Güvenlik Kamera Görüntülerindeki Tarih ve Zaman Sayacı Üzerinde Yapılan Manipülasyonların Tespit Edilebilirliği

Araştırma Makalesi/Research Article

Refik SAMET[1], Metin ATILGAN[2]

[1] Bilgisayar Mühendisliği Bölümü, Mühendislik Fakültesi, Ankara Üniversitesi, Ankara, Türkiye
[2] Adli Bilişim Programı, Adli Bilimler Enstitüsü, Ankara Üniversitesi, Ankara, Türkiye
refiksamet@gmail.com, metinatilgan@gmail.com
(Geliş/Received:17.04.2018; Kabul/Accepted:04.10.2018)
DOI: 10.17671/gazibtd.415932

Özet— Güvenlik kamera kayıtlarına ait görüntüler adli görüntü inceleme çalışmalarında önemli rol oynamakta ve bu çalışmalar sonucunda mahkemede delil olarak kullanılmaktadırlar. Ancak teknolojinin gelişmesi ile birlikte görüntüler üzerinde manipülasyon yapılması daha kolay hale gelmiş ve delillerin geçerliliğinin sorgulanması sonucu doğmuştur. Güvenlik kamera görüntüleri üzerinde bulunan tarih ve zaman bilgileri DVR (Digital Video Recorder) cihazları tarafından atanmakta olup, video düzenleme programları ile manipüle edilebilmektedir. Dolayısıyla kovuşturma aşamasında mahkeme tarafından güvenlik kamera görüntüleri üzerinde bulunan tarih ve zaman sayacı üzerinde manipülasyon olup olmadığına yönelik inceleme yapılması talep edilmektedir. Bu çalışmada güvenlik kamera görüntüleri üzerinde tarih ve zaman sayacının manipülasyon yöntemleri, bu tür manipülasyonların tespit imkânı ve sonuç olarak görüntüler üzerindeki tarih ve zaman bilgilerinin geçerliliği hususlarından bahsedilecektir.

Anahtar Kelimeler— güvenlik kamera görüntüleri, manipülasyon, tarih ve zaman sayacı, sayaç bilgilerinin geçerliliği, kapalı devre kamera sistemi

Detectability of Manipulations Made on Counter of the Date and Time on Images of Security Cameras

Abstract— Images belonging to security camera records play an important role in forensic imaging studies and the results of these studies are used as evidence in the courts. However with the development of the technology, it has became easier to make manipulations on the images and as a result go that the question of the validity of the evidence was born. The date and time informations on the security camera images assigned by DVR devices can be manipulated with video editing programs. Therefore it is requested that the court should make investigations on the date and time of the images of the security cameras if there is manipulation or not during the prosecution. In this study the methods of changing date and time counters on security camera images, the possibility of detecting such manipulations and consequently the validity of date and time information on images will be mentioned.

Keywords— security camera images, manipulation, date and time counter, validity of counter information, closed circuit camera system

1. GİRİŞ (INTRODUCTION)

Günümüzde meydana gelen adli vakalarda ilk olarak başvurulan ve olayların dilsiz tanığı olarak nitelendirilen görüntü delilleri soruşturmalarda birçok karanlık yerleri aydınlığa çıkarmaktadır. Hiçbir tanığın bulunmadığı bir bölgede konumlandırılmış olan bir güvenlik kamerası birçok tanığın üstleneceği misyondan daha fazlasını üstlenmekte ve soruşturmacı birimlere önemli derecede yardımcı olmaktadır.

Görüntü delillerinin adli bilimler alanında önemli bir yeri olmasına rağmen soruşturmacı birimlerin yanıltılması amacıyla bu delillerin karartılmaya çalışılması da ayrı bir problem olarak ortaya çıkmıştır. Kullanımı kolaylaşan görüntü düzenleme programları görüntü delillerinin manipüle edilmesinde kullanılan önemli araçlar olmuşlardır. Mahkemelere sunulan görüntüler üzerinde manipülasyon yapıldığını gösterir bulguların ortaya çıkması ve bu durumun yaygınlaşması, mağdurun mağduriyetini giderecek bulguların delil olarak kabul edilmesini sağlayacak tespitlerin yapılmasını mecbur kılmıştır.

Güvenlik kameraları halkın girebileceği açık alanları izlemek amacı ile kullanılır. Bu durum genellikle gizliliği ifade eden, mahremiyet ve kişisellik gibi insan haklarını geçersiz kılar. Çünkü sokaklar ve caddeler üzerinde bulunan kişi kendisini toplumun dışarısına çıkaramaz. Kural olarak, insanlar olağan işler sebebiyle gerçekleştirdiği aktivitelerin doğasına uygun hareket ederler [1].

Yıllar öncesinde güvenlik kameralarını siyah beyaz kayıt yapan cihazlar olarak değerlendirmemize rağmen günümüzde yüksek çözünürlükle ve dijital olarak görebiliyoruz. Kızılötesi (Infrared cameras) ve ısıya hassasiyeti olan (Thermal cameras) kameralar geceleri dahi uzak mesafeleri görebilmektedir. Mikrodalga kameralar (Microwave cameras) kişilerin elbise altında bulunan nesneleri görüntüleyebilmektedir. Güvenlik kameraları tarafından üretilen görüntüler özel görüntü işleme yazılımları tarafından işlenebilir ve kişisel bilgileri muhafaza eden veri bankalarına taşınabilirler. Bu durum ise görsel bilgilerin toplanmasına ve geliştirilmesine yeni bir boyut kazandırmıştır [1].

Güvenlik kamera görüntüleri, adli vakalar içerisinde her tür suçun tespitinde başvurulan bulgulardır. Soruşturma aşamasında kullanılan güvenlik kamera görüntülerinin delil niteliği kazanabilmesinin en önemli yolu üzerinde bulunan bilgilerin varlığı ve bu bilgilerin geçerliliğidir. Her güvenlik kamera görüntüsü üzerinde tarih ve zaman bilgisi, kaydı yapan kameranın bilgisi bulunmakta ve bu bilgilere yardımcı olarak koordinat bilgileri, konum bilgisi gibi bilgilerde bulunabilmektedir. Ancak bu görüntüler üzerinde ilk yapılabilecek manipülasyonların başında tarih ve zaman sayaçlarının değiştirilmesi gelmektedir. Şüphelilerin başvurduğu yöntemler, kayıt cihazı kullanarak tarih ve zamanın değiştirilerek farklı bir sayacın atanmasını sağlamak ya da kayıt cihazından çıkarılmış görüntülerde tarih ve zaman sayacı üzerinde görüntü düzenleme programları kullanılarak manipülasyon yapmaktır. İlk yöntem gerçekleştirildiğinde eldeki görüntü teorik olarak manipüle edilmemiş orijinal görüntüdür ve üzerinde yapılacak tespit analizleri herhangi bir sonuç vermez. Çünkü sonradan DVR cihazı tarafından görüntü üzerine atanan sayaç üzerinde değişiklik görüntünün üzerinde bir bozulmaya sebep olmaz, yapılan değişiklik sayacın kendisi ile ilgilidir ve bu sebeple analizlerde belirgin sonuçlara ulaşılamaz. Ancak ikinci yöntemde elde edilen orijinal görüntü üzerinde dijital ortamlarda yazılımlar aracılığı ile işlemler yapılır. Bu sebeple görüntülerin orijinalliği bozulmuş olur. Bu tür değişikliğin tespit edilebilme olasılığı ise çok düşüktür.

Delil olarak kabul edilen görüntüler üzerinde incelemeler yapılır iken tarih ve zaman sayacı üzerinde değişiklik yapılmış olabileceği göz önünde bulundurulmalı ve olaylar ile görüntüler arasında mantıksal bağların kurulup kurulmadığı soruşturmanın her aşamasında kontrol edilmelidir. Bu tür manipülasyonların olup olmadığına yönelik yapılacak incelemelerde görüntü düzenleme yazılımlarına haiz uzmanların analiz yapması sağlanmalıdır. Bu sayede analizi yapacak olan uzman şüphelinin bırakabileceği hataları/izleri tahmin edebilecek ve daha sağlıklı bir inceleme yapabilecektir. Uzmanlar, yazılımsal analizlerde EXIF (Extended File Information) bilgilerine, sinyal analizlerine, gürültü modeli analizlerine, görsel incelemelerde ise sayacın bulunduğu bölgede özellikle sayacın kenar kısımlarını temsil eden piksellere yoğunlaşmalıdırlar.

Görüntü inceleme alanında güvenlik kamera görüntüleri üzerinde manipülasyon olup olmadığına yönelik yapılan incelemelerde tarih ve zaman sayacının akışına dikkat edilir. Eğer sayacın akışında bir kopukluk yok ise yani herhangi bir sayaç atlaması bulunmuyor ise görüntüler üzerinde atlama veya kesiklik olmadığına yönelik rapor verilir. Bu durum alışılagelmiş yanlış bir inceleme metodudur. Tarih ve zaman sayacı üzerinde profesyonelce gerçekleştirilmiş olan manipülasyonların tespit edilemediği, uzmanların böyle bir ihtimali göz ardı ettiği durumlarla da karşılaşılmaktadır.

Yapılan literatür araştırmalarında da bu tarz manipülasyonlar ve bu manipülasyonların tespiti ile ilgili olarak herhangi bir araştırmanın yapılmadığı tespit edilmiştir. Görüntüler üzerinde yapılan manipülasyon tespit çalışmaları, kopyala-yapıştır, silme-ekleme vb. tekniklerin ortaya çıkarılmasına yönelik çalışmalardır.

Bahsi geçen manipülasyon teknikleri tarih ve zaman sayaçları üzerinde değil kamera kadrajında bulunan görüntü sahnelerinde gerçekleştirilir. Bu çalışmalarda sayısal görüntü işleme teknikleri kullanılarak görüntünün dijital özellikleri incelenir ve bu özelliklerin birbiri ile olan ilişkileri ele alınır. Bu makalenin amacı ise güvenlik kamera görüntülerine ait tarih ve zaman sayacı üzerinde yapılan manipülasyonu ortaya koyarak bu ihtimalin göz ardı edilmemesini ve incelemelerin daha sağlıklı yapılmasını sağlamaktır. Bu çalışmada güvenlik kamera görüntüleri üzerinde tarih ve zaman sayacının değiştirilme yöntemleri, bu tür manipülasyonların tespit imkânı ve sonuç olarak görüntüler üzerindeki tarih ve zaman bilgilerinin doğruluğu hususlarından bahsedilecektir.

2. GÜVENLİK KAMERASI VİDEO VE GÖRÜNTÜLERİNİN ÖZELLİKLERİ VE BU ÖZELLİKLERİN MANİPÜLASYONU (FEATURES OF VIDEO AND IMAGING OF SECURITY CAMERAS AND MANIPULATION OF THESE FEATURES)

Güvenlik kamera görüntüleri genel olarak şüphelisi bilinen olaylarda destekleyici bir delil olarak kullanılsa da, soruşturmayı daha ileriye götürebilecek güçlü bir delildir [2].

