesinde mesaja permutasyon uygulanmıştır.

Mesajın mühürlenmesinden önce altlık ve mesaj görüntülerine çeşitli ön işlem uygulaması gerçekleştirilir.

Mesaj görüntüsüne blok tabanlı DCT uygulanarak her 8x8 blokların orta frekans bandı katsayıları hesaplanır (orta frekans bandı katsayılarına AC katsayısı denilmektedir). Bu aşamada hesaplanan katsayılar mühürleme işlemi esnasında çok önemli referans noktası olarak tayin edilir. Bu katsayıların seçilmesinin en büyük nedeni insan gözünün bu katsayılara duyarlı olmasındandır.

76	74	77	105	136	122	73	37
85	112	136	137	103	49	24	35
122	104	94	102	92	48	21	32
105	81	74	92	88	47	35	65
86	84	97	118	98	42	28	62
89	83	87	101	92	50	32	52
66	79	85	79	58	34	42	76
66	79	81	71	59	44	43	59

Şekil 6.11 8X8 Boyutunda blok matris görüntüsü



Şekil 6.12 Mühürleme algoritması

Damgalama algoritması ile ilgili ara işlemler aşağıdadır.

6.4.2.1 DCT Dönüşümü

H'ın N_1xN_2 piksel boyutlarında, tüm pikselleri 0–255 renk aralığına sahip altlık görüntü olduğunu varsayalım.

$$H = \{h(x,y), 0 \le x < N_1, 0 \le y < N_2\} \tag{6.1}$$

H altlık görüntüsü öncelikle 8×8 piksellik bloklara ayrılarak bu görüntünün frekans analizi için Denklem 3.2. ile her bloğa ayrı ayrı DCT uygulanır.

$$H_b(u,v) = \alpha(u)\alpha(v)\sum_{x=0}^{7}\sum_{y=0}^{7} h_b(x,y)\cos\left(\frac{(2x+1)u\pi}{2x8}\right)\cos\left(\frac{(2y+1)u\pi}{2x8}\right) \tag{6.2}$$

Burada; b blok numarası olup $0 \le b \le \frac{N_1}{8} x \frac{N_2}{8} - 1$ arasında değer alabilir. u ve v frekans düzlemine taşınan bloğun frekans bileşenlerinin koordinatlarını, bu koordinatlardaki bileşenin değerini gösterir. $\alpha(u)$ ile $\alpha(v)$ aşağıdaki denklem kullanılarak bulunur.

$$\alpha(i) = \begin{cases} \sqrt{\frac{1}{8}}, i = 0 \\ \sqrt{\frac{2}{8}}, i = 12,...,7 \end{cases} \quad (6.3)$$

6.4.2.2 Permutasyon

Mühürleme sonucu sayısal görüntüde oluşan bozulma, kullanılan mesajın büyüklüğü ile doğru orantılıdır. Renkli ya da gri seviyeli bir mesaj yerine taşıyıcı görüntüye damgalamak için Şekil 6.9.'da görülen 20x50 piksel boyutlarındaki siyah-beyaz mesaj, M, seçilmiştir. Bu logoda, beyaz rengin piksel yoğunluğu "1" atanarak ikilik (binary) mesaja, M_b, dönüştürülür. Böylece mesajın büyüklüğü, taşıdığı bilgi değiştirilmeden en az seviyeye indirilir. Ayrıca, taşıyıcı görüntünün kırpılmasıyla kaybedilen bilginin logonun geneline yayılması için, damgalama işleminden önce ikilik logoya permutasyon uygulanır (Denklem 6.4.). Bu amaçla, bir anahtar sayı K, kullanılarak 0 ile logonun piksel sayısı arasında olan rasgele sayılar üretilir. Mesajın pikselleri, önce soldan sağa, sonra yukardan aşağıya olmak üzere numaralandırılır. Daha sonra, üretilen her rasgele sayı, mesajın bir pikselinin numarasını temsil etmek üzere, sırasıyla yan yana olan sayıların gösterdiği pikseller yerleri değiştirilerek permutasyon işlemi gerçekleştirilir. Bu işlem birden fazla da uygulanabilir.

$$M_p = P(M_b, K, M_1 x M_2) \quad (6.4)$$

Burada; $M_1 x M_2$ ikilik mesajın boyutlarını,

K, rasgele sayı üretmek için seçilen anahtar sayıyı,

M_b, ikilik mesajı,

M_p, permutasyon uygulanmış ikilik mesajı göstermektedir.

Permutasyon işleminin ardından mesaj, taşıyıcı görüntü ile aynı sayıda bloklara ayrılır. Görüntünün her bloğuna mesaj bir bloğu damgalanacaktır. Damgalama sonucu görüntü üzerinde oluşacak bozulma mesaj bloklarının büyüklüğü ile doğru orantılıdır.

6.4.2.3 Damgalama Algoritması

Damgalama için kullanılacak frekans katsayılarının seçimi, altlık görüntüye mesajın getirdiği bozulma ve mesajın çeşitli resim işleme saldırılarına karşı olan dayanıklılığı ile yakından ilgilidir. Damgalama işlemi, eğer alçak frekans bandında bulunan frekans katsayıları üzerinde yapılırsa, görüntü üzerinde gözle görülür bir bozulmaya neden olur. Ancak, kullanılacak frekans katsayıları, yüksek frekanslar arasından seçilirse, JPEG kayıplı sıkıştırma algoritmasının, kuantalama sırasında, bu banttaki frekansları göz ardı etmesinden dolayı mühürlenen mesaj kaybedilebilir. Bu iki nedenden dolayı, birçok çalışmada olduğu gibi bu çalışmada da, mühürleme için orta frekans bandından seçilen frekans katsayıları kullanılmıştır.

DCT ile frekanslarına ayrılan 8×8 piksel boyutlarındaki her blok içinde 63 frekans katsayısı bulunur. Şekil 6.13'de zikzak numaralandırılmış bir görüntü bloğu görülmektedir. Sol üstte yer alan 0 numaralı hücredeki katsayı hariç frekans katsayılarını göstermektedir. Gri renk ile doldurulmuş hücreler orta frekans bandıdır.

