

T.C.
TRAKYA ÜNİVERSİTESİ
FEN BİLİMLERİ ENSTİTÜSÜ

SIKIŞTIRILMIŞ VIDEO AKIMININ
DÜZENSİZ HARİTALAR VE
BAŞLANGIÇ KODLARINA
DAYALI ŞİFRELENMESİ

Deniz TAŞKIN

Doktora Tezi

Bilgisayar Mühendisliği Anabilim Dalı

Danışman: Yrd. Doç Dr. Nurşen Suçsuz

Edirne 2007

T.C.
TRAKYA ÜNİVERSİTESİ
FEN BİLİMLERİ ENSTİTÜSÜ

SIKIŞTIRILMIŞ VIDEO AKIMININ DÜZENSİZ HARİTALAR VE
BAŞLANGIÇ KODLARINA DAYALI ŞİFRELENMESİ

Deniz TAŞKIN
Doktora Tezi
Bilgisayar Mühendisliği Anabilim Dalı

Bu tez 06/07/2007 tarihinde aşağıdaki jüri tarafından kabul edilmiştir.

Prof.Dr. Şaban EREN
Başkan

Yrd.Doç.Dr. Nurşen SUÇSUZ
Danışman

Yrd.Doç.Dr. Cavit TEZCAN
Üye

Yrd.Doç.Dr. Seyfettin DALGIÇ
Üye

Yrd.Doç.Dr. Erdem UÇAR
Üye

ÖZET

Doktora Tezi, Sıkıştırılmış Video Akımının Düzensiz Haritalar ve Başlangıç Kodlarına Dayalı Şifrenmesi, T.C. Trakya Üniversitesi, Fen Bilimleri Enstitüsü, Bilgisayar Mühendisliği Anabilim Dalı.

Bu çalışmanın amacı, kendine has bir yapısı olan video akımın şifrenmesi için yeni bir yöntem geliştirmektir. Görsel veriye artan ilgi sebebiyle video dosyaları günlük yaşantıda çok sık kullanılmaktadır. Bu artan ilgi sebebi ile video dosyalarının güvenliği de ön plana çıkmaktadır.

Uzunca bir süredir metin dosyalarının güvenliğini başarılı şekilde koruyan geleneksel şifreleme yöntemleri, video dosyalarının güvenliğini sağlamak için yetersiz kalmaktadır. Bu yöntemler video dosyalarına uygulandığında, şifreyi kırmak isteyen kişilere açık noktalar bırakmaktadır. Video dosyaları büyük alan kapladıkları için şifreleme süresi de uzamaktadır.

Video dosyalarının şifrenmesi için kullanılan yöntemler kısmi şifrelemeye yöneliktir. Kısmi şifreleme uygulanacak bölgelerin seçimi şifreleme güvenliği açısından çok önemlidir.

Bu çalışma, kısmi şifreleme, düzensiz haritalar ve başlangıç kodları üzerine yapılmış özgün bir çalışmadır.

Bu tez 2007 yılında yapılmıştır ve 92 sayfadan oluşmaktadır.

ANAHTAR KELİMELER: MPEG kodlama, Kısmi şifreleme, Düzensiz haritalar, Başlangıç kodları, DCT

ABSTRACT

PhD Thesis, Encrypting Of Compressed Video Stream Based On Chaotic Maps And Start Codes, T.C. Trakya University, Graduate School Of Natural And Applied Sciences, Department Of Computer Engineering.

The purpose of this research is developing a new method for encrypting video stream that has particular structure. Because of increasing interest in visual data, video files are commonly used in daily life. Because of this interest, video files security become more important.

Successfully used for securing textual data for long times, traditional encryption methods are insufficient for keeping video files secure. When these methods are used for video files, leaked information can be used by the attacker. While video files cover large amounts of storage, encryption time is also extended.

Methods used for encryption video files, are based on selective encryption. Selection of areas which are used for selective encryption is very important for encryption security.

This work is an original research based on selective encryption, chaotic maps and start codes.

This thesis is done in 2007 and consists of 92 pages.

KEYWORDS: MPEG Coding, Selective encryption, Chaotic maps, Start codes, DCT

İÇİNDEKİLER

ÖZET	i
ABSTRACT	ii
ŞEKİLLER TABLOSU	v
ÇİZELGELER TABLOSU	viii
1. GİRİŞ	1
2. VIDEO VERİSİ	4
2.1. Renk Uzayları	5
2.1.1. RGB renk uzayı	6
2.1.2. YUV renk uzayı	7
2.1.3. YIQ renk uzayı	8
2.1.4. YCbCr renk uzayı	9
2.1.4.a. 4:4:4 YCbCr biçimi	10
2.1.4.b. 4:2:2 YCbCr biçimi	10
2.1.4.c. 4:1:1 YCbCr Biçimi	11
2.1.4.d. 4:2:0 YCbCr biçimi	12
2.1.5. HSI, HLS ve HSV renk uzayları	13
2.2. Video Sinyalleri	15
2.3. Sayısal Video	17
3. VIDEO SIKIŞTIRMA	19
3.1. MPEG Video Sıkıştırma Yöntemi	20
3.2. I Çerçevesi	22
3.2.1. Renk uzayı dönüşümü ve örnekleme	22
3.2.2. İç-çerçeve sıkıştırma	24
3.2.2.a. Ayrık kosinüs dönüşümü	25
3.2.2.b. Nicelendirme	27
3.2.2.c. Zig-Zag tarama	28
3.2.2.d. Değişken uzunlukta kodlama	29
3.3. P Çerçevesi	31
3.3.1. Ara-çerçeve sıkıştırması ve hareket kodlama	32
3.4. B Çerçevesi	33
4. MPEG AKIMININ ÇÖZÜLMESİ	35
4.1. Başlangıç Kodları	36
4.1.1. Akım başlangıç kodu	37
4.1.2. Resim grubu başlangıç kodu	38
4.1.3. Resim başlangıç kodu	40
4.1.4. Dilim başlangıç kodu	41
4.1.5. Makro blok ve blok başlangıcı	42
5. İÇERİK KORUMA	44
5.1. Görsel Şifreleme	45
5.2. Geleneksel Şifreleme	47
5.3. Kısmi Şifreleme	49
5.4. Düzensiz Haritalar Kullanarak Şifreleme	50
6. VIDEO ŞİFRELEME KONUSUNDA DAHA ÖNCE YAPILMIŞ ÇALIŞMALAR	51

6.1.	SECMPEG.....	51
6.2.	AEGIS	53
6.3.	Zig-Zag Permütasyon Algoritması	53
6.4.	VEA Video Şifreleme Algoritması.....	55
6.5.	Video Şifreleme Algoritmaları	57
6.5.1.	Algoritma I.....	58
6.5.2.	Algoritma II (VEA)	58
6.5.3.	Algoritma III(MVEA).....	59
6.5.4.	Algoritma IV(RVEA)	61
6.6.	Video Şifreleme Metotları.....	62
6.7.	MHT Şifreleme Metodu ve MSI kodlayıcısı.....	63
6.8.	Biçim Uyumlu Şifreleme	64
6.9.	Seçimli Karıştırma Algoritması.....	64
7.	SIKIŞTIRILMIŞ VIDEO AKIMININ DÜZENSİZ HARİTALAR VE BAŞLANGIÇ KODLARINA DAYALI ŞİFRELENMESİ.....	66
7.1.	MPEG Akımında Başlık Şifreleme.....	66
7.2.	MPEG Akımında Operatör İşlemlerinin Kısıtlanması Yoluyla İçerik Koruma.....	69
7.3.	Sıkıştırılmış Video Güvenliği.....	71
7.4.	Seçimli XOR İşlemi İle MPEG Video Akımını Koruma.....	73
7.5.	Byte Dağılımını Değiştirerek MPEG Video Akımını Koruma	74
7.6.	Önerilen Yöntem	75
7.6.1.	Algoritma I.....	76
7.6.2.	Algoritma II.....	78
8.	SONUÇ	80
	EK-A:DEĞİŞKEN UZUNLUKTA KODLAMA ÇİZELGELERİ	83
	EK-B: KISALTMALAR.....	85
	KAYNAKLAR.....	86
	TEŞEKKÜR	91
	ÖZGEÇMİŞ.....	92