2.1. Güvenlik Kamerası Video ve Görüntülerinin Özellikleri (Features of Video and Imaging of Security Cameras)

Bu altbölümde, güvenlik kamera sistemlerinden elde edilen görüntüler üzerinde yapılan incelemeler esnasında incelemeyi etkileyen başlıca özelliklerden bahsedilecektir.
1) Video sıkıştırma ve aktarım standartları (Video Compression and Transfer Standards);
2) Saniye başına düşen kare sayısı (FPS - Frame Per Second);
3) Çözünürlük (Resolution);
4) Tarih ve zaman bilgisi (Date and Time Information);
5) Dijital video kaydedici cihazı (DVR - Digital Video Recorder);
6) Operatör tarafından manuel yöntemlere müdahaleler;
7) Genişletilmiş dosya bilgisi (EXIF - Extended File Information);

2.1.1. Video sıkıştırma ve aktarım standartları (Video Compression and Transfer Standards)

Son yıllarda, SMPTE (Society of Motion Picture and Television Engineers) ve IEEE (The Institute of Electrical and Electronics Engineers) gibi standardizasyon organizasyonları tarafından birtakım video sıkıştırma ve aktarım standartları geliştirilmiştir [3]. Bu standartlara ait özet bilgi Tablo 1' de verilmiştir:

Tablo 1. Video Sıkıştırma ve Aktarım Standartları
(Video Compression and Transfer Standards)

SN	Standart	Açıklama
1	Motion JPEG	Video, JPEG resim serisi şeklinde görüntülenir.
2	Motion JPEG 2000	Resim serilerinin görüntülenmesi standardıdır. JPEG'e göre daha kaliteli sıkıştırma sağlar.
3	MPEG-1	JPEG'e ait sıkıştırma tekniği kullanılır.
4	MPEG-2	4 Mbps veya daha üzerinde bağlantıya sahip ağlarda kullanılan TV aktarım standartlarındandır. Yüksek görüntü kalitesine sahiptir ve HDTV yayınlarında kullanılan tarama tekniklerine sahiptir
5	MPEG-4:	MPEG-4, mobil cihazları, yüksek kalitede neredeyse limitsiz bant genişliğine sahip uygulamaları ve aynı zamanda düşük bant genişliğine sahip uygulamaları destekler.
6	H.261:	H.261 video konferansı destekleyen ve bunun için geliştirilmiş algoritmaları içeren bir standarttır.
7	H.263:	Görüntü kalitesi H.261'den daha yüksektir ve ½ piksel tabanlı görüntü kestirimi tekniğini kullanır. Yarım piksel teknikleri düşük çözünürlüklü görüntülerde daha iyi çalışmaktadır.
8	H.264:	MPEG ve video kodlama uzmanları tarafından geliştirilen bir standarttır. Günümüzde en yaygın olarak kullanılan standartlardan birisidir.

2.1.2. Saniye başına düşen kare sayısı (FPS - Frame Per Second)

Dijital video, dijital görüntü kaydının 4B olarak bilinen zaman boyutunda yayılmasıdır. Bundan dolayı dijital video içerisinde "frame" olarak adlandırılan parametre ortaya çıkar. Bir saniye içerisindeki resim karelerinin sayısına FPS (Frame Per Second) denilir. Genellikle FPS, dijital video ve film endüstrisinde "frame rate" olarak adlandırılır [4].

2.1.3. Çözünürlük (Resolution)

Bir video görüntüsünün çözünürlüğü, video kaydı içerisindeki her bir görüntü karesindeki piksel sayısı şeklinde tanımlanmaktadır. Yaygın olarak kullanılan çözünürlük standartları Tablo 2'de verilmektedir.

Tablo 2. Çözünürlük standartları
(Resolution Standards)

Görüntü Modu	Çözünürlük	En: Boy	Tipik Aygıt
QVGA	320 x 240	4:3	PDA'lar ve küçük video oynatıcılar
VGA	640 x 480	4:3	Monitör ve taşınabilir projektörler
WVGA	800 x 480	5:3	Araç navigasyon sistemleri ve taşınabilir PC'ler
SVGA	800 x 600	4:3	Küçük monitörler
XGA	1024 x 768	4:3	Monitör ve taşınabilir projektörler
WXGA	1280 x 800	16:10	Küçük geniş ekran dizüstü bilgisayarlar
HDTV 720p	1280 x 720	16:9	HDTV olarak adlandırılabilen en düşük çözünürlük
SXGA	1280 x 1024	5:4	Masaüstü LCD monitör için doğal çözünürlük
WSXGA	1440 x 900	16:10	Geniş ekran dizüstü bilgisayarlar
SXGA+	1400 x 1050	4:3	Dizüstü bilgisayar ekranı ve ileri teknoloji projektörler
WSXGA+	1680 x 1050	16:10	Büyük dizüstü bilgisayar ve 20" geniş ekran monitörler
UXGA	1600 x 1200	4:3	Büyük CRT monitörler
HDTX 1080p	1920 x 1080	16:9	Tam HDTV çözünürlük
WUXGA	1920 x 1200	16:10	Büyük 24" geniş ekran monitörler
WQUXGA	2560 x 1600	16:10	Büyük 30" geniş ekran monitörler

2.1.4. Tarih ve zaman bilgisi (Date and Time Information)

Tarih ve zaman bilgisi, video sinyalleri ile kaynaştırılarak üretici firmanın belirlemiş olduğu yazı tipleri ile video üzerine yerleştirilir. Güvenlik kamera video ve görüntüleri üzerine yerleştirilen bilgiler, boyut ve karakter olarak üzerinde herhangi bir değiştirme yapılmadan görüntü üzerine gömülür [5].

Tarih ve zaman bilgisi soruşturmacılar için fayda sağlar. Güvenlik kamera sistemlerinden elde edilen görüntüler üzerinde bulunan tarih ve zaman bilgisi ilgili görüntü ile bağlantılı bir şekilde ayrı bir dosya olarak kaydedilir. Ancak çoğunlukla, tarih ve zaman bilgisi akan görüntü ile birlikte tek dosya şeklinde kaydedilir ve bu durumda bu bilgi görüntüden ayırt edilemez [6].

2.1.5. Dijital video kaydedici cihazı (DVR - Digital Video Recorder)

Her güvenlik kamera sisteminin bir elemanı olan dijital kayıt cihazı, bağlı kameralardan gelen görüntüleri içerisinde bulunan depolama alanına kayıt eder. Her DVR cihazı kaydı farklı formatlarda elde eder ve kendisine özel bu formatları oynatabilen oynatıcı yazılımlara sahiptir.

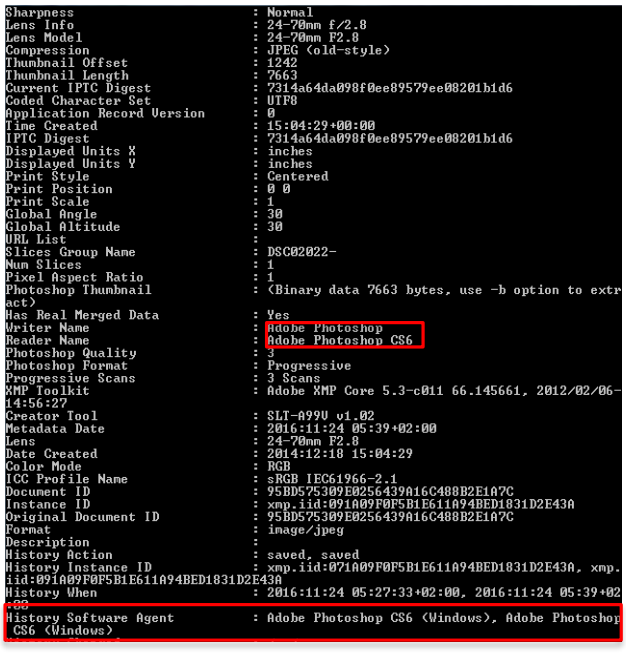
2.1.6. Operatör Tarafından Manuel Yöntemlerle Müdahaleler (Manual Interventions by Operator)

Otomasyon, karmaşık durumlarda operatörün üzerinde bulunan iş yükünü hafifletmek ve sonuç olarak hizmeti artırmak, performansı yükseltmek amacıyla kullanılmaktadır. Ayrıca, otomasyonun güvenilirliği sadece doğruluk ve kesinlikle ilişkili değil, aynı zamanda operatörlerin de sistemdeki güvenilirlikleri ile ilişkilidir [7].

2.1.7. Genişletilmiş dosya bilgisi (EXIF - Extended File Information)

Manipülasyon amaçlı değişikliklerin olduğunu gösterir yardımcı bulgular genelde EXIF bilgilerinin incelenmesi sonucunda da ortaya çıkabilmektedir. Üst veri (metadata) uzmanlar için yararlı bilgiler içerebilir. Özellikle dijital kamera resimleri, resmi çeken kameranın bilgilerini kayıtlı tutan EXIF başlığı içerir [8]. EXIF bilgileri içerisinde videonun oluşturulma tarihi, kaydedilme tarihi, video formatı, kayıt cihazının niteliği gibi bilgiler bulunur. Yazılım araçları kullanılarak bu bilgilerin değiştirilebilmesi mümkündür.

EXIF başlığı bilgilerine ait görüntü Şekil 1'de verilmektedir. Şekilde verilen "EXIF" başlığı bilgilerinden ait olduğu görüntünün Adobe Photoshop yazılımı aracılığı ile manipülasyon işlemlerine maruz kaldığı anlaşılmaktadır.



Şekil 1. Adobe Photoshop yazılımı aracılığı ile manipülasyon işlemlerine maruz kalmış bir görüntünün "EXIF" bilgisinin bir parçası

2.1.8. Görüntü Kayıt Kodek ve Formatları (Image Codec and Formats)

Görüntü Kayıt Kodek ve Formatları ve özellikleri aşağıda verilmiştir.

1) AVI (Audio Video Interleave): Microsoft tarafından üretilmiş bir video formatıdır. Bu format içerisinde birçok kodek bulunur ve bu kodeklerden bazıları sıkıştırma oranı düşük olan ".mpeg" ve ".mov" olarak gösterilebilir.

2) MPEG-4 (*.mp4) (Moving Picture Experts Group): MPEG tarafından üretilmiş olan ve MPEG-4 sıkıştırmasına sahip kodektir ve internet üzerinden paylaşılan videoların sıkıştırmasında kullanılır. MPEG-4 video formatı ses ve görüntü materyallerinin sıkıştırılmasında ayrı ayrı kullanılır. Video materyalleri MPEG-4 ile sıkıştırılırken ses materyalleri ise AAC (Advanced Audio Coding) ile sıkıştırılır.

3) DAT (Digital Audio Tape): İçerisinde birtakım bilgiler içeren genel veri dosyalarında kullanılır. DAT dosyaları tek tip dosyalar değillerdir. Yazılı veri içeren DAT dosyaları, başka bir durumda ise video verisi ihtiva edebilmektedir. Bazı DAT dosyaları görüntü verisi içeren video dosyaları olabilmekte ve bu tür dosyalar yaygın kullanıldığı için birçok oynatıcı yazılımlarla da görüntülenebilmektedirler.