0	1	5	6	14	15	27	28
2	4	7	13	16	26	29	42
3	8	12	17	25	30	41	43
9	11	18	24	31	40	44	53
10	19	23	32	39	45	52	54
20	22	33	38	46	51	55	60
21	34	37	47	50	56	59	61
35	36	48	49	57	58	62	63

Şekil 6.13 Görüntü bloğu

Mühürleme işlemi için bir referans noktası belirlemek gereklidir. Bu yöntemde, orta frekans bandından katsayılar rasgele olarak alınmıştır. Kullanılacak referans katsayısı için bir de anahtar sayı k belirlenir.

$$I_{W\,x,y}(u,v) = \begin{cases} I_{x,y}(u,v) + 1 + k * W_{x,y}(u,v), & u,v \in F_M \\ Ix,y(u,v), & u,v \notin F_M \end{cases} \tag{6.5}$$

W , orta frekans bandındaki katsayıyı,

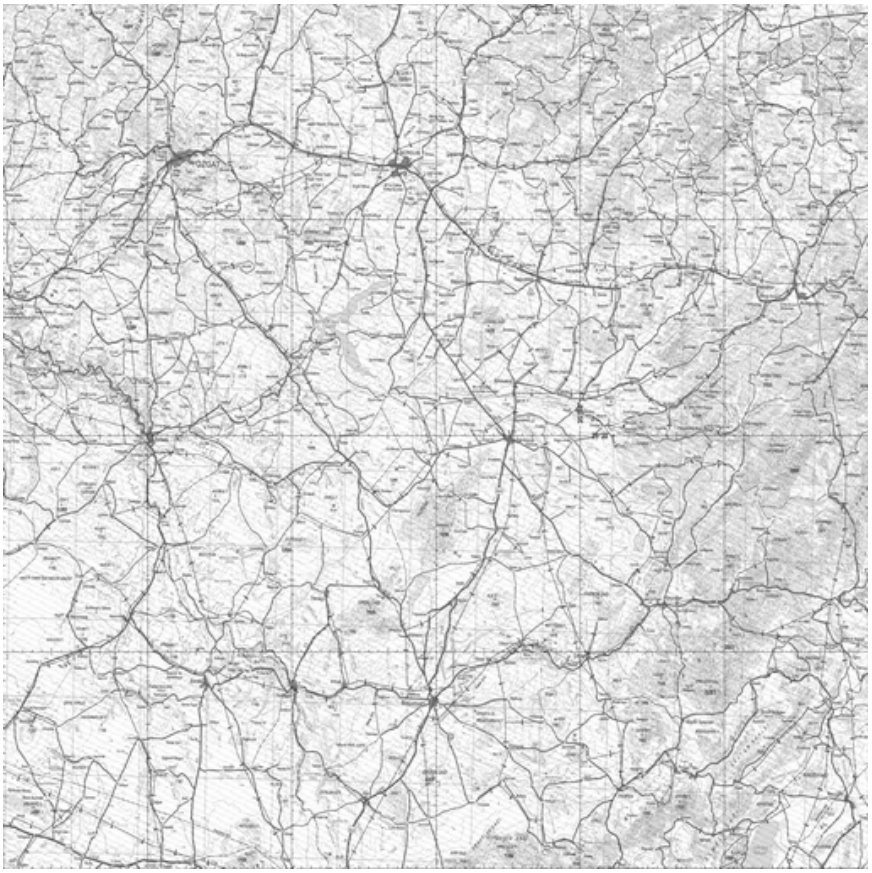
I , bloktaki piksel yerini,

k katsayıya uygulanacak anahtarı,

F_M orta frekans bandını,

I_w sonuç mühürlü görüntüyü göstermektedir.

Görüntünün her $8x8$ bloktaki yeri hesaplanır. Bu bloktaki seçilen frekans katsayısı belirlenen anahtar ile çarpılır. Bu anahtar sayısı sadece kullanıcı tarafından bilinmektedir. Ayrıca, işlemden önce belirlenebilmektedir. Bu hesaptan sonra orta band frekans katsayılarına dönüşüm gerçekleştirilir. Dönüşüm sonucu mühürlenmiş görüntüyü elde ederiz.



Şekil 6.14 Mühürlenmiş altlık görüntü

6.4.3 Mührün Geri elde Edilmesi

Altlık görüntüye mühürlenen mesajın geri elde edilmesi için asıl görüntü kullanılmaz. Görüntüden mesajın elde edilmesinde, mühürleme işleminde kullanılan frekans katsayıları ile seçilen anahtar sayı kullanılır. Öncelikle damgalanmış görüntü 8×8 piksel boyutlarında bloklara ayrılarak her bloğun frekans bileşenleri Denklem 6.4. kullanılarak hesaplanır. Mesaj taşıyıcı görüntüden geri elde edilmesi damgalanma algoritmasına benzer şekilde yapılır.

$$W_i = W_i + kW \tag{6.6}$$

Altlık görüntüden elde edilen ikilik desen, permutasyon uygulanmış mesaj verisidir. Mesaja, altlık görüntüye damgalanmadan önce bir anahtar sayı kullanılarak permutasyon uygulandığından, elde edilen mesaj verisine de aynı anahtar sayı ile aynı sayıda ters-permutasyon uygulanır (Denklem 6.7). Böylece ikilik mesajın aslı elde edilir. Son olarak elde edilen ikilik

mesajın beyaz renk “1” ile temsil edildiğinden yoğunluğu “1” olan pikseller “255” atanarak siyah-beyaz mesaj elde edilir.

$$M_p^{'} = P^{-1}\left(M_b^{'}, K, M_1 x M_2\right) \tag{6.7}$$

Şekil 6.15’de mühürleme sonucu geri elde edilmiş mesaj gösterilmektedir.

Şekil 6.15 Geri elde edilmiş mesaj

6.5 Mühürlemeye Karşı Yapılacak Saldırı Çeşitleri

6.5.1 Basit Saldırılar

Gizli ve dayanıklı bir şekilde mühürlenen mesajın yok edilmesi amacıyla yapılan basit saldırılar, görüntü kalitesinde fark edilmeyecek derecede değişiklik yapabilen çeşitli görüntü işleme algoritmalarıdır. Saldırı sonucu taşıyıcı görüntüdeki mesaj bozulabilir ya da mesaj geri elde edilemeyecek derecede zarar görebilir (ARNOLD ve ark., 2003).