ŞEKİLLER TABLOSU

Şekil 2.1. Video, bir grup hareketsiz görüntüden oluşmaktadır	5
Şekil 2.2. RGB renk uzayı.....	7
Şekil 2.3. UV renk bileşenleri	8
Şekil 2.4. I ve Q renk bileşenleri	9
Şekil 2.5. 4:4:4 YCbCr biçimi	10
Şekil 2.6. 4:2:2 YCbCr biçimi	11
Şekil 2.7. 4:1:1 YCbCr biçimi	11
Şekil 2.8. MPEG İçin YCbCr örneklemeleri.....	12
Şekil 2.9. HLS renk uzayı	13
Şekil 2.10. Altıgen huni şeklinde HSV renk uzayı.....	14
Şekil 2.11. Çift altıgen huni şeklinde HSI renk modeli	15
Şekil 2.12. Video çerçevelerinin taranması.....	16
Şekil 2.13. Analog siyah-beyaz video sinyali	16
Şekil 2.14. Renkli analog video sinyali	17
Şekil 2.15. Analog videonun sayısallaştırılması.....	18
Şekil 3.1. Mpeg çerçeve tipleri.....	21
Şekil 3.2. I çerçevesinin kodlanması	22
Şekil 3.3. Değişik Y değerlerine karşılık CbCr tonları.....	23
Şekil 3.4. Renk uzayı dönüşümleri ve örnekleme	24
Şekil 3.5. Ayrık kosinüs dönüşümü	26
Şekil 3.6. Örnek sıkıştırma.....	27
Şekil 3.7. İç-nicelik matrisi ve iç-olmayan-nicelik matrisi	27
Şekil 3.8. Niceleme işlemi	28
Şekil 3.9. Zig-Zag tarama.....	29
Şekil 3.10. Örnek çerçeve ve hareket vektörleri.....	32
Şekil 3.11. P çerçevesinin kodlanması.....	33
Şekil 3.12. B çerçevesinin kodlanması	34
Şekil 4.1. MPEG video katman yapısı	35
Şekil 4.2. Akım başlangıç kodu ve akımın devamı	37

Şekil 4.3. Resim gurubu başlangıç kodu	39
Şekil 4.4. Resim başlangıç kodu ve akımın devamı	40
Şekil 4.5. Video gösterim ve akım sıraları.....	41
Şekil 4.6. Dilim başlangıç kodları	42
Şekil 4.7. Makro blok	43
Şekil 5.1. Görsel şifreleme	44
Şekil 5.2. Nagravizyon şifreleme aşamaları.....	45
Şekil 5.3. Örnek blok parlaklık değerleri.....	46
Şekil 5.4. Geleneksel şifreleme	47
Şekil 5.5. Simetrik şifreleme	47
Şekil 5.6. Asimetrik şifreleme	48
Şekil 5.7. Kısmi şifreleme	50
Şekil 6.1. SECMPEG video şifreleme metodu birinci seviye.....	51
Şekil 6.2. SECMPEG video şifreleme metodu ikinci ve üçüncü seviye	52
Şekil 6.3. SECMPEG video şifreleme metodu dördüncü seviye	52
Şekil 6.4. AEGIS şifreleme metodu	53
Şekil 6.5. Zig-zag sıralama.....	54
Şekil 6.6. Zig-zag permütasyon şifreleme metodu	54
Şekil 6.7. Video şifreleme algoritması (VEA) ikinci yaklaşım.....	56
Şekil 6.8. Video şifreleme algoritmaları	57
Şekil 6.9. VEA şifreleme algoritması	59
Şekil 6.10. MVEA şifreleme algoritması.....	60
Şekil 6.11. Orijinal görüntü ve şifrelenmiş görüntü sonuçları	61
Şekil 6.12. $n=3$ için metot 1 şifreleme	62
Şekil 6.13. Huffman ağacının değişimi.....	64
Şekil 7.1. 1 Numaralı dilim	67
Şekil 7.2. Orijinal ve şifrelenmiş MPEG akımları.....	67
Şekil 7.3. Şifrelenmiş akım izleme hatası	68
Şekil 7.4. Video boyutuna göre toplam başlık boyutları	68
Şekil 7.5. MPEG akımında başlık şifreleme metodu.....	69
Şekil 7.6. Movie Maker yazılımı ve korunmuş video akımı.....	70
Şekil 7.7. Açık ve öngörülen yöntemle şifrelenmiş video akımları	72

Şekil 7.8. Şifrelenmiş akım izleme hatası	73
Şekil 7.9. Seçimli XOR işlemi	74
Şekil 7.10. Byte dağılımı değiştirme	75
Şekil 7.11. Temel tarama desenleri.....	77
Şekil 7.12. Örnek video akımı ve şifrelenmiş görüntü	78
Şekil 7.13. Sıkıştırılmış video akımının düzensiz haritalar ve başlangıç kodlarına dayalı kısmi şifrelenmesi.....	79

ÇİZELGELER TABLOSU

Çizelge 2.1. Küp köşegenlerinde elde edilen renk tonları	6
Çizelge 4.1. Başlangıç kodları.....	36
Çizelge 4.2. Akım başlangıç kodu ve örnek akım ile ilgili bilgiler.....	37
Çizelge 4.3. Resim grubu başlangıcı ve örnek akım ile ilgili bilgiler	39
Çizelge 4.4. Resim başlangıcı ve örnek akım ile ilgili bilgiler	40
Çizelge 4.5. Dilim başlangıcı ve örnek akım ile ilgili bilgiler	42
Çizelge 8.1. İncelenen yöntemlerin şifreleme hızları	80
Çizelge 8.2. Önerilen yöntemin dosya boyutuna bağlı performansı	81

BÖLÜM 1

GİRİŞ

Video belli bir zaman aralığında ardı ardına gösterilen resim kareleri olarak tanımlanabilir. Birçok çeşit ve uygulama tekniği olduğu halde video sinyalleri, temel olarak görsel bilgiyi bir noktadan başka bir noktaya taşıma yoludur. Başlangıçta analog olarak kaydedilip üzerinde işlem yapılarak yayınlanan video, teknolojideki ilerlemeye bağlı olarak sayısallaştırılarak bilgisayar ortamında işlenmeye ve yayınlanmaya başlamıştır. Bugüne dek çoğu video cihazı birincil olarak analog video için tasarlanmış ve sayısallaştırılmış video, düzenleme işlemleri gibi profesyonel uygulamalarla sınırlandırılmıştır. Sayısallaştırılmış video yüksek kalitede ses ve resim gibi avantajlar sağlamanın yanında görüntü kalitesini uzun süreler boyunca koruyabilmektedir. Tüm pozitif özelliklerine rağmen video verisi, kapladığı alan bakımından geleneksel veriden farklılık göstermektedir. Sayısallaştırılmış video görüntüleri büyük miktarda yer kaplamaktadır ve iletim zorlukları bulunmaktadır. Sayısallaştırılmış bir video görüntüsünün gerçek zamanlı olarak iletilebilmesi için, bugünün imkânlarında bile çok yüksek sayılabilecek, yaklaşık 200Mps'lik bir bant genişliğine ihtiyaç duyulmaktadır.