4) FLV (Flash Video): FLV ya da tam adıyla Flash Video, Adobe Flash Player'in ön tanımlı video biçimidir. Sadece Macromedia/Adobe ürünlerince değil, pek çok internet tarayıcı ve çoklu ortam oynatıcısı tarafından da desteklenen FLV, günümüzün en yaygın video formatlarından biridir.

2.2. Güvenlik Kamerası Video ve Görüntüleri Özelliklerinin Manipülasyonu (Manipulation of features of Video and Imaging of Security Cameras)

Güvenlik kamerası video ve görüntülerinde değiştirilebilecek parametreler görüntü sahneleri, içerik, konum ve koordinat bilgisi, tarih ve zaman sayacı, kamera kanal bilgisi, EXIF bilgisi olarak gösterilebilir. Bu parametreler görüntü işleme yazılımları aracılığıyla, değiştirilir ve bu değişikliklerden sonra ise iz bırakılmaması amacıyla yeniden sıkıştırılır. Bu işlemler kayıt cihazlarından görüntüler elde edildikten sonra yapılan işlemlerdir. Tarih ve zaman bilgileri video sinyalleri ile kaynaştırılarak üretici firmanın belirlemiş olduğu yazı tipleri ile video üzerine yerleştirilir. Güvenlik kamerası videoları üzerine yerleştirilen bilgiler, boyut ve karakter olarak üzerinde herhangi bir değiştirme yapılmadan görüntü üzerine gömülür [5]. Üzerinde tarih ve zaman bilgisi bulunan güvenlik kamera kaydına ait orijinal görüntü karesi Şekil 2'de verilmiştir.

Şekil 2. Üzerinde tarih ve zaman bilgisi bulunan güvenlik kamera kaydına ait orijinal görüntü karesi

Yukarıda verilen görüntü karesi Nepal'de meydana gelen depremi görüntüleyen videodan elde edilmiştir. Görüntü karesinde görüldüğü üzere tarih ve zaman bilgisi sağ üst köşede konumlandırılmış ve Çince karakterlerden oluşturulmuştur. Görüntü kareleri üzerinde bulunan bu bilgiler kayıt cihazı tarafından belirlenir. Bu bilgilerin değiştirilmesi, kaldırılması veya pozisyonlarının değiştirilmesi kayıt cihazı üzerinde operatör tarafından yapılır. Kayıt cihazı üzerinden yapılan değişiklikler dijital görüntü düzenleme yazılımları ile yapılan değişiklikler ile ilgisi yoktur. Güvenlik kamera görüntüleri üzerinde bulunan tarih ve zaman bilgileri video düzenleme programları kullanılarak yeniden düzenlenebilir ve görüntüler üzerine yerleştirilebilir. Şekil 3'de görüntü karesi üzerinde bulunan tarih ve zaman sayacının manipüle edilmesi sonucu elde edilen görüntü karesi görülmektedir.

Şekil 3. Görüntü karesi üzerinde bulunan tarih ve zaman sayacının manipüle edilmesi sonucu elde edilen görüntü karesi

Yukarıda sunulan görüntü karesi, orijinal görüntü karesinden tarih ve zaman sayacının silinerek yeni bir sayaç eklendiğini göstermektedir. Bu görüntü karesi üzerinde görsel olarak yapılacak detaylı incelemede herhangi bir iz veya bozukluğun olmadığı görülecektir.

Güvenlik kamera görüntüleri üzerinde bu tür manipülasyonların yapılması belirli adımlarla gerçekleşmektedir.

1) Tarih ve Zaman Sayacının Kaldırılması. Bu işlem için sayacın bulunduğu bölgedeki komşu piksellerden faydalanılır. Komşu piksellerden bloklar halinde seçim yapılarak "kopya" ile kopyalanır ve orijinal tarih ve zaman sayacının üzerine "yapıştır" ile yerleştirilir. Bu işlem için bölgeden çok fazla uzaklaşmamaya dikkat edilmelidir. Çünkü görüntü içerisinde her bir pikselin birbiri ile bir korelasyonu bulunmaktadır. Bu korelasyonun bozulmaması için yakın bölgelerde çalışılması tespiti zorlaştıracaktır.

2) Tarih ve Zaman Sayacının Oluşturulması. Silinen sayacın bulunduğu bölgeye yeni bir sayaç eklenmesi için öncelikle bir sayacın oluşturulması gerekmektedir. Bu sayaç içerisinde önceki sayacın ihtiva ettiği bilgiler mutlaka bulunmalıdır. Örneğin, önceki sayaç saat/dakika/saniye şeklinde oluşturulmuş ise yeni sayaçta da aynı bilgilerin bulunması gerekir. Bu işlem kısa bir kod sayesinde rahatlıkla yapılabilir.

```
beginHr = 23;
beginMin = 59;
beginSec = 59:
beginHun = 0;

beginTime = (beginHr*60 + beginMin)*60 + beginMin + beginHun/100;

function digits(myVal, myNumDigits){
var s = myVal.toString();
while (s.length < myNumDigits) s= '0' + s;
return s;
}

currTime = beginTime + time;

hr = digits(Math.floor(currTime/3600),2);
min = digits(Math.floor((currTime%3600)/60),2);
sec = digits(Math.floor(currTime)%60,2);
hun = digits(Math.floor(currTime%1*100),2);
hr + ":" + min + ":" + sec + ":" + hun
```

Görüntü düzenleme yazılımları içerisinde bu kod kullanılarak yapılacak bir düzenleme ile saat-dakika-

saniye ve tercihe göre salise oluşturulması mümkündür. Yukarıda gösterilen kod sayesinde "23:59:59.00" zamanından başlayan bir sayaç oluşturulabilir. Bu kod sayesinde oluşturulan sayaç bilgisinin yazı karakteri ve rengi önceki sayaca göre düzenlenir ve konumlanırsa bu manipülasyonun tespiti zor olacaktır.

3) Tarih ve Zaman Sayacının Yerleştirilmesi. Yeniden oluşturulan tarih ve zaman sayacının görüntü üzerine yerleştirilmesi sırasında önceki sayacın konum ve pozisyonu detaylı bir şekilde belirlenir. Bu işlem görüntü üzerindeki sayacın koordinatlarının tespit edilmesi şeklinde olmaktadır. İlgili koordinat bilgileri tespit edilmesi sonrasında yeni oluşturulan tarih ve zaman sayacı bu koordinat noktalarına tam yerleşecek şekilde konumlandırılması gereklidir.

Görüntü düzenleme yazılımları kullanılarak manipüle edilmiş görüntülerin çıktısı alınması durumunda ise şüpheliler açısından dezavantajlı bir durum söz konusudur. Çünkü bu tür yazılımlar sınırlı sayıda görüntü formatı üzerinde değişiklik yapmaya ve çıktı almaya müsaade etmektedirler. Dolayısıyla bahsedilen bu tür işlemlerin yapılabileceği görüntü formatları yaygın şekilde kullanılan ve sınırlı formatlardır. Güvenlik kamera kayıtlarını yapan cihazlar ise farklı şirketler tarafından üretildiği için kendilerine özgü formatlar kullanırlar. Sonuç olarak güvenlik kamera görüntüleri üzerinde bulunan tarih ve zaman sayacının değiştirilmesi bu işlemi yapan şüphelinin yeteneği ile orantılıdır. Şüphelinin bu işlemi detaylı ve titiz bir şekilde gerçekleştirmesi ve sonrasında bırakacağı izleri göz önüne alarak çalışma yapması gerekir.

3. GÜVENLİK KAMERASI VİDEO VE GÖRÜNTÜLERİNDE TARİH VE ZAMAN SAYAÇLARI ÜZERİNDE YAPILAN MANİPÜLASYONLARI TESPİT ETME TEKNİKLERİ (TECHNIQUES FOR DETECTING THE MANIPULATIONS MADE ON DATE AND TIME COUNTERS OF VIDEO AND IMAGING OF SECURITY CAMERAS)

Güvenlik kamera görüntüleri üzerindeki tarih ve zaman sayacında yapılabilecek manipülasyonların tespiti tamamıyla mümkün olamamaktadır. Birçok parametrenin bulunduğu bu tür incelemeler şüphelilerin yetenekleriyle ilgilidir. Şüphelinin yapmış olduğu manipülasyon sonucu bırakmış olduğu hatalar incelemeyi bir sonuca götürebilir. Günümüzde ise bu tür incelemeler sonucu verilecek olumlu veya olumsuz kanaatlerin sağlıklı olmayacağı değerlendirilmektedir.

Görüntüler üzerinde yapılan manipülasyonların analizi, yapılan manipülasyonun çeşidine göre değişiklik gösterir. Piksel tabanlı çalışan algoritmalarla yapılan manipülasyon analizleri örnek olarak gösterilebilir. Piksel piksel yapılan manipülasyonların tespiti için birçok araştırmacı tarafından geliştirilen çok fazla sayıda yaklaşım vardır. Bu yaklaşımların uygulama adımları ortak olarak, dijital görüntünün yazılım ile açılması, birbiri ile örtüşen bloklara ayrılması, öznitelik çıkartılması, özniteliklerin sıralanması, manipüle edilmiş bölgenin belirlenmesi ve analizin sonuçlanması şeklinde gösterilebilir. Kayıt formatları, yazı karakterleri ve saniye başına düşen görüntü karesi sayısı gibi özellikler incelenerek te manipülasyon tespit edilebilir.

3.1. Öznitelik Çıkarma Teknikleri (Features Extracting Techniques)

3.1.1. PCA (Principal Component Analysis)

Çok değişkenli istatistik tekniklerinden biri olan PCA, değişkenler arasındaki bağımlılık yapısının yok edilmesi ve(ya) boyut indirgeme amacını taşımaktadır. Başlı başına bir analiz tekniği olduğu gibi, başka analizler için bir veri hazırlama tekniği olarak da kullanılmaktadır [10].

3.1.2. DCT (Discrete Cosine Transform)

DCT zamanla ilgili sayısal karmaşıklığı azaltır. Başlangıçta, orijinal resim satır ve sütunlar olmak üzere matrislere bölünür. Sonrasında, DCT satır ve sütun indirgeme tekniklerinin yardımıyla bütün satır ve sütunlara uygulanır, çeşitli boyutlarda çeşitli sayıda bloklara dönüştürülür. Son olarak, kopyalanmış resim, eşik değerine göre ayıklanmış olacaktır. Bu işlem sonrasında resim üzerinde manipülasyon sonrasında tespit edilen eksiklikler simüle edilir [11].

3.1.3. DWT (Discrete Wavelet Transform)

DWT resim piksellerini dalgalara dönüştüren tekniktir. Bu dönüşüm sıkıştırma ve kodlamada kullanılır [12].

3.1.4. SVD (Singular Value Decomposition)

SVD, dönüşümler ile ilgili olarak önemli geometrik ve teorik yaklaşımlar içermektedir [13]. SVD simetrik matrislerin köşegenleştirilmesi teorisi ile çok yakından ilişkilidir. SVD en önemli ve en yaygın matris işlemlerinden birisidir. Karmaşık olan dört alt uzaya sahip matrisin doğal yolla kolay anlaşılmasını sağlar ve bu alt uzayların önemli ilişkilerini ortaya çıkarır. Bu sebeple verilerin analizinde önemli rol oynayan araçtır ve matris teorisinde birçok temel sonucun kolayca anlaşılmasını sağlar.