6.5.1.1 JPEG Kayıplı Sıkıştırması

JPEG, günümüzde en yaygın olarak kullanılan sıkıştırma yöntemlerinden biri olmasının yanında, görüntü boyutunun küçülmesine ters oranla koruduğu görüntü kalitesi nedeniyle de tercih edilen bir sıkıştırma yöntemidir. JPEG sıkıştırması DCT kullanılarak yapılan blok tabanlı bir dönüştürme algoritmasına dayanmaktadır. Temel olarak JPEG kayıplı sıkıştırması, DCT ile dönüştürülen görüntünün yüksek frekanslı bileşenlerinin istenen sıkıştırma oranında silinmesine dayanır. JPEG algoritmasının bu özelliğinden faydalanılarak damgalanmış görüntüden mesajın yok edilmesi amaçlanır. Eğer mesaj bilgisi taşıyıcı görüntünün yüksek frekans bileşenlerine saklanmışsa, JPEG kayıplı sıkıştırması sonucu mesaj tanınabilir benzerlikte elde edilemeyecek şekilde yok olabilir. Böylece görüntü kalitesinde önemli bir düşmeye sebep olmadan mesaj yok edilebilir.

6.5.1.2 Kırpma (Cropping)

Kırpma, taşıyıcı görüntünün bir bölümünün kesilmesi ile gerçekleştirilir. Taşıyıcı görüntülere yapılan gizli ve dayanıklı damgalama işleminde damganın yeri belli değildir. Kırpma işlemi ile görüntüden ayrılan bölümde var olabilecek mesaj bilgisinin yok edilmesi ve böylece mesajın geri elde edilemeyecek derecede zarar görmesi amaçlanır. Eğer damga taşıyıcı görüntüye görünür bir şekilde yerleştirilmişse, damganın yok edilmesi için yapılabilecek en kolay saldırı kırpmadır. Bununla birlikte, damganın kırpılıp görüntüden ayrılması görüntünün bütünlüğünde ciddi bir etki bozulmaya sebep olacaksa, kırpma saldırısının yapılması, geriye kalan görüntü değerlendirildiğinde anlamsız olmaktadır.

6.5.1.3 Gürültü Ekleme

Taşıyıcı görüntülere yapılacak gizli mesaj damgalama işlemleri sonunda görüntü piksellerinin önemli bir bölümü ya da hepsi değişikliğe uğramaktadır. Dolayısıyla görüntünün değişen her pikseli damganın bilgisini taşımaktadır. Gürültü ekleme saldırısı gizli damgalama yöntemlerinin bu özelliğini hedef alır. Görüntü kalitesinde önemli bir düşmeye sebep olmayacak bir şekilde, görüntünün her pikselinin rasgele arttırılması ya da azaltılması ile gürültü ekleme saldırısı gerçekleştirilir. Böylece görüntü içindeki damga, bu saldırı sonucu değişen piksel yoğunluklarından dolayı tanınamayacak bir nitelikte bozulmuş olarak elde edilebilir.

6.5.1.4 Tekrar Damgalama

Taşıyıcı görüntüye yapılabilecek saldırılardan bir diğeri de başka bir damgalama algoritması kullanarak görüntünün tekrar damgalanmasıdır. Böylece pikseller üzerinde yapılacak ikinci

değişiklik, taşıyıcı görüntüye damgalanan ilk bilgiyi yok edebileceği gibi saldırganın da aynı görüntü üzerinde kendi haklarını savunabileceği bir bilgiyi görüntüye eklenmesine sebep olur.

6.5.2 Geometrik Saldırılar

6.5.2.1 Yatay Eksende Döndürme

Bu işlem, görüntünün yatay eksen etrafında 180 derece döndürülmesi ile yapılır. Görüntünün yatay eksende döndürülmesi kayıpsız bir şekilde gerçekleşeceğinden damgalanmış bir taşıyıcı görüntü yatay eksende tekrar döndürüldüğünde görüntünün aslı geri elde edilebilir. Böylece damgalanan bilgi bir bozulmaya uğramamış olur.

6.5.2.2 Dikey Eksende Döndürme

Görüntünün dikey bir eksen etrafında 180 derece döndürülmesi ile kayıpsız bir biçimde yapılabilir. Görüntünün kendisini elde etmek için dikey eksen etrafında tekrar döndürülmesi gerekir. Böylece görüntüye damgalanan bilgi kayıpsız bir şekilde geri elde edilebilir.

6.5.2.3 Açılı Döndürme

Genelde küçük bir açı oranında taşıyıcı görüntünün saat yönünde ya da tersi yönde döndürülmesi ile görüntü içindeki mesajın yok edilmesi amaçlanır. Yatay ve dikey eksende döndürmenin aksine açılı döndürme işleminde görüntü ebadı değişmekte ve orijinal ebat için görüntüye sonradan kırpma işlemi de uygulanmaktadır. Birçok damgalama algoritması bu saldırı türüne karşı hassastır.

6.5.2.4 Ölçekleme

Bu durum kâğıda basılmış bir görüntünün tekrar bir tarayıcıda taranması ya da Internet'te yayınlanmak üzere yüksek çözünürlüklü görüntünün çözünürlüğünün azaltılmasıyla ortaya çıkar. Ölçekleme, yatay ve dikey yönde aynı oranda yapılan ölçekleme ile farklı oranlarda yapılan ölçekleme olarak iki gruba ayrılır. Birçok sayısal damgalama algoritması aynı oranda yapılan ölçeklemeye karşı dayanıklıdır.

6.5.2.5 Satır ya da Sütunların Silinmesi

Satır ya da sütunların silinmesi, uzay düzleminde yapılan en yaygın saldırılardan biridir. Satırlar ile sütunlar sonrakilerle yer değiştirilerek ya da silinenlerin yerine yanındakilerin kopyalanması

ile gerçekleştirilen bir saldırı türüdür. Görüntü piksellerinin orijinal koordinatlarından ayrılmasıyla yapılan bu değişiklik, gözle fark edilemeyecek derecede olmasına rağmen görüntüye gizli bir şekilde damgalanan mesajın bozulmasına yol açabilmektedir.