Video verisinin kapladığı alan ve bant genişliği gereksinimlerinden dolayı sıkıştırılması gerekmektedir. Günümüzde neredeyse tüm video gösterici cihazlar depolama, bant genişliği ve daha da önemlisi, maliyeti düşürmek için sıkıştırma metotlarına dayanmaktadır. Video verisinin sıkıştırılmasında geleneksel verilere uygulanan yöntemler kullanıldığında yüksek sıkıştırma oranları yakalanamamaktadır. Büyük miktarda görsel veri içeren sayısallaştırılmış video eşsiz bir yapıya sahiptir. 1988 yılında video dosyalarının sayısallaştırılması ve video dosyalarına özel, sıkıştırma yöntemlerinin standartlaşması için ISO tarafından MPEG kurulmuştur. Bu grubun çalışmaları sonucunda oluşturulan MPEG video sıkıştırma yöntemi günümüz video depolama ve iletiminin temelini teşkil etmektedir. Benzersiz ve yüksek sıkıştırma oranları MPEG video sıkıştırmasını vazgeçilmez kılmış ve video verisinin geleneksel

verilerden farklı bir biçimde ele alınması durumunda ne kadar başarılı olunabileceğini göstermiştir.

Son dönemlerde MPEG sıkıştırma yöntemi anahtar teknoloji olarak karşımıza çıkmakta ve birçok platformda, paralel olarak MPEG çözümler geliştirilmektedir. Günümüz koşullarında artan kullanım alanlarına bağlı olarak video dosyalarının güvenlik şartlarının yerine getirilmesi kaçınılmazdır. Şifreleme ve şifre çözme, güvenli sistem kurmanın temel teknolojileridir. İçerik koruma ve erişim kontrolü genellikle şifreleme ile sağlanmaktadır. Video verisinin içeriğiyle ilgili bilgiler doğrultusunda güvenliğinin sağlanması sistematik biçimde ele alınmalıdır. Buna yönelik çalışmalar temel olarak ikiye ayrılmaktadır. Video sayısallaştırıldıktan hemen sonra şifrelenebilir ya da sayısallaştırılmış video verisi sıkıştırıldıktan sonra şifrelenebilir. Kendine has özel bir yapısı olan video verisinin sayısallaştırıldıktan hemen sonra şifrenmesi, bu yapı düşünülerek tasarlanmış video sıkıştırma yöntemlerinin sıkıştırma yüzdelerini ve video kalitelerini büyük oranda düşürmektedir. Diğer yaklaşım video verisinin sayısallaştırıldıktan sonra şifrenmesidir. Günümüz şifreleme algoritmaları alfa-sayısal veriyi şifreleme ve çözmeye yönelik kullanılmaktadır. Prensipte olarak sayısal video verisi bir bit akımına dönüştürülerek geleneksel veri gibi şifrelenebilir. Tıpkı sıkıştırma işleminde olduğu gibi, düz metinden yapısal farklılıklar gösteren video verisinin güvenlik gereksinimleri de farklılık göstermektedir. Sayısallaştırılmış ve sıkıştırılmış video verisinin alfa-sayısal biçimde ele alınıp şifrenmesi hatalı bir yaklaşımdır. Video verisinin eşsiz doğasında dolayı “ya hep- ya hiç” koruma mantığına sahip geleneksel şifreleme yöntemleri video verisinin güvenliği için uygun değildir. Şifreli bir veriden anahtar bilinmeden yapılabilecek kırma işleminin ardında şifreli metinden elde edilebilecek açık noktaları vardır. Düşman video verisinin fark edilebilir güvenlik açıklarını kullanarak şifrelenmiş görüntüyü izlenebilir kılabilir. Sıkıştırılmış video dosyaları, metin dosyaları gibi değerlendirilip geleneksel şifreleme yöntemleriyle korunamazlar. Bu yüzden video verisinin korunması, video kodlamanın bir alanıdır. Geleneksel yöntemle şifrelenmiş video dosyaları diğer tür dosyalara göre çok daha kolay çözülebilir. Geleneksel şifreleme metodlarının güvenilirliği arttırıldıkça yapılan matematiksel işlemlerin karmaşıklığı da artmaktadır. Yüksek miktarda veri içermesinden dolayı video verisinin şifrenmesi bu bakımdan da yüksek maliyet getirmektedir.

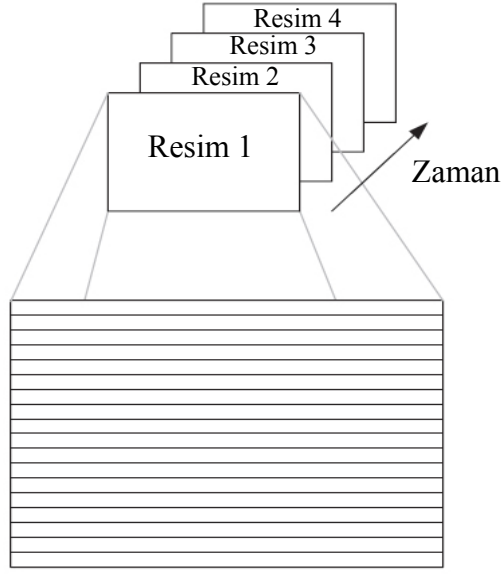
Nasıl ki video verisini sıkıřtırmak için video verisine özel metotlar geliştirilmiř ise, video dosyalarının řifrenmesi için de geleneksel metotlar kullanılmamalı, video verisine özel metotlar geliştirilmelidir. Tıpkı video verisini sıkıřtırma geleneksel sıkıřtırma yöntemleriyle yapılamayacağı gibi video verisinin güvenlięi de geleneksel řifreleme metotlarıyla sağlanamaz. Bu tez video verisinin erişim kontrolünü denetlemek için gerçek zamanlı çalışabilecek düzeyde yeni bir yöntemi öne sürmektedir. Önerilen yöntem düşük sistem kaynak ihtiyacı ve karmaşıklık seviyesine karşılık sıkıřtırılmıř video akımına özel řifreleme, yüksek güvenlik, taşınabilirlik ve hız sağlamaktadır.

BÖLÜM 2

VIDEO VERİSİ

Birçok çeşidi ve uygulama şekli olmasına rağmen video, temelde görsel bir bilginin bir noktadan diğer bir noktaya transfer edilmesinde kullanılan sinyale verilen isimdir (Jack, 1995). Genellikle kamera tarafından görsel bilgiler video sinyaline dönüştürülmekte, dağıtım kanalları yoluyla alıcıya kadar iletilmekte ve alıcı tarafından tekrar görsel hale dönüştürülmektedir. Kelime köken olarak Latince Videre (görmek)'den gelmektedir ve video *görüyorum* demektir. Video teknolojisi ilk olarak televizyon yayınlarında kullanılmıştır. Gelişen teknolojiyle birlikte birçok kişisel kullanım alanı bulmuştur.

Başlangıçta video, sadece renksiz analog bilgi içermektedir. Renkli yayınlar geliştirildiğinde renkler, analog RGB verisi şeklinde ifade edilmiştir. Bununla birlikte bu teknik siyah-beyaz çözümün 3 katı bant genişliği gerektirdiğinden renk bilgisini YIQ ya da YUV şeklinde ifade eden alternatif yöntemler geliştirilmiştir. YIQ ya da YUV analog bilgiyi üç farklı sinyal yerine orijinal siyah-beyaz video sinyali ile aynı bant genişliğinde tek bir sinyal olarak ileten bir yöntemdir. Bu bileşik sinyal günümüzde hala kullanılan NTSC, PAL ve SECAM video standartlarının temelini oluşturmaktadır. Bugün videoyu ifade etmenin birçok yolu bulunmaktadır ve bunlar matematiksel olarak hala RGB'ye bağlıdır.



Şekil 2.1. Video, bir grup hareketsiz görüntüden oluşmaktadır

Video, devamlı hareket eden bir görüntü olarak görülmesine rağmen, şekil 2.1’de gösterildiği gibi hareketli gözükecek kadar hızlı değişen bir grup hareketsiz görüntüden oluşmaktadır (Jack, 1995).

Video görüntüsünün piksel cinsinden büyüklüğüne *çözünürlük* denmektedir.