3.1.5. SIFT (Scale Invariant Feature Transform)

SIFT genellikle resim üzerinde bölgesel olarak özniteliklerin ortaya çıkarılması için kullanılır. SIFT metodunun birçok avantajı vardır:
- SIFT rotasyon, büyütme/küçültme ve ışık etkenlerinden bağımsız olarak öznitelikler üzerinde çalışır;
- SIFT metodu ile elde edilen öznitelikler perspektif değişikliklerinde ve gürültü eklenmesi durumlarında da büyük oranda korunur;
- Ayrıca SIFT tarafından elde edilen öznitelikler eşsiz ve aydınlatıcı bilgiler içerirler [14].

3.1.6. SURF (Speed Up Robust Features)

Birçok görüntü işleme yaklaşımları, bölgesel parçaların ve özniteliklerin farklı resimlerden çıkartılarak karşılaştırılmasıdır. Ancak hızlı çalışan bir algoritmanın tasarımı için bazı ölçütler gerekmektedir. Resim üzerinde yapılan bölgesel çalışmaların seyrek olması, hesaplamaları güç olan karşılaştırmalı işlemlerden de kaçınılmasını sağlar. En büyük zorluklar resmin dikkat çekici özniteliklerinin korunması ve bundan sonra bu özniteliklerin karışıklıklardan, gürültü ölçümlerinden, fotometrik değişimlerden bağımsız olarak bölgesel tanımlamalarının yapılmasıdır [15].

3.2. DVR Kayıt Formatlarını İnceleme Teknikleri (Techniques for Examining the DVR Recording Formats)

Öncelikle bir görüntü üzerinde manipülasyon yapılabilmesi için formatının video düzenleme programlarına uygun olması gereklidir. Farklı bir formatı olan görüntüler üzerinde manipülasyon yapılabilmesi için format dönüştürme yapılması ve daha sonrasında yeniden orijinal formatı ile kaydedilmesi gereklidir. Bu amaçla her türlü incelemelerde görüntülerin kaydı alan kaynağın orijinal formatında istenmesi en önemli faktörlerden birisidir. Her türlü formattaki görüntüler üzerinde manipülasyon yapılması mümkün değildir. Günden güne firmalar tarafından üretilen kayıt cihazlarının render (çıkarım) ettiği görüntülerin formatları da kendilerine özgü algoritmalar sayesinde birbirinden farklı olmaktadır. Dolayısıyla her türlü format için dönüştürme yazılımları da bulunmamaktadır. Bilinen ve üzerinde manipülasyon yapılması mümkün olan DVR kayıt formatları Bölüm 2.1.8'de sıralanmıştır.

Güvenlik kamera görüntüleri üzerinde format yönünden yapılacak olan incelemelerde görüntünün sonradan değiştirilip değiştirilmediği, kodek üzerinde oynamalar yapılıp yapılmadığına dair bilgilere ulaşılabilir. Ayrıca kaynak kayıt cihazı üzerinden elde edilecek olan başka bir kayıt sayesinde de cihazın kayıt bilgileri elde edilerek mevcut kaydın orijinal olup olmadığı konusunda fikir sahibi olunabilir.

3.3. Yazı Karakterlerini İnceleme Teknikleri (Text Characters Examining Techniques)

Güvenlik kamera görüntüleri üzerinde bulunan tarih ve zaman sayaçlarının yazı karakteri üretici firma tarafından belirlenir. Uzman inceleme esnasında aynı DVR cihazından elde edilecek başka bir kayıt üzerindeki tarih ve zaman sayacı ile doğrulamak amaçlı karşılaştırmalı bir inceleme yapmalıdır. Çünkü bu sayacın değiştirilmesi aşamasında, şüpheli kaydın üzerinde bulunan sayaç tipinin birebir özelliklerine sahip yazı tipi kullanması gerekecektir.

3.4. Saniye Başına Düşen Görüntü Karesi Sayısını İnceleme Teknikleri (FPS Examining Techniques)

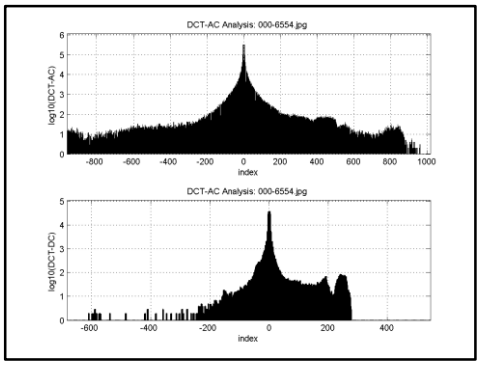
Güvenlik kamera görüntüleri üzerinde yapılacak olan sayaç değişikliklerinde şüpheli tarafından göz ardı edilebilecek diğer durumlardan biri ise yeni atanacak olan sayaç ile eldeki görüntünün saniye başına düşen görüntü karesi sayısı arasında orantılı bir şekilde ilişkinin kurulması gerektiğidir. Yapılacak incelemelerde, cihazdan elde edilecek bir başka kayıt ile bu yönden bir karşılaştırmalı analizler yapılması da şüphelinin bırakmış olduğu hatayı ortaya çıkarabilir.

4. GÖRÜNTÜLER ÜZERİNDE YAPILAN GENEL MANİPÜLASYONLARIN ANALİZİ (ANALYSIS OF GENERAL MANIPULATIONS ON IMAGES)

Görüntüler üzerinde yapılan manipülasyonların tespiti görsel ve yazılımsal incelemeler sayesinde yapılır. Bu adımda görsel incelemelerin yapıldığı varsayılarak yazılımsal incelemelerden bahsedilecektir. Yazılımsal incelemelerin amacı, görüntünün ihtiva etmiş olduğu sayısal değerlerin bilgisayar ortamında analizi yapılarak doğal durumu bozan değerlerin ortaya çıkarılmasını sağlamaktır. Dolayısıyla bu aşamada görüntünün sayısallaştırılması sırasında kullanılan tekniklerin adım adım analizi yapılarak analog ortamdan dijital ortama geçiş esnasında bulunmayan ancak sonradan müdahale edilerek manipüle edilen bölgeler tespit edilir.

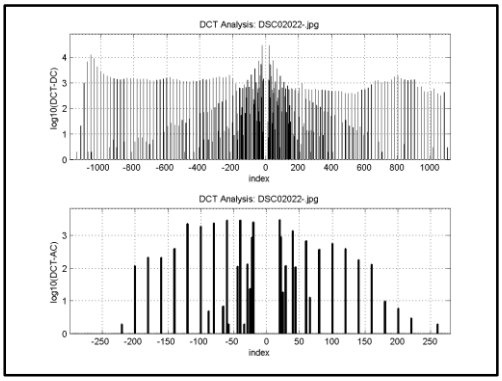
4.1. DCT Analizi (DCT Analysis)

Manipüle edilmiş görüntüler üzerinde yapılacak analizlerden birisi DCT grafiklerinin incelenmesidir. DCT, görüntü sinyalinin temel frekans içeriklerine dönüştürülmesi tekniğidir [16]. Görüntü sıkıştırma alanında yaygın olarak kullanılan bir tekniktir [17]. Dolayısıyla manipülasyon tespit analizlerinde de sıkıştırılan bu sinyallerin durumuna bakılır. Elde edilen DCT grafikleri görüntü üzerinde yapılmış olan sıkıştırmanın miktarı hakkında bilgi verir (Şekil 4).



Şekil 4 (a) Orijinal resme ait DCT grafiği

Elde edilen DCT grafikleri incelendiğinde, orijinal görüntüye ait grafikteki dalgalanmaların belirli bir düzen içerdiği görülür iken (Şekil 4 (a)) manipüle edilmiş görüntüye ait grafiğin ise düzensiz dalgalanmalar içerdiği görülmektedir (Şekil 4 (b)).

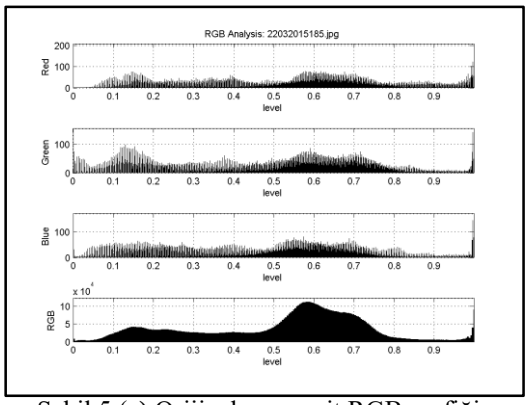


Şekil 4 (b) Manipüle edilmiş ve sonrasında sıkıştırmaya uğramış resme ait DCT grafiği

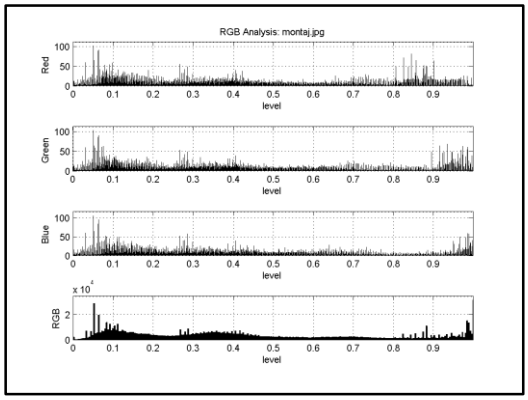
Bunun sebebi manipülasyon işlemi sonrasında görüntüye uygulanan sıkıştırma işleminin sinyalleri bozması sebebiyle bu durumun grafiğe yansımasıdır. Manipüle edilmiş resme ait grafiğe bakıldığında orijinal resmin en az 3 defa sıkıştırmaya uğradığı söylenebilir. Görüntü üzerinde yapılacak her sıkıştırma işlemi grafikte yeni bir dalgalanma oluşmasına sebep olacaktır.

4.2. RGB Katmanları Analizi (RGB Analysis)

Bir görüntü içerisinde üç katmanlı olarak bulunan ve insan retinasında bulunan RGB renk modeli, bilgisayar ortamında kullanılan [18], rengin sayısallaştırılması aşamasındaki en önemli analiz faktörlerinden birisidir (Şekil 5).