6.5.2.6 Yok Etme Saldırısı

Yok etme işlemi, taşıyıcı görüntüye damgalanan bilgiyi sadece geri elde edilemeyecek şekilde bozmaya yönelik olmayıp onun yerinin tahmin edilip görüntüden ayrılması için yapılan saldırı türüdür. Bu saldırı ile damgalanan bilginin görüntüde sebep olduğu değişikliğin geri alınması ve böylece orijinal görüntünün elde edilmesi amaçlanır.

6.5.3 Kaliteye Yönelik Saldırılar

6.5.3.1 Filtreleme

Median filtresi ile alçak ve yüksek geçiren filtreler, sıklıkla kullanılan filtreleme çeşitleri arasında yer almaktadır. Median filtresi bir görüntünün ayrıntılarını koruyarak, üzerindeki gürültüyü yok etmek amacıyla kullanılır. Alçak geçiren filtre ile görüntünün yüksek frekanslı bileşenleri görüntüden ayrılır. Böylece daha düz ve yumuşak bir görüntü elde edilir. Yüksek geçiren filtre ise alçak frekans bileşenlerini görüntüden ayırarak daha keskin bir görüntü elde edilmesinde kullanılır. Filtreler ile yapılan saldırılarla, onların görüntü kalitesi üzerinde yaptığı değişiklikler göz önünde bulundurularak, taşıyıcı görüntüdeki mesajın bozulması hedeflenir.

6.5.3.2 Kontrast

Birçok görüntü işleme yazılımında standart olarak bulunan bir fonksiyondur. Görüntünün kontrastında yapılacak değişiklik ile yapılacak saldırı bazı damgalama algoritmaları için başarılı olabilmektedir.

6.5.3.3 Renk Kuantalama

Renk kuantalama, taşıyıcı görüntünün genelde Internet'te yayınlanacağı zaman GIF (Graphic Interchange Format) biçimine dönüştürülmesinde uygulanır.

6.6 Sayısal Coğrafi Veri İzin Dışı Kullanımı Tespit Eden Yöntem Uygulaması

Bu uygulamanın hazırlanabilmesi için izlenen yöntemler aşağıdaki gibidir:

- Sayısal coğrafi verilerinin tamamen bağımsız ve farklı bir yazılım ortamında incelenmesi

gerekmektedir.

- İncelenecek veriler iki ayrı klasör altında HARİTA ve NİRENGİ klasörleri bir araya getirilmiştir. HARİTA klasöründeki veri ile NİRENGİ klasöründeki veriler farklı operatörler tarafından gerçekleştirilmiştir.

- Her iki veri setinin, belirli olan bir (Caris) yazılımının veri formatında olması ve çalışmanın bu programdan bağımsız bir yazılım olan ArcGIS yazılımında gerçekleştirilebilmesi için format dönüşümleri gerçekleştirilmiştir. Bu işlem farklı bir (CARIS) yazılımının dönüşüm araçları ile önce uluslararası bir standart olan DXF (Drawing Exchange Format) formatına dönüştürülmüş, sonra ArcGIS yazılımının kullandığı MDB (Microsoft Database) formatına dönüştürülmüştür.

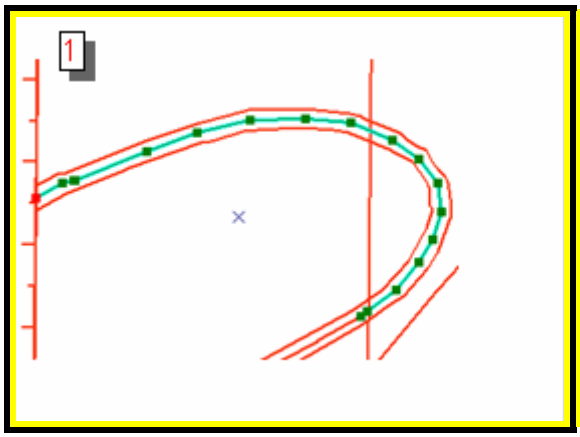
- Verilerin projeksiyon bilgileri UTM (Universal Transverse Mercator) formatı olarak belirlendiğinden dönüşümden önce tekrar düzenlenmemiştir.

- Veriler ArcMap programına uygulamanın içerisinde belirtilen klasörlerin veri kümeleri şeklinde yüklenmiştir.

- Sayısal coğrafi verilerinden bazılarının daha kolay karşılaştırma ve ayırt etme işlemi yapılabilmesi için sembolleştirilmiştir.

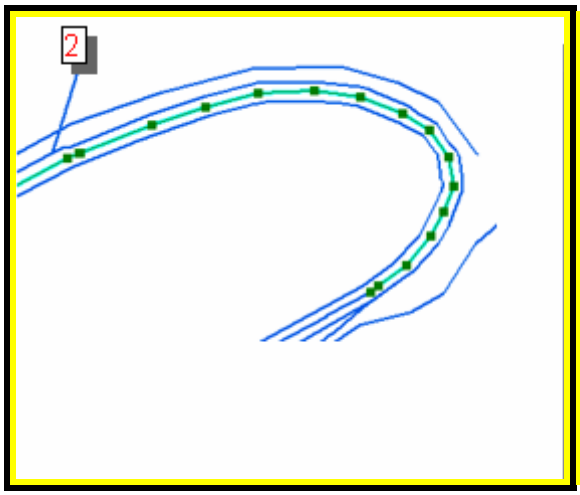
6.6.1 Aynı Kaynaktan Türetilmiş Vektör Verilerin Tespit Yöntemleri

Bu yöntemde; iki ayrı verinin aynı koordinat bölgesinden alınan harita verisi ile bilgilerin karşılaştırılması yapılmıştır. Her iki bölgede bulunan vektör veriyi oluşturan aynı nokta kümesine ait koordinat bilgileri karşılaştırılarak bir benzerlik olup olmadığı değerlendirilecektir. UTM sol alt köşesi ve sağ üst yukarı köşesi için belirlenen değerlere sahip çerçeveye giren bölgede yapılan değerlendirme sonucunda aşağıdaki görüntüde tespit edilen bilgilere rastlanmaktadır.