2.1. Renk Uzayları

Renk uzayları, renkleri tanımlamak için kullanılan matematiksel modellerdir. Renk uzayları, bütün renkleri temsil edecek şekilde oluşturulmaktadır. Renkmetri biliminin temelini oluşturan Grassmann’ın birinci kuralına göre, bir rengi belirlemek için birbirinden bağımsız 3 değişkene ihtiyaç vardır. Bu yüzden renk uzayları 3 boyutlu olarak tasarlanmaktadır. En popüler üç renk modeli bilgisayar grafiklerinde kullanılan RGB, video sistemlerinde kullanılan YCbCr ve renkli dökümlerde kullanılan CMYK’dır. Tüm renk uzayları, kamera ve tarayıcı gibi aygıt kaynaklı RGB bilgisi kullanılarak elde edilmektedir (Yılmaz, 2002).

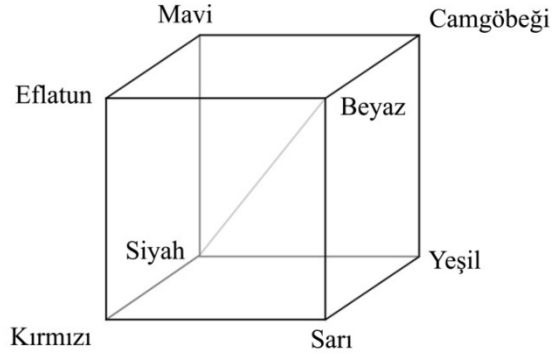
2.1.1. RGB renk uzayı

RGB renk uzayı bilgisayar grafikleri üzerinde yoğun bir kullanım alanına sahiptir. Kırmızı(R) , yeşil(G) ve mavi(B) birbirine karıştırılabilen üç temel renktir. Diğer renkler ise, bu üç renk karıştırılarak elde edilebilmekte ve şekil 2.2’de olduğu gibi 3 boyutlu olarak gösterilmektedir. Küpün köşegenleri tarafından gösterilen, her bir rengin eşit miktarda bulunduğu bölgelerde değişik tonlar elde edilmektedir. Çizelge 2.1’de bu seviyelere karşılık ortaya çıkan renkler gösterilmektedir.

Çizelge 2.1. Küp köşegenlerinde elde edilen renk tonları

	Aralık	Beyaz	Sarı	Camgöbeği	Yeşil	Eflatun	Kırmızı	Mavi	Siyah
R	0-255	255	255	0	0	255	255	0	0
G	0-255	255	255	255	255	0	0	0	0
B	0-255	255	0	255	0	255	0	255	0

RGB renk uzayı, renkli monitörlerin istenilen rengi oluşturmak için kırmızı, yeşil ve mavi rengi kullanmalarından dolayı bilgisayar grafikleri için en uygun renk uzayıdır. Bu yüzden RGB renk uzayının seçilmesi, sistemin tasarım ve mimarisini basitleştirmektedir. RGB renk uzayı uzun yıllardır kullanıldığından çok sayıda hazır yazılım rutinlerini bulunmaktadır. Bir sistemin RGB renk uzayı kullanılarak tasarlanması avantaj sağlamaktadır. Buna rağmen RGB, gerçek dünya resimleriyle çalışırken çok da etkin olmamaktadır. RGB renk küpündeki herhangi bir rengi oluşturmak için üç RGB bileşeninin aynı bant genişliğine sahip olması gerekmektedir. Bunun bir sonucu olarak RGB bileşenlerini tutan çerçeve tamponu, aynı piksel derinliğe ve gösterim çözünürlüğüne sahip olmak zorundadır (Jack, 1995).



Şekil 2.2. RGB renk uzayı

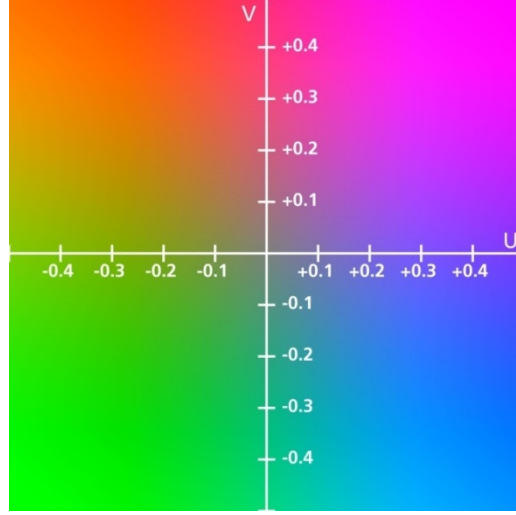
RGB renk uzayındaki bir resmi işlemek etkili bir yol değildir. Örneğin verilen bir pikselin renk yoğunluğu değiştirilmek istendiğinde, çerçeve tamponundan üç RGB değeri de okunmak zorundadır. Ardından renk yoğunluğu hesaplanmakta ve istenilen değişiklik yapıldıktan sonra yeni RGB değeri elde edilerek çerçeve tampona geri yazılmaktadır. Farklı bir renk uzayı kullanılarak sistemin, saklanan resmin yoğunluk ve renk biçimine doğrudan erişim hakkı olduğu taktirde bazı işlem basamakları daha kolay ve hızlı yapılabilir.

Bu ve bunun gibi birkaç nedenden dolayı birçok video standardı parlaklık ve iki farklı renk sinyali kullanmaktadır. Bunlardan en genel olanları YUV, YIQ ve YCbCr renk uzaylarıdır. Bu renk uzaylarının birçok benzerliği olmasına rağmen bir takım farklılıkları da bulunmaktadır.

2.1.2. YUV renk uzayı

YUV renk uzayı PAL, NTSC ve SECAM bileşik ve renkli video standartlarında kullanılmaktadır. Siyah-beyaz sistem parlaklık bilgisini Y bileşeni ile tutmaktadır. U ve V Renk bilgisi bir siyah-beyaz televizyon alıcısının görüntüyü hala siyah-beyaz gösterebileceği şekilde sinyale dahil edilmektedir. Bu renk uzayının geliştirilmesindeki temel amaç siyah-beyaz alıcıların, renkli video sinyalini siyah-beyaz şeklinde gösterebilmeleridir. Renkli televizyon alıcıları ise ilave renk bilgisini görüntüyü

renklendirmek için kullanılmaktadırlar. Şekil 2.3 U ve V renk bileşenlerini göstermektedir.



Şekil 2.3. UV renk bileşenleri

RGB renk uzayındaki bir rengi YUV renk uzayındaki bir renge dönüştürmek için denklemler

$$Y = 0.229R + 0.587G + 0.114B$$

$$U = -0.147R - 0.289G + 0.436B = 0.492(B - Y)$$

$$V = 0.615R - 0.515G - 0.100B = 0.877(R - Y)$$

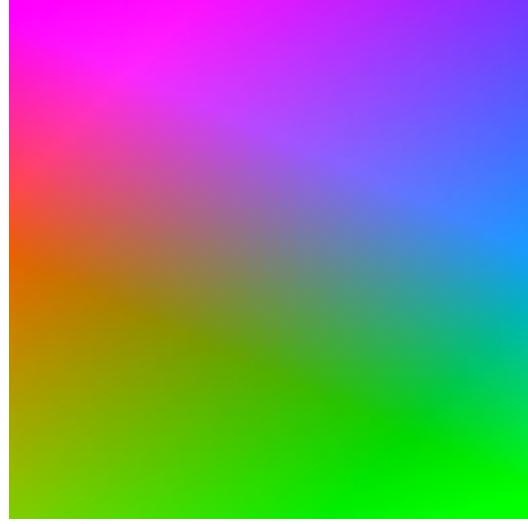
formlarında verilmektedir (Jack, 1995).

Sayısal RGB değerleri 0 ile 255 arasındadır. Y bileşeni 0-255 arasında, U bileşeni +/- 112 arasında, V ise +/- 157 arasında değerler almaktadır.