Şekil 5 (a) Orijinal resme ait RGB grafiği

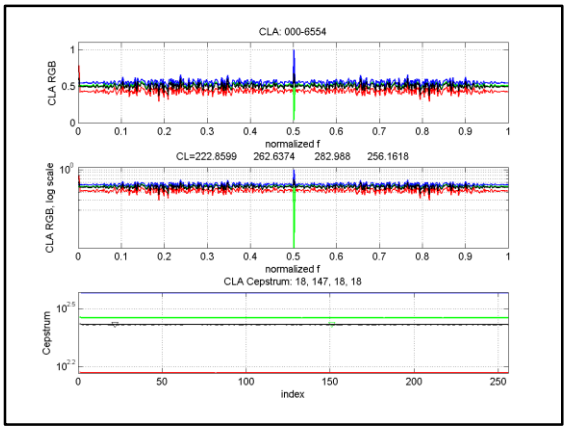


Şekil 5 (b) Manipüle edilmiş ve sonrasında sıkıştırmaya uğramış resme ait RGB grafiği

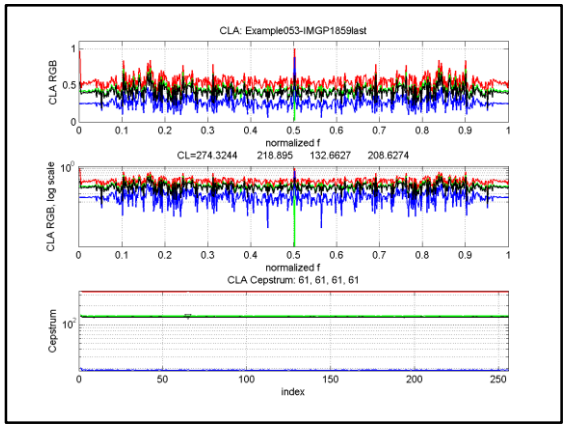
Elde edilen RGB katman analiz grafikleri incelendiğinde, orijinal görüntü üzerine uygulanan manipüle işlemleri ve sıkıştırma eylemleri renk katmanlarının bozulduğunu ve görüntüye ait renk zenginliğinin azaldığını görmek mümkündür (Şekil 5 (b)). Orijinal görüntülere ait RGB katman analiz grafiklerinde birbirinden bağımsız dağılım gösteren yapıların görülmesi pek mümkün değildir (Şekil 5 (a)). Dolayısıyla bu grafik üzerinde inceleme yapan görüntü uzmanları bu görüntünün bir bozma işlemine uğradığı kanaatine varacaktır.

4.3. CLA Analizi (CLA Analysis)

Bir görüntünün orijinalliği ile ilgili kullanılan analiz yönteminden diğeri CLA tekniğidir. Bir görüntü eğer orijinal veya kaynağından direkt olarak elde edilmiş ise, CLA analizi sonucunda kayıt cihazına bağlı olarak herhangi bir sıkıştırmaya rastlanılmaz. Görüntü bir yazılıma yüklendiğinde veya internet ortamına eklendiğinde, internet ortamından indirildiğinde yeniden bir sıkıştırmaya uğrar [19]. CLA analizleri sonucunda görüntünün sıkıştırma oranları hakkında bilgi sahibi olunur ve sonuca götürecek olan adımlar hakkında fikir edinilir (Şekil 6).



Şekil 6 (a) Orijinal resme ait CLA grafiği



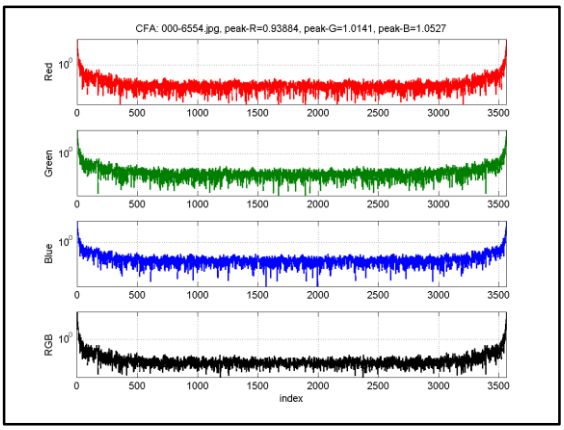
Şekil 6 (b) Manipüle edilmiş ve sonrasında sıkıştırmaya uğramış resme ait CLA grafiği

Orijinal görüntülere ait CLA grafiklerinde renk katmanları üzerindeki sıkıştırma seviyeleri düşük ve her bir katmanın sıkıştırma seviyesi birbiri ile ilişki içerisinde

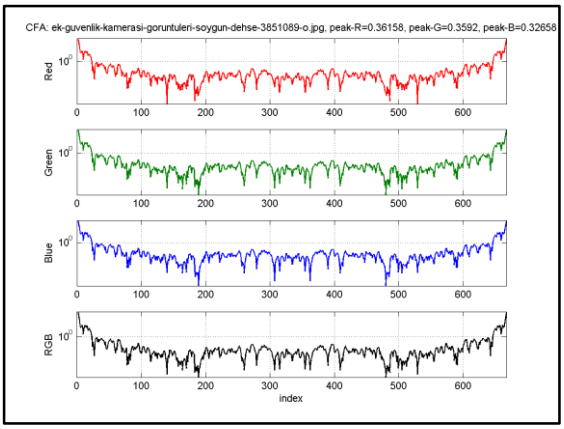
olmaktadır (Şekil 6 (a)). Ancak, görüntü üzerinde yapılacak manipülasyon işlemleri sonucunda elde edilecek grafiklerde renk katmanları üzerindeki sıkıştırma ve bozulma seviyesi artacak ve bu katmanların birbirleri ile olan ilişki düzensiz bir hale gelecektir. Nitekim Şekil 6 (b)'de görülen manipüle edilmiş görüntüye ait CLA grafiğinde bu durum açıkça görülmektedir.

4.4. CFA Analizi (CFA Analysis)

Bloklaşma gideren algoritmalar ile CFA kullanılmasının sonucu olarak pikseller ile dijital kamera görüntüleri arasında CFA enterpolasyonu ilişkisi olduğu bilinmektedir [20]. Bu sebeple görüntüler üzerinde CFA analizi yapılarak bloklaşmaların olduğu bölgelerde değer sapmaları ortaya çıkartılır ve manipülasyon tahmin edilmeye çalışılır (Şekil 7).



Şekil 7 (a) Orijinal resme ait CFA grafiği



Şekil 7 (b) Manipüle edilmiş ve sonrasında sıkıştırmaya uğramış resme ait CFA grafiği

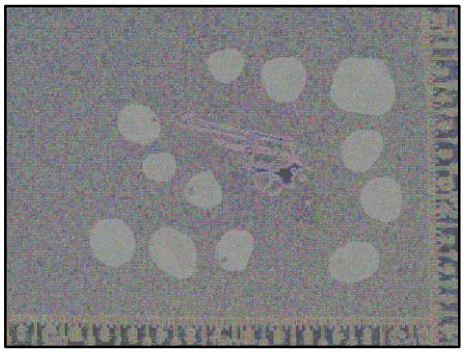
Görüntünün oluşturulması ve analog sinyalin dijitale döndürülmesi aşamasından önce ışığın renk filtresinden geçme aşaması bulunur. Bu aşamada ışık renk katmanlarına ayrılır. Orijinal görüntülere ait CFA grafiklerine bakıldığında çeşitliliği yüksek ve birbirleri ile ilişki içerisinde olan sinyal bilgisi görülecektir (Şekil 7 (a)). Ancak sonradan bu görüntüler üzerinde yapılacak olan manipülasyon işlemleri sonucunda uygulanmış olan bozma işlemleri sinyallerin çeşitliliğiniz azaltacak ve birbirleri ile olan ilişkilerin yok olmasına sebep olacaktır (Şekil 7 (b)). Bu sebeple manipüle edilmiş görüntülere ait CFA grafiklerinde düzensiz ve seyrek dalgalanmaların bulunduğu görülür.

4.5. ELA Analizi (ELA Analysis)

ELA tekniği, farklı sıkıştırma seviyeleri ile görüntünün parçalarının tanımlanması amacıyla kullanılır. Eğer bir görüntü dijital ortamda değiştirilmiş ise ELA tekniği kullanılarak bu durum ortaya çıkarılabilir. ELA tekniği, değerlerin yüksek olduğu, manipüle edilmiş bölgeleri ve parlak beyaz bölgeleri daha aydınlık olarak gösterir [21]. ELA ile aydınlık bölgelere yoğunlaşılır ve manipüle edilmiş bölgeler tespit edilmeye çalışılır (Şekil 8).

Şekil 8 (a) Orijinal görüntü

Şekil 8 (b) Adobe Photoshop "Content Aware" fonksiyonu kullanılarak manipülasyon işlemlerine maruz kalmış görüntü



Şekil 8 (c) Adobe Photoshop "Content Aware" fonksiyonu kullanılarak yapılan manipülasyonun ELA analizi sonucu

Görüntüler üzerinde yapılan manipülasyon tespit incelemelerinde ELA analizleri en güçlü analizlerden birisidir. Elde edilebilecek başarılı ELA analizi sonuçları

bazı durumlarda tek başına dahi manipülasyonu ortaya koyacak delillerden birisi olabilir. Yukarıda sunulan ELA analizi sonucuna bakıldığında ortaya koymuş olduğu analiz sonucu tek başına manipülasyonu ortaya koyabilmektedir. Manipülasyonun nerede ve ne şekilde yapıldığı konusuna rahatlıkla cevap veren ELA analizi, mahkemede hakimi ikna edebilecek düzeyde sonuçları ortaya koymuştur.

5. GÜVENLİK KAMERASI VİDEO VE GÖRÜNTÜLERİNDE TARİH VE ZAMAN SAYAÇLARI ÜZERİNDE PROFESYONELCE YAPILAN MANİPÜLASYONLARIN ANALİZİNE AİT UYGULAMALAR

(APPLICATIONS OF ANALYSIS OF MANIPULATIONS MADE PROFESSIONALLY ON DATE AND TIME COUNTERS OF VIDEO AND IMAGES IN SECURITY CAMERAS)

Görüntüler üzerinde yapılan analizlerde sayısal görüntü işleme teknikleri kullanılır. Aslında bu teknikler görüntüler üzerinde yapılan kopyala yapıştır şeklindeki klonlamaların tespitinde daha başarılıdırlar. Çünkü tarih ve zaman sayaçları kaydı alanın kameranın gördüğü sahnede bulunmayan kayıt cihazının sonradan yerleştirdiği bilgiler olduğu için bu tür analizlerde manipülasyon tespiti yapılması pekte mümkün olmayacaktır. Bu bölümde analizler, görüntünün üzerinde yalnızca tarih ve zaman sayacına yönelik manipüle işlemleri yapıldığı varsayımından yola çıkılarak gerçekleştirilmiştir. Aşağıda sunulan görüntü kareleri tarih ve zaman sayacı üzerinde yapılan manipülasyonun öncesini (Şekil 9 (a)) ve sonrasını (Şekil 9 (b)) göstermektedir.