	X	Y	Z
0	410333,875	4043871,375	0,000
1	410335,500	4043872,500	0,000
2	410341,750	4043877,250	0,000
3	410347,000	4043883,250	0,000
4	410350,000	4043888,500	0,000
5	410352,000	4043894,500	0,000
6	410351,250	4043901,000	0,000
7	410347,000	4043906,500	0,000
8	410341,000	4043910,750	0,000
9	410331,750	4043914,500	0,000
10	410321,500	4043915,500	0,000
11	410309,250	4043915,250	0,000
12	410297,500	4043912,250	0,000
13	410286,000	4043908,000	0,000
14	410270,125	4043901,750	0,000
15	410270,000	4043901,750	0,000
16	410269,750	4043901,750	0,000

Şekil 6.16 HARİTA koordinat bilgileri ve vektör verisi



	X	Y	Z
0	410333,875	4043871,375	0,000
1	410335,500	4043872,625	0,000
2	410341,875	4043877,250	0,000
3	410347,249	4043883,626	0,000
4	410349,875	4043888,875	0,000
5	410352,125	4043894,625	0,000
6	410351,124	4043901,000	0,000
7	410347,000	4043906,875	0,000
8	410341,125	4043910,625	0,000
9	410331,626	4043914,374	0,000
10	410321,500	4043915,625	0,000
11	410309,250	4043915,250	0,000
12	410297,625	4043912,125	0,000
13	410285,874	4043908,124	0,000
14	410270,125	4043901,876	0,000
15	410269,876	4043901,876	0,000
16	410267,249	4043900,875	0,000

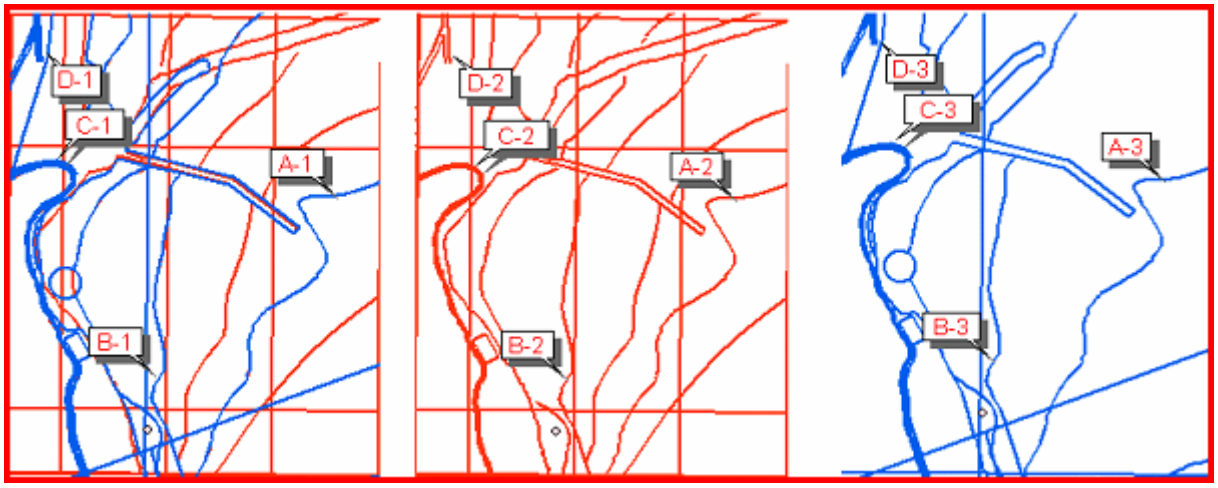
Şekil 6.17 NİRENGİ koordinat bilgileri ve vektör verisi

Şekil 7.14'teki görüntü HARİTA verisi, Şekil 7.15'deki görüntü NİRENGİ firmasının harita verisine ait bilgileri içermektedir. Her iki görüntünün sağ tarafında bulunan tablolarda, görüntülerin sol tarafındaki çizgileri oluşturan nokta kümesine ait koordinat bilgileri görülmektedir. Buna göre söz konusu çizginin her iki görüntüde de görülen parçaları aynı veya birbirine 1 metre civarında yakın koordinat değerlerine sahip noktalardan meydana geldiği apaçıktır. Dikkat edildiğinde yukarıdaki bazı noktalara ait koordinat değerleri birbirine çok yakın bazıları da aynıdır. Bu durum aynı veri kümesine ait olmadıkları sonucunu yaratmaz.

Yukarıdaki tablo değerleri arasındaki farklı değerler daha önce açıklanmış olan sebeplerden kaynaklanmaktadır. Bu koordinat çiftlerinin arasındaki farklar, HARİTA verisinin hangi işlemlere tabi tutulduğu bilinmediğinden, NİRENGİ firmasının üretim aşamasında haritaya uygulanan projeksiyon dönüşüm işleminden kaynaklanmaktadır. Dolayısıyla bu çizgiyi oluşturan nokta kümesinin birbirinin aynısı olduğu değerlendirilebilir. Her iki veride de bulunan çizgileri oluşturan nokta sayıları ve doğru parçalarının aynı olmasının rastlantısal bir durum olmadığı

değerlendirilmektedir. Tüm bu bulgular ışığında; her iki veri kümesinin birbirinin kopyası olduğu açıkça ortadadır.

Aşağıdaki Şekil 23'te görülen A, B, C ve D işaretleri ile gösterilen çizgi detaylarının aynı veri olduğu, Aynı Kaynaktan Türetilmiş Vektör Verilerin Tespit Yöntemleri kullanılarak tespit edilmiştir. Şekilde üst üste örtüştüğü tespit edilen çizgi detaylar üzerinde detaylara ait karakteristik özelliklerin karşılaştırıldığında aynı veri olduğu anlaşılmaktadır.