2.1.3. YIQ renk uzayı

YIQ renk uzayı, YUV renk uzayından türetilmiş ve NTSC bileşik video standardında seçimlilik olarak kullanılan bir renk uzayıdır. Burada Y parlaklık değerini

göstermekte, I ve Q değerleri ise renk bilgisini transfer etmek için kullanılmaktadır. Şekil 2.4 I ve Q renk bileşenlerini göstermektedir.



Şekil 2.4. I ve Q renk bileşenleri

Temel dönüşüm denklemleri

$$Y = 0.299R + 0.587G + 0.114B$$

$$I = 0.596R - 0.275G - 0.321B = V \cdot \cos 33^\circ - U \cdot \sin 33^\circ$$

$$Q = 0.212R - 0.532G + 0.311B = V \cdot \sin 33^\circ + U \cdot \cos 33^\circ$$

formlarında verilmektedir (Jack, 1995).

Sayısal RGB bileşenleri 0-255 arasında değerler almaktadır. Y 0-255 arasında, I +/- 152, Q ise +/- 134 arasında değerler almaktadır. I ve Q değerleri, U ve V kesişiminin 33 derece döndürülmesi ile elde edilmektedir.

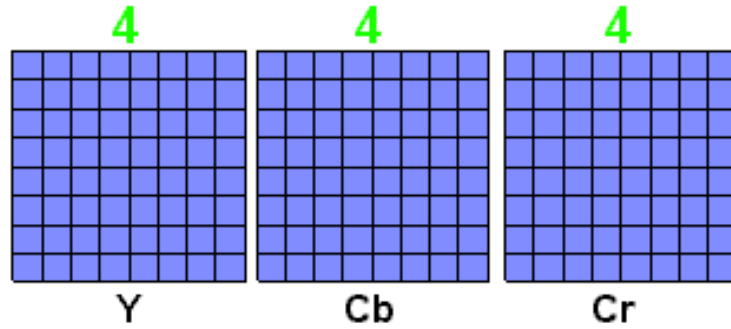
2.1.4. YCbCr renk uzayı

YCbCr renk uzayı, dünya çapında sayısal video standardı oluşturma çabaları sırasında ortaya çıkmıştır. YCbCr, YUV renk uzayının boyutlandırılmış ve kaydırılmış

bir şeklidir. Y , 8 bitliklik 16-235 aralığında tanımlanmaktadır. Cb ve Cr ise de 16-240 arasında tanımlanmaktadır. 4:4:4, 4:2:2, 4:1:1, 4:2:0 gibi birçok YCbCr örnekleme biçimi bulunmaktadır (Jack, 1995).

2.1.4.a. 4:4:4 YCbCr biçimi

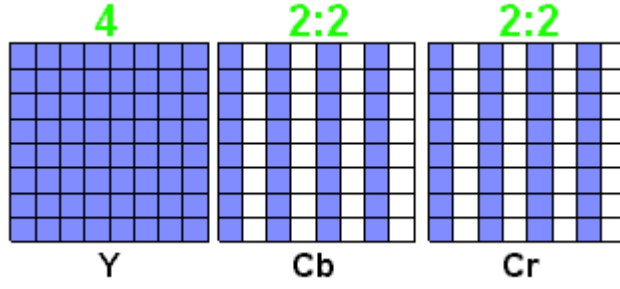
Şekil 2.5, YCbCr örnek dağılımını 4:4:4 biçiminde göstermektedir. Her bir örnek bir Y , bir Cb ve bir de Cr değerine sahiptir. Tipik olarak her bileşen 8 bitlik yer kapladığından her bir örnek 24 bit yer kaplamaktadır.



Şekil 2.5. 4:4:4 YCbCr biçimi

2.1.4.b. 4:2:2 YCbCr biçimi

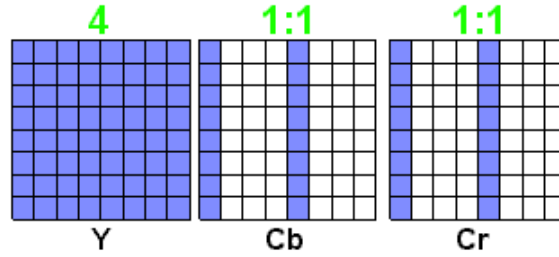
Şekil 2.6, 4:2:2 biçimi için YCbCr yerleşimini göstermektedir. Her yatay iki Y örneği için, sadece bir Cb , Cr örneği bulunmaktadır. Her bir bileşen tipik olarak 8 bitlik yer kapladığından toplam 16 bite ihtiyaç duyulmaktadır. 4:2:2 YCbCr biçimindeki verinin gösterilebilmesi için öncelikle 4:4:4 YCbCr biçimine dönüştürülerek eksik $CbCr$ değerlerinin yeniden oluşturulması gerekmektedir.



Şekil 2.6. 4:2:2 YCbCr biçimi

2.1.4.c. 4:1:1 YCbCr Biçimi

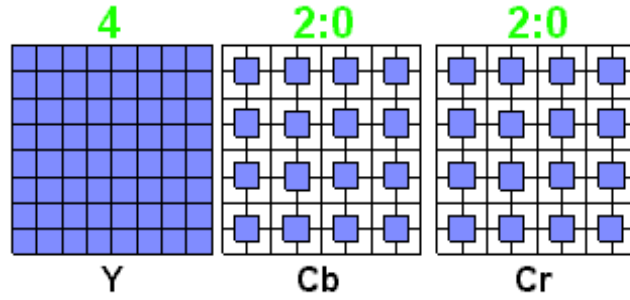
Şekil 2.7, YUV12 olarak da bilinen 4:1:1 biçimi için YCbCr yerleşimini göstermektedir. Bu biçim bazı son kullanıcı video ve DV sıkıştırma uygulamalarında kullanılmaktadır. Her bir dört yatay Y örnekleme için sadece bir Cb ve Cr değeri bulunmaktadır. Her bileşen tipik olarak 8 bit olduğundan örneklemler şekildeki gibi konumlandırılmış 12 bit gerektirmektedir. 4:1:1 YCbCr biçimindeki verinin gösterilebilmesi için öncelikle 4:4:4 YCbCr biçimine dönüştürülerek eksik CbCr değerlerinin yeniden oluşturulması gerekmektedir.



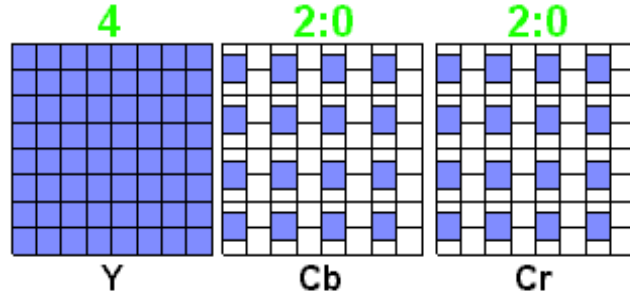
Şekil 2.7. 4:1:1 YCbCr biçimi

2.1.4.d. 4:2:0 YCbCr biçimi

4:2:2 biçiminde kullanılan, sadece yatayda 2:1 oranında *Cb* ve *Cr* örneklerinde azaltma işlemi yerine 4:2:0 YCbCr biçimi *Cb* ve *Cr* örneklerindeki 2:1 oranındaki azaltma işlemini, hem yatay hem de dikey yönlerde gerçekleştirmektedir. Bu biçim genel olarak video sıkıştırma için kullanılmaktadır. Çeşitli 4:2:0 örnekleme biçimleri vardır, bir kısmı şekil 2.8’de gösterilmektedir.



a) MPEG-1 için 4:2:0 örnekleme



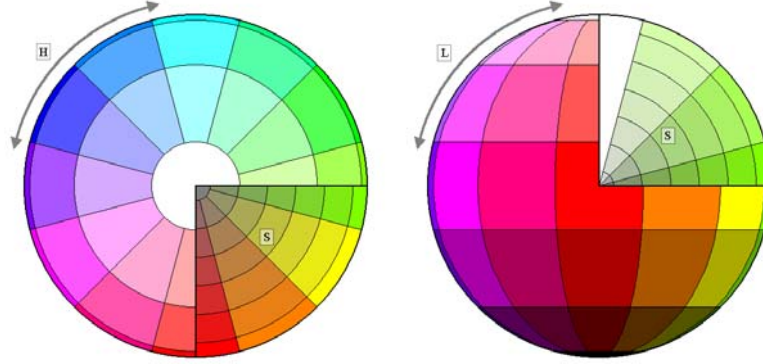
b) MPEG-2 için 4:2:0 örnekleme

Şekil 2.8. MPEG için YCbCr örnekleme

4:2:0 biçimindeki verinin gösterilebilmesi için öncelikle 4:4:4 YCbCr biçimine dönüştürülmesi gerekmektedir.