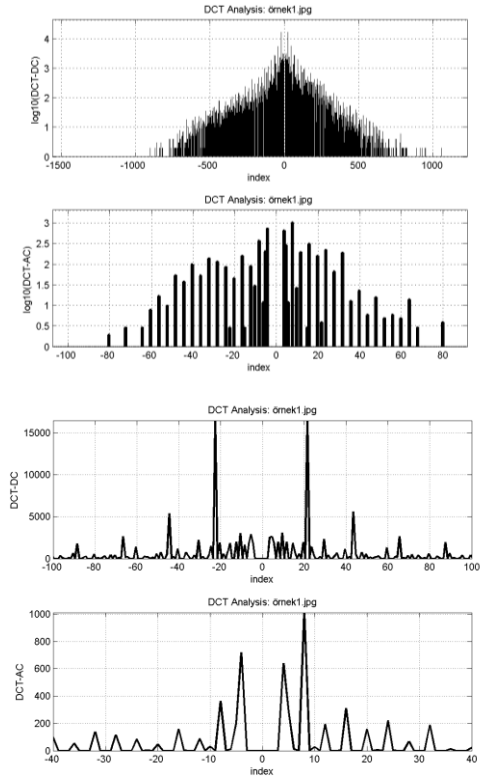
Şekil 9 (a) Orijinal kayıttan elde edilen görüntü karesi

Şekil 9 (b) Manipüle edilmiş kayıttan elde edilen görüntü karesi

Görüldüğü üzere Şekil 9 (a)'daki görüntü karesinin elde edildiği kaydın tarih ve zaman sayacı üzerinde bu makalede anlatılan manipülasyon teknikleri kullanılarak manipülasyon işlemi gerçekleştirilmiş ve bu işlem sonrasında görüntünün yeniden çıktısı alınmış ve Şekil 9 (b) elde edilmiştir. Sonraki bölümlerde gösterilecek olan analiz sonuçlarının kıyaslanması amacıyla hem orijinal görüntü hem de manipüle edilmiş görüntüye ait analiz sonuçları sunulacaktır. Bu sayede tarih ve zaman sayacı üzerinde yapılan manipülasyonun analizi ile genel manipülasyon analizleri sonuçları da karşılaştırılarak tarih ve zaman sayacına ait manipülasyonların günümüz imkanları ile sağlıklı bir şekilde tespit edilemeyeceğinin de anlaşılması sağlanacaktır.

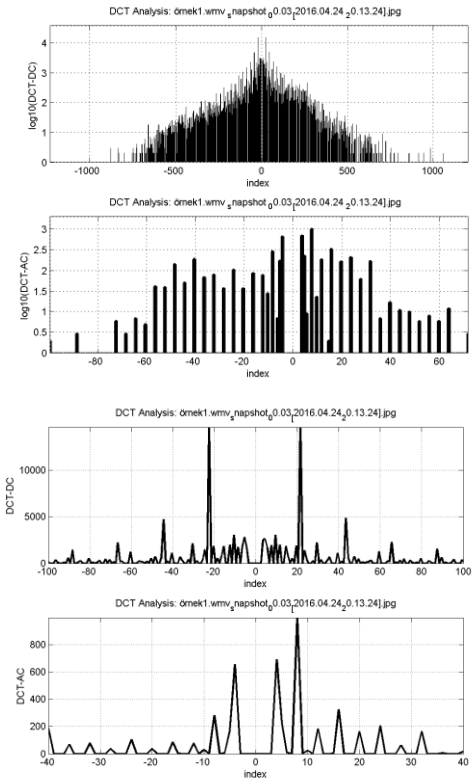
5.1. DCT Analizi (DCT Analysis)

Şekil 9 (a)'da verilen orijinal kayıttan elde edilen görüntü karesine uygulanan DCT analiz sonuçları Şekil 10 (a)'da verilmektedir.



Şekil 10 (a) Orijinal görüntü karesine ait DCT Dönüşüm Grafiği

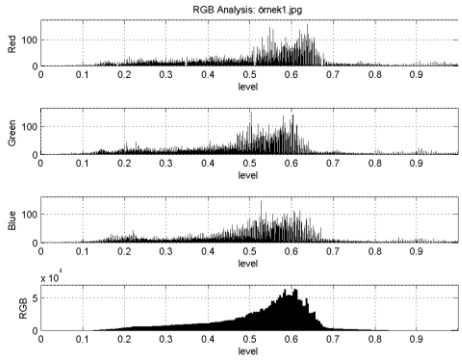
DCT, özellikle JPEG resimlerde kullanılan kayıplı sıkıştırma algoritmasıdır. DCT analizleri üzerinden sağlıklı bir karar verilmesi için grafikler üzerinde sıkıştırma oranına bağlı olarak yüksek miktarda homojen olmayan dalgalanmaların görülmesi gerekir. Bu sayede sıkıştırma oranı hakkında fikir edinilir. Ancak Şekil 9 (b)'de verilen manipüle edilmiş kayıttan elde edilen görüntü karesine uygulanan DCT analiz sonuçlarına (Şekil 10 (b)) bakılırsa, sağlıklı bir karar vermenin mümkün olamayacağı açıkça görülebilir.



Şekil 10 (b) Manipüle edilmiş görüntü karesine ait DCT Dönüşüm Grafiği

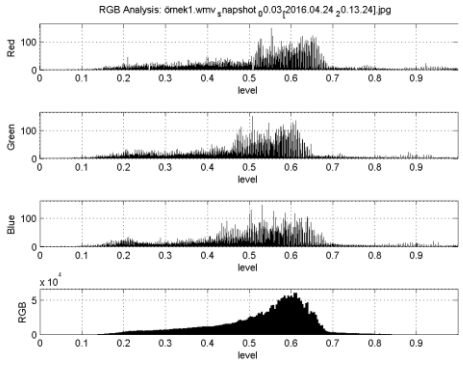
5.2. RGB Analizi *(RGB Analysis)*

Manipülasyonun gerçekleştirilmesi aşamasında en çok işlemin yapıldığı aşamalardan birisi RGB katmanlarının yeniden düzenlenmesi aşamasıdır. Çünkü yapılan işlemlerin kamufle edilmesi bu aşamada gerçekleştirilir. Renkler üzerinde yapılan ince çalışmalar sonucunda manipüle izleri rahatlıkla silinebilir. Şekil 9 (a)'da verilen orijinal kayıttan elde edilen görüntü karesine uygulanan RGB analiz sonuçları Şekil 11 (a)'da verilmektedir.



Şekil 11 (a) Orijinal görüntü karesine ait RGB Analizi

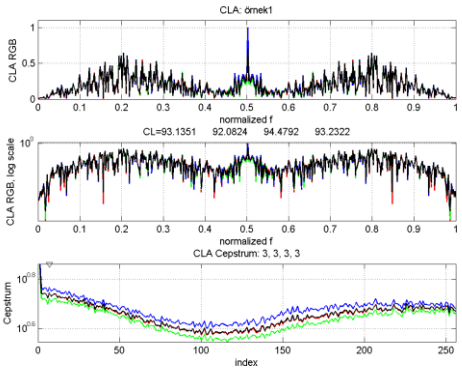
Manipülasyon tespit analizlerinde, bu renk katmanların analizleri çok önemlidir. Manipülasyon işlemlerinde yeni oluşturulan manipülasyon parçası görüntüye yerleştirilir iken renkler üzerinde bazı ayarlamalar yapılır ve bu ayarlamalar tespit analizlerinde kendilerini gösterirler. Ancak Şekil 9 (b)'de verilen manipüle edilmiş kayıttan elde edilen görüntü karesine uygulanan RGB analiz sonuçları tarih ve zaman sayacı bölgesinde yapılan manipülasyonların renk analiz grafiklerini gözle görülür şekilde etkilemedikleri görülmektedir (Şekil 11 (b)).



Şekil 11 (b) Manipüle edilmiş görüntü karesine ait RGB Analizi

5.3. CLA Analizi *(CLA Analysis)*

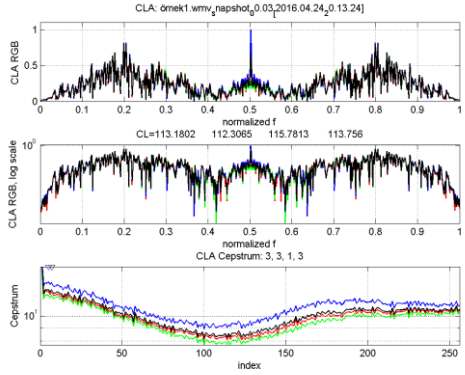
Dijital cihazların artışı ile birlikte mahkemede delil olarak kullanılabilecek görüntülerin de bu cihazlar tarafından kayıt edilebileceği rahatlıkla söylenebilir. Deliller içerisinde bu tür kayıtlarında kabul edilebilmesi için bazı durumlarda kaydın orijinalliğinin incelenmesi gerekir. Bu incelemelerde kullanılan tekniklerden birisi de CLA analizidir [19]. Bir görüntü üzerinde yapılan manipülasyonun tespitini zorlaştırmak için başvurulan ilk teknik çıkarım (render) sırasında yapılacak olan sıkıştırma işlemleridir. Görüntü ne kadar yüksek düzeyde sıkıştırılırsa tespit analizlerinin başarısı da o kadar düşük olur. CLA analizlerinde bu sıkıştırmaların oranına bakılır ve manipülasyonun aşamaları hakkında fikir edinilmeye çalışılır. Şekil 9 (a)'da verilen orijinal kayıttan elde edilen görüntü karesine uygulanan CLA analiz sonuçları Şekil 12 (a)'da verilmektedir.



Şekil 12 (a). Orijinal görüntü karesine ait CLA Analizi

Şekil 9 (b)'de verilen manipüle edilmiş kayıttan elde edilen görüntü karesine uygulanan CLA analiz sonuçları Şekil 12 (b)'de verilmektedir. Görüldüğü gibi, elimizdeki görüntü üzerinde yapılan CLA analizinde orijinal ve manipüle edilmiş görüntüye ait grafikler arasında küçük oranlarda değişiklik olmuş ise de, manipüle edildiğini

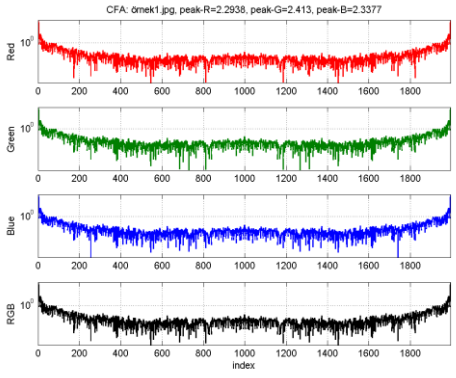
gösterir herhangi bir şekilde güçlü kanıt elde edilmediği açıkça görülmektedir.



Şekil 12 (b) Manipüle edilmiş görüntü karesine ait CLA Analizi

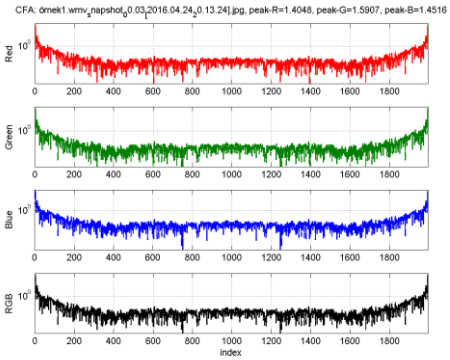
5.4. *CFA Analizi (CFA Analysis)*

CMOS ve CCD sensörlerindeki pikseller yalnızca ışık değerleri ile belirtilir ve spektrum dalga boylarında ayırt edilmezler. Ancak Foveon X3 sensörü, her pikselin konumunda aynı zamanda renk bilgisini de kaydeder. Bu sınırlamadan dolayı sensörlerin üzerine renk filtresi yerleştirilerek ışık renklere ayrılır. Bu sebeple her piksel renklerin değerini veren dalga boyları için gerekli olan ışık yoğunluğunun değerini ihtiva eder. Bu filtreleme işlemi CFA olarak adlandırılır [22]. CFA analizleri renk katmanları ile ilgili bilgiler verir. Kırmızı, yeşil ve mavi katmanlar üzerinde meydana gelen değişimler bu analizler sonucunda ortaya çıkar. Manipüle işlemleri sonucunda her defasında renk katmanları üzerinde meydana gelen değişimler bu analizin grafiğine yansımaktadır. Şekil 9 (a)'da verilen orijinal kayıttan elde edilen görüntü karesine uygulanan CFA analiz sonuçları Şekil 13 (a)'da verilmektedir.