Şekil 6.18 HARİTA ve NİRENGİ firmalarına ait çizgi detaylar

7. SONUÇLAR ve ÖNERİLER

Haritalar insanların kendilerine yurt edinme duygusunun kazanılmasından itibaren kullanılmaya başlanmıştır ve teknolojide meydana gelen büyük atılımlarla değişim geçirmiştir. CBS'nin teknoloji ile birlikte kullanımıyla harita üzerinde yapılan karmaşık analizler sayısal ortamda bilgisayarlar tarafından yürütülmüştür. Sayısal veri kavramının oluşmasından sonra ülkeler bu verileri kullanarak sayısal harita üretimine geçiş yapmıştır. Bu verilere ulaşmanın sistematik bir yapıya dönüştürülmesi için veritabanları oluşturuldu. İnsanların coğrafi ve konumsal verilere ihtiyaçlarının artmasıyla CBS yazılım sistemleri kuruldu.

Haritaların üretim aşamasında, bilgisayar yazılımlarının hazırlanması ve kullanıcılara sunulması, veri tabanlarının oluşturulması ne kadar pahalı ve alın teri gerektiriyorsa o kadar bunların kopyalanması ucuz ve kolaydır. Birçok mühendisin, büyük emek ve zaman harcayarak yarattığı ürünleri bire bir kopya edilmesi veya taklit edilerek benzerinin üretilmesinin, diğer ürünlere göre daha kolay ve ucuz olması bu alandaki ihlalleri arttırmıştır.

Haritalar, bilgisayar programları ve veri tabanları, uluslararası platformda birer eser olarak kabul edilmiş, eser sahibi hakları kapsamında koruma altına alınmıştır. Haritalar XX. Yüzyılın başından beri korunuyorken, bilgisayar programları ve veri tabanları, 1990'lı yılların ortalarında dünya genelinde koruma altına alınmıştır. Haritalar herkesin bildiği bilgilerin yorumlanması ve daha sonra sunulmasındaki orijinallik nedeniyle artık bir eserdir.

Türkiye'de sanat eserlerin korunması konusunda 1951 tarihinde yürürlüğe giren ve bugüne kadar 1983, 1995, 2001 ve 2004 yıllarında değişikliğe uğrayan 5846 sayılı Fikir ve Sanat Eserleri Kanunu (FSEK) uygulanmaktadır. 2001 yılında yapılan değişiklik uluslararası düzeyde yapılan anlaşmaların getirmiş olduğu zorunluluktan dolayıdır. 1996 yılında Avrupa Birliğinde veritabanları ilgili değişikliği kabul etmesinden sonra Türkiye'de yürürlülüğe girmemesi haritacılık sektörüne büyük zararlar vermiştir. FSEK'te sayısal coğrafi veriler korunmamaktadır, verilerin korunma konusunda Türk Ceza Kanunu işletilmiştir. Steganografya güvenlik için geliştirilmiş bir tekniktir. Steganografya kriptolamanın yerine planlanmamıştır onu destekleyen bir tekniktir. Steganografya ile bir mesajı saklamak onu sadece bulunma şansını azaltır. Fakat şifreleme çözülebilir ya da kırılabilir.

Sonsuz sayıda Steganografya tekniği çıkartılabilir. Bu çalışmada Steganografya tekniğinin bir kısmından bahsedildi. Haritacılıkta bir görüntü içerisine mesaj saklama tekniği daha önemlidir. Steganografya gizlilik için iyi bir çözüm değildir fakat, ne basit bir yerine koyma işlemidir ne de şifreleme tekniğinin değişik biçimidir. Ama bu özellikler birleştirilirse güçlü bir şifreleme yöntemi oluşturulabilir.

Steganografya bir gizliliğin açık taraflarını örtmek için tamamen zararsız bir şekilde verileri iletme çabası içerisindedir. Sayısal görüntü steganografyası ve onun türevleri uygulaması ve kullanımı gelişim içerisindedir. Bu alanda kriptolama ve güçlü şifreleme işlemleri yasa dışıdır. Kullanıcılar artık steganografyaya bir mesajın gizlenmesi politikalarını arıyorlar. Sayısal mühürleme ve sayısal işaretleme formunda steganografya uygulamaları eser koruma hakları ve elektronik medya mülkiyetini belirtmek için kullanılmaktadır. Yapılan araştırmalar ve soruşturmalar incelendiğinde uygulama çok güçlü çözümler vermiştir. Tasarlamada sağlam bir mühürleme sisteminin eser haklarını koruma ve lisanslama bilgileri gibi yerleştirilmiş bilgilerin korunmasını diğer uygulamalara göre daha önemlidir. Güçlendirilmiş mühürleme tekniklerinin gelişimi için mühürlemenin hayatta kalabilme yeteneği belirten araçlar çok önemlidir. Çalışmada sayısal mühürleme araçlarını ve yöntemler tanıtılmıştır. Burada görüldüğü gibi mühürleme araçlarıyla mühürleme tekniğini uygulamak çok az bir çaba gerektirmiştir.

Belki de birçok mühürlemenin doğasındaki güçsüzlüğü yaklaşımının olması, görülebilir mühürlemenin bir dosya içerisinde mevcut olmasındadır. Steganografya tekniği ile yerleştirilmiş mesajın varlığını veri kullanıcıları tespit edemeyecektir bundan dolayı da işareti uzaklaştırmak için bir girişim olmayacaktır. Bazı mühürleme sistemleri Adope Photoshop gibi yazılımlarla dağıtılabilir. Herhangi bir internet aracı kullanılarak mühürleme kırılabilir. Belki teknolojinin gelişmesiyle gelecekte geçerli olan altlığa “dövülmüş” mühürleme kullanılarak ekleme yapılabilecektir. Şunu belirtmek gerekir ki insanoğlu eğer bir örtü ile bilgiyi gizleyebiliyorsa, yine insanoğlu yerleştirilmiş bilgiyi yıkarak yeni bir sistem geliştirilebilir. Çalışmada mümkün olduğunca dünyada kullanılan veri saklama, koruma ve görüntü içerisine metin yerleştirme araçları tanıtıldı. Daha önce coğrafi verilerin teknik koruması ile ilgili bir çalışma olmadığından, ülkemizde bu konuda kaynak sayısı yok denecek kadar kısıtlıdır. Bu çalışmada sayısal coğrafi verilerin korunmasına yönelik mevcut yöntemler araştırılmış ve bunlarla ilgili uygulamalar gerçekleştirilmiştir. Gelecekte daha güvenli koruma yöntemleri mutlaka geliştirilecektir.