2.1.5. HSI, HLS ve HSV renk uzayları

HSI ve HSV renk uzayları, insanın sezgisel olarak ve daha kolay renk seçimi yapabilmesi amacıyla geliştirilmişlerdir. Renklerin el ile gösterilmeleri gerektiğinde ve kullanıcıların renkleri görerek seçmeleri gerektiği durumlarda idealdirler. HLS ve HSI birbirine çok benzerdirler. Parlaklık bileşeni L yerine yoğunluk bileşeni I kullanılmıştır. HSI ile HSV arasındaki fark ise parlaklık bileşeninin hesaplanma şekli, I yada V renk doyumuğunun dağılım ve dinamik aralığın değişmesiyle gerçekleşmektedir. Şekil 2.9 HLS renk uzayını göstermektedir.

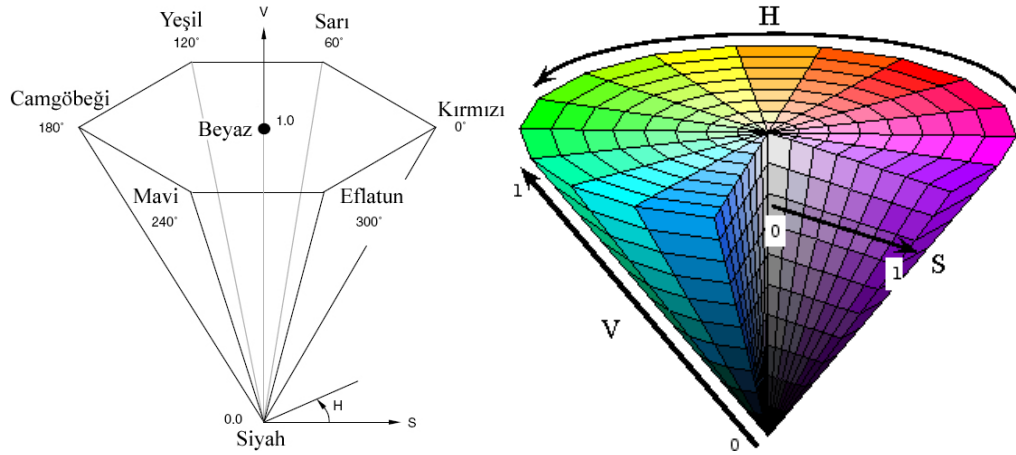


Şekil 2.9. HLS renk uzayı

HSI renk uzayı, R , G , B değerlerine eşit oranda bağlı olan parlaklık değerleri ile doğrudan alakalı katsayı, eşitleme, histogram gibi geleneksel resim işleme metotları için en iyi renk uzayıdır. HSV renk uzayı ise renk doyumu açısından büyük bir dinamik aralığa sahip olduğu için, renkleri değiştirme ya da renk yoğunluğu ayarlama kullanılmaktadır.

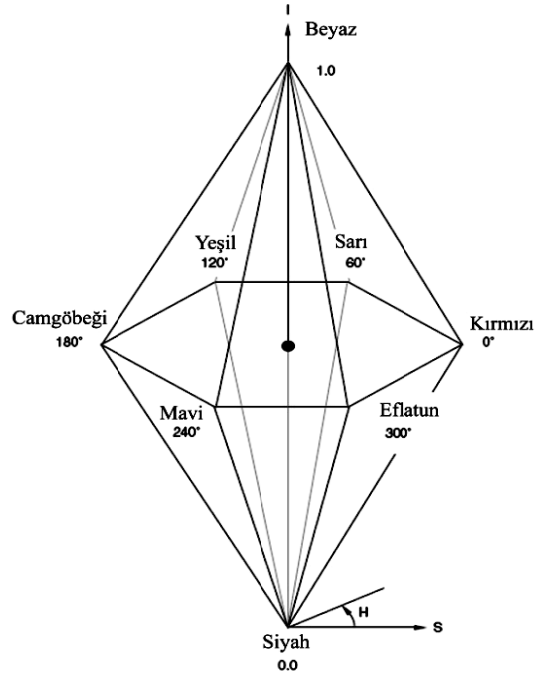
Şekil 2.10, altıgen huni şeklinde HSV renk uzayını göstermektedir. Altıgen huninin en alt kısmı siyah ve $V=0$ 'dır, tepesi ise $V=1$ değerine karşılık gelmektedir. Bu konumda en yoğun renkler elde edilmektedir. Kırmızı 0° olmak üzere tamamlayıcı renkler H 'ye göre 180° karşılıklıdır. S ile gösterilen ve 0 ile 1 arasındaki değere *oran* denilmektedir. $S=0$ iken ve $V=1$ beyaz rengi ve V 'nin diğer değerleri ise grileri göstermektedir. $S=0$ iken H değerinin önemsiz olduğu görülmektedir. $V=1$ ve $S=1$ olduğunda da katıksız renkler görülmektedir. V değerini değiştirmeden S 'i azaltarak

renge beyaz ekleyebilmek, S 'i deðiřtirmeden V 'yi azaltarak renge siyah eklemek mümkündür. Tonlar ise hem S , hem de V 'yi azaltarak elde edilebilmektedir (Jack, 1995).



Şekil 2.10. Altıgen huni şeklinde HSV renk uzayı

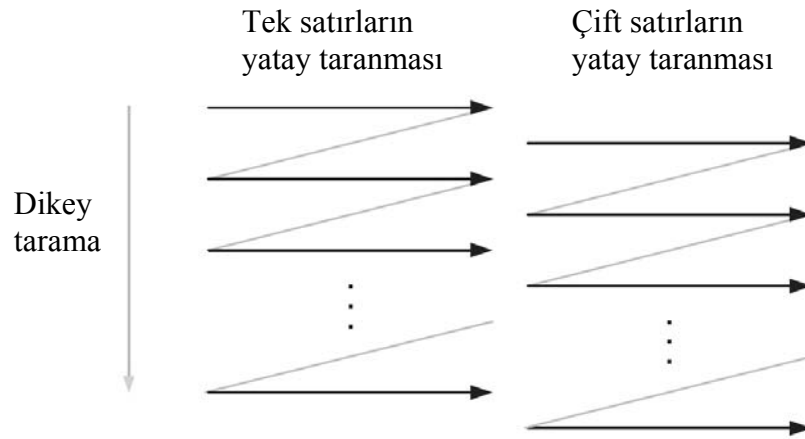
Şekil 2.11 çift altıgen huni şeklinde HSI renk modelini göstermektedir. Altıgen huninin tepesi $I=1$ 'e karşılık gelmektedir ve beyazı göstermektedir. Altıgen huninin tabanı $I=0$ ile gösterilmektedir ve siyah renge karşılık gelmektedir. Birbirini tamamlayan renkler 180° karşılıklıdır ve H ile ifade edilmektedirler. Dikey eksen üzerindeki S değerleri 0 ile 1 arasındadır. Gri seviyeler $S=0$ iken elde edilmektedir. Tonların en yüksek değeri $S=1$ ve $I=0.5$ iken elde edilmektedir.