Şekil 13 (a) Orijinal görüntü karesine ait CFA Analizi

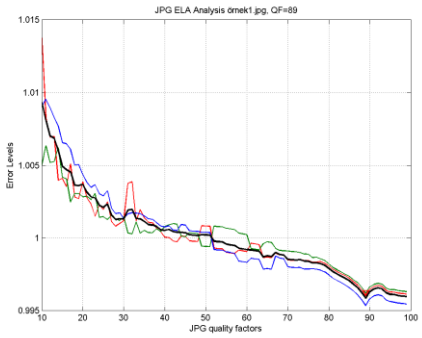
CFA analizlerinde sonradan renk ile ilgili olarak yapılan manipülasyonlarda grafiklerde belirgin bir değişimin olması beklenir. Şekil 9 (b)'de verilen manipüle edilmiş kayıttan elde edilen görüntü karesine uygulanan CFA analiz sonuçları Şekil 13 (b)'de verilmektedir. Görüldüğü gibi, elimizdeki manipüle edilmiş ve orijinal görüntülere ait CFA analizlerinde, grafikler arasında gözle görülür bir farkın bulunmadığı ve eğer orijinal görüntünün elde olmadığı düşünülürse bu analizlerden manipülasyon olduğunu gösterir sonuca ulaşılamadan geçeceği görülebilmektedir.



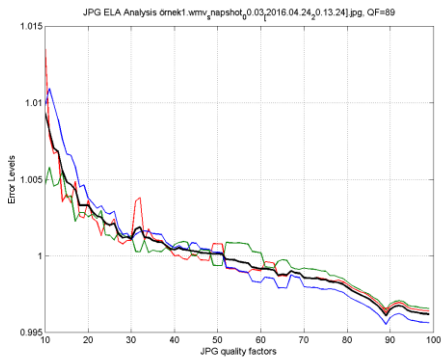
Şekil 13 (b) Manipüle edilmiş görüntü karesine ait CFA Analizi

5.5. *ELA Analizi (ELA Analysis)*

ELA analizi manipülasyon tespiti için diğer yöntemlerden birisidir. ELA farklı sıkıştırma seviyelerini resmin tamamı içerisinde gösterir [23]. ELA analizlerinin sonuçları hem grafik hem de görsel olarak sunulur. Görsel olarak sunulan analizlerde her farklı hata seviyesi için farklı bir görsel sonuç sunulur. Yapılan işlemin tespiti bu seviyeler içerisinden herhangi birisinde gözlemlenebilir. Manipülasyonun bulunduğu bölgeler bu görsel sonuçlarda görüntünün geneline göre daha farklı bir şekilde boyanırlar. Şekil 9 (a) ve (b)'de verilen orijinal ve manipüle edilmiş kayıtlardan elde edilen görüntü karelerine uygulanan CLA analiz sonuçlarına ait grafikler Şekil 14 (a) ve (b)'de verilmektedir.



Şekil 14 (a) Orijinal görüntü karesine ait ELA Analizi



Şekil 14 (b) Manipüle edilmiş görüntüye ait ELA Analizi

Şekil 9 (a) ve (b)'de verilen orijinal ve manipüle edilmiş kayıtlardan elde edilen görüntü karelerine uygulanan CLA analiz sonuçlarına ait görüntüler Şekil 15 (a) ve (b)'de verilmektedir.

Şekil 15 (a) Orijinal görüntü karesine ait ELA Analizi

Şekil 15 (b) Manipüle edilmiş görüntü karesine ait ELA Analizi

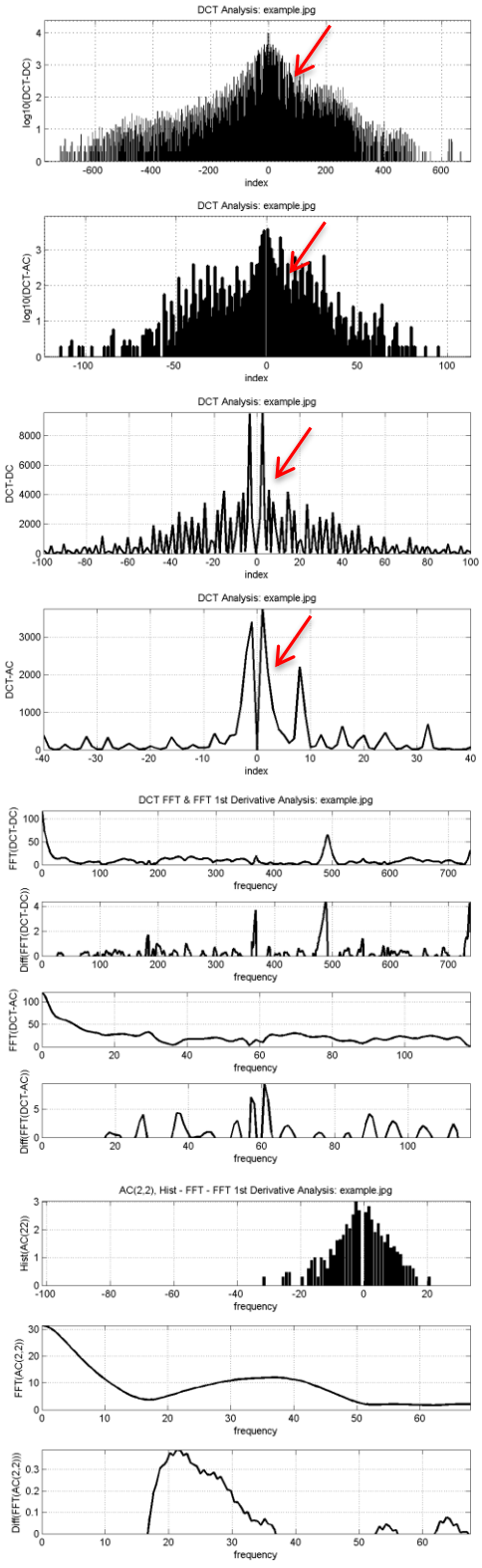
Yapılan ELA analiz sonuçlarında her iki görüntü arasında tarih ve zaman sayacının bulunduğu bölgede manipülasyon yapıldığını gösterir bir bulguya rastlanılmamıştır. Bu analizde görülebilecek en ufak detay, orijinal görüntünün tarih ve zaman sayacının bulunduğu bölgenin aydınlık olarak işaretlenmesidir. Bunun sebebi ise kayıt cihazı tarafından sonradan atanan tarih ve zaman sayacının beyaz renkli olmasıdır. Fakat manipüle edilmiş görüntüde aynı bölgenin aydınlık gösterilememesinin sebebi bölgede manipülasyon sonrasında yapılan yumuşatma işlemleri olabilir. Ancak elde orijinal görüntünün olmadığı durumlarda buradan yola çıkılarak bu bulgunun direkt olarak manipülasyon emaresi olduğuna karar vermek sağlıklı bir karar olmayacaktır.

6. GÜVENLİK KAMERASI VİDEO VE GÖRÜNTÜLERİNDE TARİH VE ZAMAN SAYAÇLARI ÜZERİNDE AMATÖRCE YAPILAN MANİPÜLASYONLARIN ANALİZİNE AİT UYGULAMALAR *(APPLICATIONS OF ANALYSIS OF MANIPULATIONS MADE AMATEURISH ON DATE AND TIME COUNTERS OF VIDEO AND IMAGES IN SECURITY CAMERAS)*

Yukarıda sunulan sonuçlar profesyonelce yapılmış olan tarih zaman manipülasyonunun sonuçlarını göstermektedir. Şüphelinin manipüle işleminden sonra kalan izleri temizlemesi tespiti de zorlaştıracaktır. Ancak amatör şekilde yapılan manipülasyon işlemlerinin tespit çalışmalarında ise rahatlıkla bırakılan izler görülebilir ve analiz sonuçları uzmana manipülasyon yapıldığını işaret edebilir. Aşağıda sunulan analiz sonuçları ise profesyonel olmayan manipüle işlemleri sonrasında yapılan analiz sonuçlarını göstermektedir.

6.1. DCT Analizi (DCT Analysis)

Analiz sonuçları orijinal görüntüye ait analiz sonuçları referans alınarak incelendiğinde, görüntünün en az bir defa sıkıştırmaya uğradığını göstermektedir (Şekil 16).

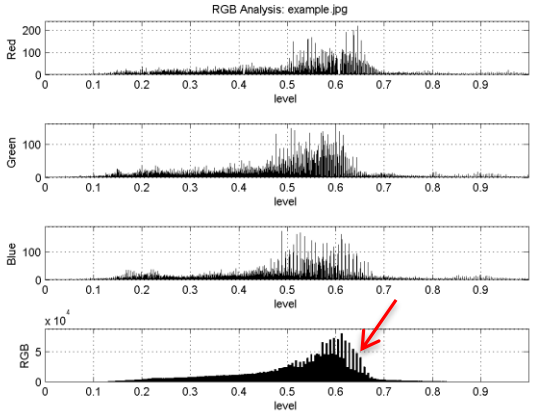


Şekil 16. Manipülasyon bulgusu görülebilen manipüle edilmiş görüntü karesine ait DCT Analizi

Bu analiz sonuçları değerlendirildiğinde, görüntü üzerinde manipülasyon varlığının bulunduğu yönünde kanaat verilebilecektir.

6.2. RGB Analizi *(RGB Analysis)*

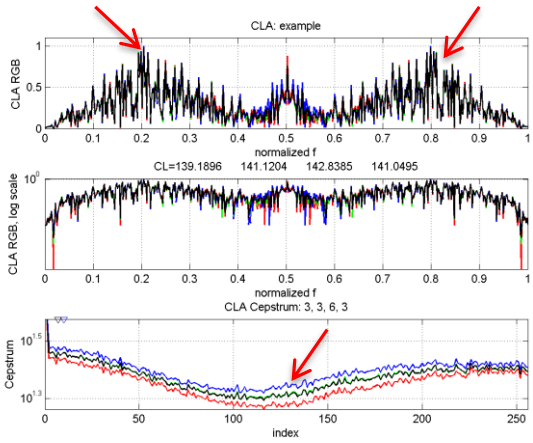
RGB kanalları üzerinde yapılan analizde orijinal görüntü karesine ait analiz sonuçları referans alındığında grafikteki homojen ve düzenli dağılımın bozulduğu rahatlıkla görülebilir (Şekil 17).