7.1 Öneriler

Sayısal coğrafi verilerinin koruma yöntemlerinin, fikri haklar endüstrisinde ve yan endüstrilerde yeni kaynaklar oluşturması ve yetkisiz kullanımı önlemeye yönelik etkin olması sebebiyle kurumlar tarafından benimseneceği ve geniş kapsamda kullanılacağı açıktır. Ancak eser sahibi hakları, karşılıklı işlerlik, rekabet, etkin ve planlı gibi hususlardan dolayı sayısal coğrafi verilerin korunmasına yönelik uygulamaları ile ilgili esasların belirlenmesi ve bu doğrultuda denetlenmesi gerekir.

Yukarıda belirtilen düzenlemelerle etkin bir sistem gerçekleştirilebilir. Bu sistemle, yasallaştırmanın öngörebileceği değişikliklerle bağlayıcılık özelliği kazandırılır ve ulaşılması gereken hedefler belirlenir.

Bu sistemin sağlanabilmesi, yasalarla desteklenen ve sektörler arası iletişimi sağlayan yapısı ile birlikte bağımsız bir kurumsal yapının oluşturulması gerekir. Bu kurumsal yapı Başbakanlığın bünyesinde, uluslararası ilgili kamu kurumları, hak sahipleri, meslek birlikleri, üniversite ve üretici kuruluşlarından oluşturulabilir.

Bu doğrultuda oluşturulacak kurumsal yapı öncelikle ilgili kurumları, eser sahiplerini, bağlantılı hak sahiplerini sayısal coğrafi veri hakları konusunda bilinçlendirmek ve kullanabilirliği artırmak için gerekli tanıtım ve bilgilendirme çalışmaları yağılmalıdır. Çalışmalar geniş kapsam içerisinde ele alınarak ilgili birimlere teknik ve hukuk danışmalık ve eğitim hizmetlerinin verilmesini içermelidir.

Kurumsal yapı eser sahipleri haklarının korunması için gerekli denetleme organizasyonunu kendi içerisinde oluşturmalıdır. Özellikle ülke içerisinde kullanılacak veri koruma yöntemleri teknolojileri arasında karşılıklı standardın sağlanabilmesi amacıyla kurumsal yapı ilgili sektör ve kurumlar arasındaki iletişimi sağlamalı ve gerektiğinde uzlaşma yöntemleri geliştirmelidir. Ayrıca sayısal coğrafi ürünlerinin korunması açısından, koruma yöntemleri ile ilgili araştırma çalışmaları ve hukuka uygunluk analiz çalışmaları gerçekleştirmeli ve sonuçlarını ilgili kamu ve tüzel kişilere duyurmalıdır.

E-Devlet kapsamında sayısal coğrafi verilerin korunmasında kullanılacak teknolojiler ile ilgili uluslararası standardın sağlanması, ülke görüşlerinin hazırlanması ve bunların dile getirilmesi söz konusu kurumun görev ve sorumluluğunda olması gerekir. Ayrıca kurumsal yapı metaveri,

lisans tanımlayıcı gibi konularda uluslararası kuruluşların Türkiye kayıt yöneticisi görevini yerine getirebilir.

Ulusal Bilgi Güvenliği Teşkilatı Kurulması Hakkında Kanun Tasarı Taslağı TBMM'e sunulmuştur. Taslak, ülkemizin ulusal bilgi güvenliği politikasının kapsamını ve çerçevesini belirlemesi, politikayla ilgili sorumlu kurum ve kuruluşları vizyon, yetki ve yapılandırma açılarından düzenlemesi nedeniyle olumlu bir yasal gelişmedir. Ancak, taslakta belirtilen Ulusal Bilgi Güvenliği Kurumunun yapı, yetki ve görev tanımları ve sınırları yukarıda anlatılar kapsamında yeniden düzenlemeler yapılmalıdır. Kurum'un yapılanmasında Avrupa Birliği için akademik ve danışma açıdan benzer bir yapıda olan diğer organizasyon yapısı, çalışmaları ve hedefleri göz önünde tutulmalıdır.

KAYNAKLAR

Acun, R., (2000), "D.P.T.VIII nci beş Yıllık Kalkınma Planı Fikrî Haklar Özel İhtisas Komisyonu Raporu", Ankara, 2000.

Anderson, Ross J, Fabien, AP Petitcolas, (1998), "On the Limits of Steganography. IEEE Journal on Special Areas in Communications", 16(4):474-481, May 1998.

ARNOLD, M., SCHMUCKER, M. and WOLTHUSEN, S. D., (2003), "Techniques and Applications of Digital Watermarking and Content Protection", Artech House, 273, London.

Aura, T., (1995), "Invisible Communication," EET 1995, technical report, Helsinki Univ. Of Technology, Finland, Nov. 1995.

Ayiter N., (1981), "Hukukta Fikir ve Sanat Ürünleri", Sevinç Matbaası.Ankara, 1981.

Baytan, D. (2001), "İbrahim NALCI' nın Kişisel Görüşmesi(Avukat)", Kültür Bakanlığı Uzman Personeli, 2001.

Belgesay, M. R., (2001), "Fikir ve Sanat Eserleri Kanunu Şerhi", Temel Yayınları, İstanbul, 2001.

Bender, W., Gruhl, D., N Morimoto, N., Lu A., (1996), "Techniques for data hiding", IBM Systems Journal, Vol 35, No 3&4, 1996.

Beşiroğlu, A., (2000), "D.P.T.VIII nci beş Yıllık Kalkınma Planı Fikrî Haklar Özel İhtisas Komisyonu Raporu", Ankara, 2000.

Beşiroğlu A.(1999) "Düşünce Ürünleri Üzerine Haklar", Ankara Patent Bürosu, Ankara, 1999.

Brassil, J., Low, S., Maxemchuk, N. O'Gorman, L., (2004), Electronic Marking and Identification Techniques to Discourage Document Copying.