Şekil 2.11. Çift altıgen huni şeklinde HSI renk modeli

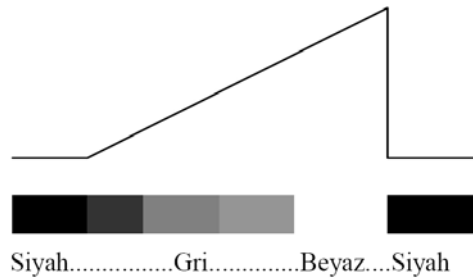
2.2. Video Sinyalleri

Video sinyali, bir görüntünün kamera kullanılarak elektriksel hale dönüştürülmüş halidir. Video sinyali ilk zamanlarda, renksiz olarak ifade edilmiş, daha sonra siyah/beyaz sinyale renk de eklenerek, renkli hale getirilmiştir. Resmi göstermeye yarayan televizyon tüpünde, resim 625 satırın birleştirilmesiyle oluşmaktadır. Tüpte görünebilir resmin oluşturulabilmesi için satırlar tek-teke soldan sağa ve yukarıdan aşağıya taranmaktadır. Tarama ekranın en üst noktasından başlar ve tek satırlar taranarak ekranın en alt noktasında biter. Daha sonra çift satırlar taranarak tam bir resim çerçevesi tamamlanmış olur. Şekil 2.12 video çerçevelerinin taranması işlemini göstermektedir.



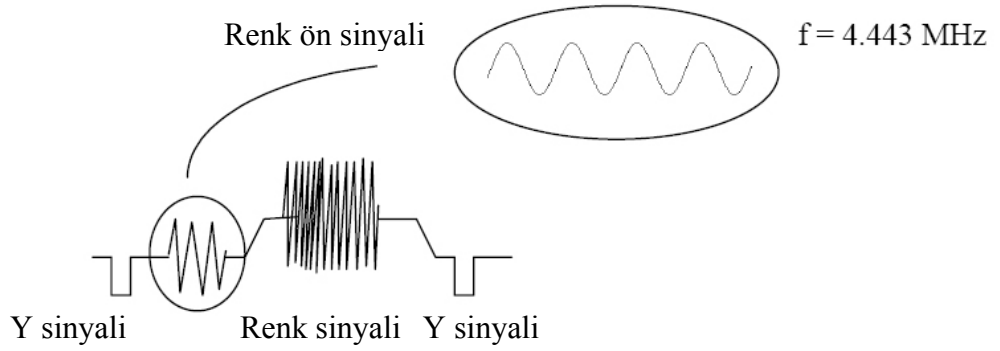
Şekil 2.12. Video çerçevelerinin taraması

Tarama işlemi için analog sinyal kullanılmaktadır. İlk video sinyali siyah-beyaz ve grinin tonlarını tarayabilmektedir. Şekil 2.13 analog siyah-beyaz video sinyal seviyelerini göstermektedir. Bunun dışında video sinyalinin içinde, satır tarama sonuna geldiğini bildiren *yatay senkronizasyon* ve çerçeve sonuna geldiğini bildiren *dikey senkronizasyon* sinyalleri de bulunmaktadır.



Şekil 2.13. Analog siyah-beyaz video sinyali

Renkli görüntü yakalayabilen video kameraların geliştirilmesi ile renkli video sinyali ortaya çıkmıştır. Bu kameralar, renkleri R , G , B bileşenleri kullanarak ifade etmekte idiler. Fakat RGB renk uzayının kullanılması renksiz televizyonları tamamen ortadan kaldıracığından görüntünün YUV renk uzayının kullanılarak aktarılmasına karar verilmiştir. Şekil 2.14'te gösterildiği gibi, analog video sinyaline U ve V bileşenlerinin özel senkronizasyon sinyalleri ile dahil edilmesi sonucunda analog renkli video yayını siyah-beyaz televizyon alıcıları da gösterebilmektedir (Cücioğlu, 2003).

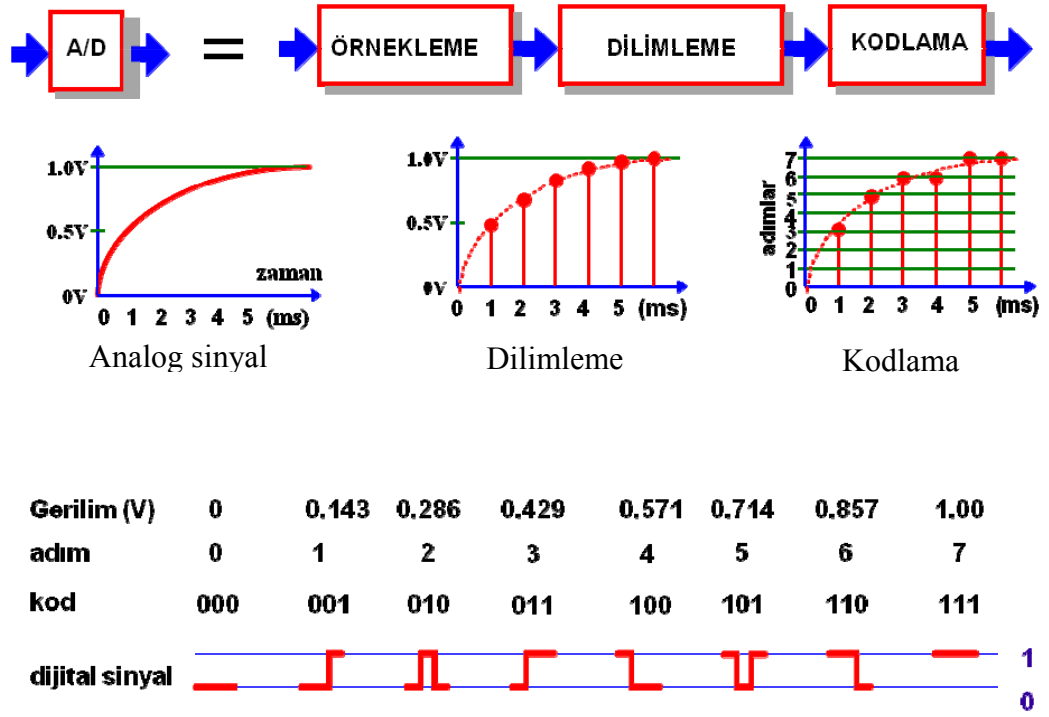


Şekil 2.14. Renkli analog video sinyali

2.3. Sayısal Video

Geçmişte video'nun iletimi ve saklanması için çoğunlukla analog video sinyalleri kullanılmıştır. Analog video sinyali, görüntüleri elektrik akımı gibi sürekli değişen sinyallerden oluştururken, sayısal videoda sadece 0 ve 1'lerden oluşan bit akımı vardır. Analog sinyaller iletim ve depolama esnasında oluşan gürültü ve parazitlere karşı çok duyarlıdır. Bu yüzden orijinal videodan alınan kopyaların görüntü kalitesi düşmektedir. Analog sinyaller sıkıştırılamayacağından, artan yayın sayısına sınırlama getirmektedir.

Günümüzde *sayısal video* adında hızlı bir dönüşüm başlamıştır ve analog yayınların yerini almaktadır. Sayısal video gürültü ve parazitlerden daha az etkilenmekte ve görüntü kalitesi hiç bozulmadan kopyalanabilmektedir. Sıkıştırma işlemine tabi tutulabilen sayısal video sayesinde aynı bant genişliğinden daha fazla yayın iletmek mümkün olmaktadır. Şekil 2.15 analog video sinyalinin sayısallaştırılması aşamalarını göstermektedir.