Şekil 17. Manipülasyon bulgusu görülebilen manipüle edilmiş görüntü karesine ait RGB Analizi

6.3. CLA Analizi *(CLA Analysis)*

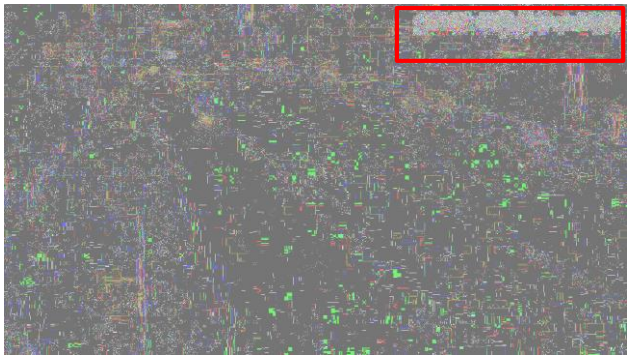
Elde edilen CLA analizi sonuçlarında renk kanallarına ait her bir sinyalin sıkıştırma sebebiyle birbirlerinden uzaklaştığını ve orijinal görüntüye ait analiz sonuçları referans alındığında dalgalanmaların değiştiği görülebilir (Şekil 18).



Şekil 18. Manipülasyon bulgusu görülebilen manipüle edilmiş görüntü karesine ait CLA Analizi

6.4. ELA Analizi *(ELA Analysis)*

Elde edilen ELA analizi sonuçlarına bakıldığında, kopyala-yapıştır şeklinde manipüle işleminin yapıldığını gösterir emareler rahatlıkla görülebilmektedir. Bu görüntü karesi üzerinde Adobe Photoshop CS6 yazılımının *"Stamp Tool"* fonksiyonu kullanılarak kopyala-yapıştır işlemi gerçekleştirilmiştir (Şekil 19).



Şekil 19. Manipülasyon bulgusu görülebilen manipüle edilmiş görüntü karesine ait ELA Analizi

Amatör ve profesyonel düzeyde yapılan manipülasyonların analiz sonuçlarına bakıldığında şüphelinin bıraktığı izlerin ne derecede sonuçları etkilediği görülmektedir. Amatör düzeyde yapılmış olan manipülasyon işleminde kopyala-yapıştır işlemi detaylı olarak çalışılmadığından görüntünün kendi içerisindeki bütünlüğü bozulmuş bu sebeple piksellerin birbirleri ile olan ilişkisi ortadan kalkmıştır. Yazılımsal analizler ise matematiksel işlemler olduğundan doğrudan pikseller arasında bulunan bu korelasyonu incelerler.

Güvenlik kamera kayıtları üzerinde kesme-kesinti ile ilgili olarak yapılan incelemelerde ilk olarak başvurulan gözlem tarih ve zaman sayacının akışının kesintili olup olmadığıdır. Genellikle bu gözlemde herhangi bir eksiklik görülmezse eldeki kaydın orijinal olduğu düşünülmektedir. Bu çalışmamızda bu tür bir gözlemin aslında yanlış bir inceleme metodu olduğu rahatlıkla görülebilmektedir. Elde bulunan video kayıtlarının orijinal olup olmadığı hususunda tarih ve zaman sayacının akışına bakılması alışılagelmiş olmasına rağmen yapılan en büyük yanlışlardan bir tanesidir. Yukarıda da görüldüğü üzere tarih zaman sayacı üzerinde yapılan manipülasyonların tespiti, günümüzde kullanılan hazır paket programların aracılığı ile mümkün değildir. Tarih zaman bilgilerinin orijinal olup olmadığına yönelik yazılan raporların da aslında sağlıklı kanaatler içermediği söylenebilir. Uzmanların bu tür bir eksikliği göz önünde bulundurarak incelemelerini farklı yöntemlerle yapması gerekmektedir. Aksi taktirde belki de çok büyük adli vakaların bu tür manipülasyonlar ile gizlenmesi ve bunun tespit edilememesi içten bile değildir.

Uzmanların tarih ve zaman sayacına yönelik yapacakları analizlerde, ellerindeki delil hakkında her türlü bilgiyi dijital ortamda elde etmeleri, bu bilgilerden yola çıkarak bir değerlendirme yapmaları gerekmektedir. Değerlendirmenin aşağıdaki sıra ve içerikte yapılması önerilmektedir:

1. Görsel değerlendirmeler yapılmalı, kayıt izlenmeli, sayaç dikkatlice takip edilmelidir;

2. Görüntünün EXIF bilgilerine başvurulmalı, bu sayede varsa bilgiler geçmişine ait yorumlamalar yapılmalı, sayısal görüntü işleme teknikleri ile yazılımsal incelemeler yaparak kesin sonuçlar elde etmeye çalışmalıdır;
3. Bütün bu sonuçlar hep birlikte değerlendirilerek bir sonuca varılmalıdır. Verilecek olan kanaatler adli makamlara yol gösterecek nitelikte açıklamalarla desteklenmeli ve sonuçlar raporda görsel olarak ifade edilebilmelidir. Bu sayede adli makamlarda görevli kişilerin sonuçları net olarak görmesi sağlanır ve sonucunda doğru hükmün verilmesine önemli derecede yardımcı olunur.

7. SONUÇ (CONCLUSION)

Sonuç olarak güvenlik kamera kayıtlarından elde edilen görüntüler üzerindeki tarih ve zaman sayacında yapılacak olan profesyonel manipülasyon işlemlerinin neredeyse tamamı sayısal analizler ile tespit edilememektedir. Bunun sebebi ise tarih ve zaman sayaçları görüntüler üzerine sonradan DVR cihazı aracılığı ile eklenen bileşenlerdir. Dolayısıyla manipülasyon tespit yazılımları görüntünün bütünüyle ilgilenirler ve sonucunda görüntünün bütününe haliyle uyumlu olmayan sayaçları manipüle edilmiş olarak tespit ederler. Her ne kadar tarih ve zaman sayacı orijinalde doğru bir sayaç olsa dahi görüntülenen alanla ilgili olmadığı için karşımıza bu şekilde çıkacaktır. Bu sebeple görüntü üzerinde yapılabilecek diğer manipülasyon işlemleri rahatlıkla tespit edilir iken tarih zaman sayacı üzerinde yapılacak manipülasyonların tespiti pekte mümkün olmamaktadır. Bu şekilde yapılan manipülasyonların tespit edilenlerinde ise manipüle eden şüphelinin iyi ve detaylı bir çalışma yapmamış olması analiz eden uzman için avantaj olmuştur.

Elde edilen sonuçlarda kanaate götürecek bulgular olmasa da, görsel olarak yapılacak incelemelerde mantıksal bir hata *(yazı karakteri, boyutları, renkleri, harekete duyarlı kameralar haricinde sayaç atlamaları, frame sayısı-sayaç orantısızlığı vb. hatalar)* bulunduğu taktirde fikir vermesi açısından bir beyanda bulunmak sağlıklı olacaktır. Görüntüler üzerinde yapılan manipülasyon analizlerinin, görsel ve yazılımsal olarak yapılmasının birbirlerini destekleyici olacağı ve bu yönüyle tam ve sağlıklı bir kanaat vermede önemli rol oynayacağı unutulmamalıdır.

Tarih ve zaman sayacı üzerindeki yapılan manipülasyonların tespitine yönelik incelemelere daha sonraki yazılarda değinilecektir.

KAYNAKLAR (REFERENCES)

[1] B. Silva, T. Larsen, "Setting the Watch Privacy and the Ethics of CCTV Surveillance", *The Modern Law RevieW*, 77(3), Oregon, 2014.

[2] NPIA (National Policing Improvement Agency), "Practice Advice on the Use of CCTV in Criminal Investigations", 2011.

[3] E.M. Harwood., **Digital CCTV A Security Professional's Guide – Understand the Effects of Digital Technology on the Security Industry**, Pamela Chester, Elsevier, ABD, 2008.

[4] W. Jackson, **Digital Video Editing Fundamentals**, Welmoed Spahr, Apress&Harryarts, ABD, 2016.

[5] G.M. Gines, G.M. Andres, "Time and Date OCR in CCTV Video", **Image Analysis and Processing-ICIAP 2005**, 3617, F.Roli&S.Vitulano, Springer, Verlag Berlin Heidelberg, 703-710, 2005.

[6] İnternet: "Scientific Working Group Imaging technology", www.swgit.org, 23.10.2016.

[7] N. Dadashi, **Automatic Surveillance and CCTV Operator Workload**, Yüksek Lisans Tezi, University of Nottingham, School of Computer Science, 2008.

[8] P. Alvarez, "Using Extended File Information (EXIF) File Headers in Digital Evidence Analysis", *International Journal of Digital Evidence*, 2(3), 1-5, 2004.

[9] L. Haitao, S. Refik, "A Low Complexity Algorithm for H.264/AVC Intra Prediction", **International Conference on Cyberworlds**, 77-81, 2013.

[10] İnternet: M. Richardon, "Principal Component Analysis", http://people. maths. ox. ac. uk/richardsonm/SignalProcPCA. Pdf, 24.05.2016.

[11] M.B. Ranjani, R. Poovendran, "Image Duplication Copy Move Forgery Detection Using Discrete Cosine Transforms Method", *International Journal of Applied Engineering Research*, 11(4), 2671-2674, 2016.

[12] R. Gonzalez, R. Woods, **Digital Image Processing**, Marcia J. Horton, Prentice Hall, New Jersey, ABD, 2008.

[13] İnternet: D. Kalman, "A Singularly Valuable Decomposition: The SVD of a Matrix", http://www-users.math.umn.edu/~lerman/math5467/svd.pdf, 25.06.2016.

[14] W. Yu-Yao, L. Zheng-Ming, L. Wang, M. Wang, "A Scale Invariant Feature Transform Based Method", *Journal of Information Hiding and Multimedia Signal Processing*, 4(2), 73-89, 2013.

[15] E. Oyallon, J. Rabin, "An Analysis of the SURF Method", *Image Processing On Line*, 5, 176-218, 2015.

[16] İnternet: "A Guide to Understanding Video Containers & Codecs", http://www.netmode.ntua.gr/courses/postgraduate/video_communications/2014/Rice_U_Video_Formats_Guide.pdf, 24.04.2016.

[17] A.B. Watson, "Image Compression Using the Discrete Cosine Transform", *Mathematica Journal*, 4(1), 81-88, 1994.

[18] K.N. Plataniotis, A.N. Venetsanopoulos, **Color Image Processing and Applications**, Springer, 2000.

[19] P.M. Badgley, **Compression Level Analysis: Examining Video Recompression Levels for Forensic Examination**, Yüksek Lisans Tezi, University of Colorado Denver, Media Forensic, 2015.

[20] P. Prasad, "Image Forgery Localization via CFA Based Feature Extraction and Poission Matting", *International Journal of Science and Research (IJSR)*, 3(10), 1273-1278, 2014.

[21] A.M. Arun, "A Review on Image Forgery and Its Detection", *International Journal of Computing and Technology*, 2(5), 139-149, 2015.

[22] A.D. Anderson, **Digital Image Analysis: Analytical Framework For Authenticating Digital Images**, Yüksek Lisans Tezi, University of Colorado Denver, Media Forensic, 2001.

[23] C.G. Marrion, **Digital Image Manipulation Detection on Facebook Images**, Yüksek Lisans Tezi, University of Colorado Denver, Media Forensic, 2001.