Brown A., (2004), S-Tools forWindows,1994, (16 Mart 2004)

Buke A., (2004), Steganografi, IEEE Reports, 2004

Cox et all, I. (1996), "A Secure, Robust Watermark for Multi-Multimedia,"Proc. First Int'l Workshop Information Hiding, Lecture Notes in Computer Science No. 1, 174, Springer-Verlag, Berlin, pp. 185-206, 1996.

Dericioğlu, K., (1998) " Orta Doğu Teknik Üniversitesi Mimarlık ve Mühendislik Fakültesi Fikri Haklar Ders Notları", 2002. http://www.apb.com.tr/dersler (09 Mart 2004)

Erel Ş., (1998), "Türk Fikir ve Sanat Hukuku", İmaj Yayıncılık, Ankara, 1998.

Franz, E., Jerichow, A., Moller, S.,Pfitzmann, A., Stierand, I.., (1996), "Computer Based Steganography. In Information Hiding", Springer Lecture Notes in Computer Science, v1174, 1996.

Fred, M., Gordon, W Braudaway, Alan, E, Bell., (1998), "Opportunities for Watermarking Standards", In Communications of the ACM, v 41, no 7, July 1998.

Gökcü, S**., (**2000), "Devlet Planlama Teşkilatı Sekizinci Beş Yıllık Kalkınma Plân Fikri Haklar Özel İhtisas Komisyonu Raporu", Ankara Türkiye, 2000.

Gökyayla, K.E., (2000), "Telif Hakkı ve Telif Hakkının Devri Sözleşmesi", Yetkin Yayınları, Ankara, 2000.

HARTUNG, F. and KUTTER, M., (1999), "Multimedia Watermarking Techniques", Proceedings of IEEE, 1079-1107.

Huber, B., (2004), "GIS & Steganography - Part1", Directions Magazine, 2002a.

Huber, B., (2004), "GIS & Steganography – Part3: Vector Steganography", Directions Magazine, 2002c

Johnson, N.F., Jajodia, S., (1998), "Exploring Steganography:Seeing the Unseen", Computer Journal, No. February-1998, s26-34.

Kurak, C, Mchugh, J.,(1992), "A Cautionary Note On,Image Downgrading", Proc. IEEE Eighth Ann. Computer Security Applications Conf., IEEE Press, Piscataway,N.J., 1992, pp. 153-159.

Linnartz, JP, AAC, Kalker, GFG, Depovere, RA, Beuker, (1992), "A reliability model for the detection of electronic watermarks in digital images", IEEE Press, 1992, pp.123-131.

Nalcı, İ., (2002), "Harita, Coğrafi Bilgi Sistem Yazılımları ve Coğrafi Veri Tabanlarının Hukuki olarak Korunmasına Yönelik İnceleme",Yüksek Lisans Tezi, 2002

Pfitzmann, B., (1996), "Information Hiding Terminology," Proc.First Int'l Workshop Information Hiding, Lecture Notes in Computer Science No. 1,174, Springer-Verlag, Berlin,1996, pp. 347-356.

Pfitzmann, B., (1996), "Information hiding terminology", Information hiding: first international workshop, Cambridge, UK, May 1996.

Raymond, B Wolfgang, Christine, I. Podilchuk, Edward, J. Delp, (2002), "Perceptual Watermarks for Digital Images and Video", Cambridge, UK, 2002

Shaw, S., (2004), "Overview of Watermarks, Fingerprints and Digital Signatures", Reports of the University of Edinburgh, 1998. <http://www.jtap.ac.uk/reports/htm/jtap-034.html> (25 Mart 2004).

SHIH, F. Y. and WU, S. Y. T., (2003), "Combinational Image Watermarking in the Spatial Domain and Frequency Domains", The Journal of Pattern Recognition, 36 (2003): 969-975.

Şerbetci, M., (1996), "Haritacılık Bilimi Tarihi", HGK, Harita Dergisi Özel Sayı No: 15, Ankara, 1996

Talay, M.İ., (2000), "Kültür Bakanı,Kültür Bakanlığı Telif Hakları ve Sinema Genel Müdürlüğü Fikir ve Sanat Eserleri Kanunu ve İlgili Mevzuat", 2002,Ankara.

Taştan, H., (2003) Coğrafi Bilgi Sistemleri ve Jeodezik Ağlar Çalıştayı, Coğrafi Bilgi Sistemlerinde Telif Hakları ve Veri Koruma Yöntemleri, 24-26 Eylül 2003, Konya

Taştan, H., Maraş, H., Şahin, K., Kurt, M., Ünlü, T., Çağlar, Y., Yılmaz, E., (2000) Raster Harita Sayısal Mühürleme (Telif Hakları Koruma) Sistemi Konulu, 3996- -01/Sis. Giş. Ve Uyg. Ş. (01), BSDD Tarafından Hazırlanan Andıç, Mayıs 2002, HGK, Harita Dergisi, Sayı No: 124, Ankara, Temmuz 2000

Thoen, B., (2002), GIS & Steganography – Part2: As Applied to Mapinfo and Arcview, Directions Magazine, 2002

INTERNET KAYNAKLARI

[1]www.directionsmag.com/article.php?article_id=1

[2]www.cl.cam.ac.uk/~fapp2/papers/steganography/bibliography/05415 6.html

[3]www.directionsmag.com/article.php?article_id=195

[4]www.directionsmag.com/article.php?article_id=1

[5]www.tursign.com/products/steganography.htm

[6]ftp://idea.sec.dsi.unimi.it/pub/security/crypt/code/s-tools3.zip

[7] //deadlock.hut.fi/ste/ste_html.html

[8]www.cl.cam.ac.uk/~fapp2/papers/jsac98-limsteg

ÖZGEÇMİŞ

Doğum tarihi	05.12.1979	
Doğum yeri	Çorum	
Lise	1993-1997	Kuleli Askeri Lisesi
Lisans	1997-2002	Kara Harp Okulu
Lisans	2002-2004	Harita Genel Komutanlığı Harita Teknik Yüksek Okulu

Çalıştığı kurum(lar)

2002-	Harita Genel Komutanlığı Bilgi Sistem ve Destek Dairesi Başkanlığı