Şekil 2.15. Analog videonun sayısallaştırılması

BÖLÜM 3

VIDEO SIKIŞTIRMA

Bir video akımı, basit olarak yakın zaman aralıkları ile arka arkaya çekilmiş resimler serisi olarak tanımlanabilir. Analog video verisi tüm bu resim serilerini alıcıya iletmektedir. Geçmişte çoğu video donanımı birincil olarak analog video için tasarlanmıştır. Resim serisinin sayısallaştırılması sonucunda sayısal video ortaya çıkmaktadır. Sayısal video genellikle video düzenleme gibi profesyonel uygulamalarla sınırlandırılmıştır. Sayısallaştırılmış video yüksek kalitede ses ve resim gibi avantajlar sağlamanın yanında, görüntü kalitesini uzun süreler koruyabilmektedir. Tüm pozitif özelliklerine rağmen sayısallaştırılmış video verisi, kapladığı alan bakımından geleneksel veriden farklılık göstermektedir. Sayısal videonun günümüze kadar pahalı olarak nitelendirilmesinin ve son kullanıcıya geç ulaşmasının nedeni kapladığı alandan dolayı iletimdeki ve depolamadaki yüksek maliyettir.

Sayısal videoyu oluşturan her bir resim karesine *çerçeve* denilmektedir. 360*288 boyutundaki bir *çerçeve* 103.680 adet pikselden oluşmaktadır. Her bir piksel için 0–255 aralığında değişen *R*, *G* ve *B* renk bileşenleri 3 byte'lık renk bilgisi ile tanımlanmaktadır. Bu durumda bir video çerçevesi yaklaşık olarak 303 KB (360*288*3), saniyede 25 çerçevenin oluşturduğu 1 saniyelik video ise yaklaşık 7 MB (360*288*3*25) alan kaplamaktadır. Günümüzde yüksek kapasiteli depolama ortamı olarak kullanılan 4,7 GB hacimli bir DVD sıkıştırılmamış olarak sadece 11 dakikalık görüntü saklayabilmektedir.

Sayısallaştırılmış video büyük hacminden dolayı iletimde ve depolamada büyük zorluklar çıkarmaktadır. Sayısallaştırılmış videonun pratikte kullanılabilir olması için sıkıştırılması gerektiği çok açıktır. Bu işlem için en basit düzeyde önerilen ilk yaklaşımlar video verisinin metin verisi gibi sıkıştırılmasıdır. Sayısallaştırılmış videonun metin tipi veriler için tasarlanmış sıkıştırma metotlarıyla sıkıştırılması, düşük kazanç oranlarından dolayı tercih edilmemektedir. Bu hatalı yaklaşım, video verisinin metin tipi geleneksel verilerden son derece farklı olduğunun ve metne dayalı geleneksel algoritmalarının video verisine uygulanmasının fayda getirmeyeceğinin ispatıdır.

Video verisi eşsizdir ve video ile ilgili işlemler için özel algoritmalar kullanılmalıdır. Sahne değişimleri haricinde videoyu oluşturan çerçeveler birbirlerine büyük oranda benzemektedirler. Bir sıkıştırma yöntemi bu benzerliklerin avantajını kullanmak zorundadır. Sıralamadaki diğer çerçevelerdeki benzerlikleri avantaj olarak kullanan sıkıştırma yöntemleri, *ara-çerçeve* tekniği kullanan sıkıştırma yöntemleridir.

Bir sahne değişimi oluştuğunda, ara çerçeve tahmini çalışmayacak ve sıkıştırma modelinin değişmesi gerekecektir. Bir çerçevedeki birbirine yakın piksellerdeki benzerlikleri kullanarak sıkıştırma işlemi gerçekleştirilebilir. Bu tip, tek bir çerçevedeki bilgileri kullanarak sıkıştırma işlemi gerçekleştiren sıkıştırma yöntemleri *iç-çerçeve* teknikleridir.

Son dönemlerde MPEG sıkıştırma yöntemi anahtar teknoloji olarak kullanılmakta ve birçok platformda paralel olarak MPEG çözücüler geliştirilmektedir. MPEG sıkıştırma metodu birbirini izleyen video çerçevelerinde büyük oranda tekrar eden benzerlikleri ve insan gözünün algılayamayacağı düzeydeki detayları yok sayarak, yüksek oranda sıkıştırma sağlayan bir yöntemdir. MPEG video sıkıştırma yöntemi iç-çerçeve ve ara-çerçeve sıkıştırma tekniklerinin her ikisini de kullanmaktadır. Bu yöntem sıkıştırma sonucunda resim kalitesinde kabul edilebilir bir bozulmaya karşılık orijinal sinyalin büyük bir bölümünü attığından kayıplı bir sıkıştırma metodudur.

3.1. MPEG Video Sıkıştırma Yöntemi

Saklama hacmi olarak toplamda daha az bit kullanılması, hareketli resimlerin çok daha hızlı bir şekilde transfer edilmesi anlamına gelmektedir. Böylece pahalı haberleşme hatları ve depolama cihazları, yeni video uygulamalarında daha verimli kullanılmaktadır. MPEG sıkıştırma metodu kullandığı birçok yöntem sayesinde yüksek sıkıştırma oranları yakalamaktadır.

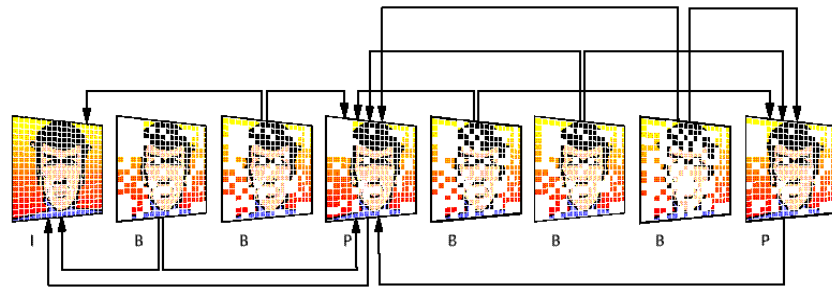
Sayısallaştırılmış video akımını sıkıştırma, hazır çorbaya benzetilebilir. Çorba paketlenirken taşıma ve saklamayı daha etkin yapmak için çorba içindeki tüm su ayrıştırılır, kurutulmuş çorba paketlenerek satılır. Paket müşteriye ulaştığında karışıma su eklenerek çorba tekrardan oluşturulur. MPEG sıkıştırması da ses ve görüntü

akımından gereksiz bilgileri çıkartarak, sinyali orijinal boyutundan daha küçük hale getirmektedir. Akım izleyiciye ulaştığında kod çözücü birim orijinal içeriği tekrardan oluşturup videoyu izlenebilir kılmaktadır. Sıkıştırma sayesinde depolama ve iletimde büyük kolaylıklar sağlanmış ve video dosyalarının kullanım oranları artmıştır.

MPEG sıkıştırma yöntemi kayıplı bir sıkıştırma yöntemidir. Bu yüzden video dosyası sıkıştırıldıktan sonra açıldığında görüntüde fark edilemeyecek düzeyde bir kayıp söz konusudur. MPEG sıkıştırma yöntemi izleyici tarafından fark edilemeyecek alanlarda kaliteyi düşürerek sıkıştırılmış sinyalin kalitesini yüksek tutmaktadır. MPEG sıkıştırma yönteminde birden fazla teknik kullanılarak bir sinyal, resim kalitesinden uzaklaştırılmadan hatırı sayılır biçimde sıkıştırılabilir, ancak bant genişliğini ekonomik kullanmak için daha fazla sıkıştırma gerektiğinde görüntü kalitesi de düşecektir.

MPEG, kayıplı bir sıkıştırma yöntemi olduğundan farklı MPEG sıkıştırıcı birimlerin oluşturduğu akımlar bire bir aynı olmamaktadır. Bu yüzden bazı algoritmalar (stenografi, şifreleme, video işleme gibi) akım kodlandıktan sonra uygulanmalıdır. Aksi takdirde sıkıştırma işlemi sırasında algoritmayı aktif kılan elementler sıkıştırma işlemi sonucunda yok olmaktadır.

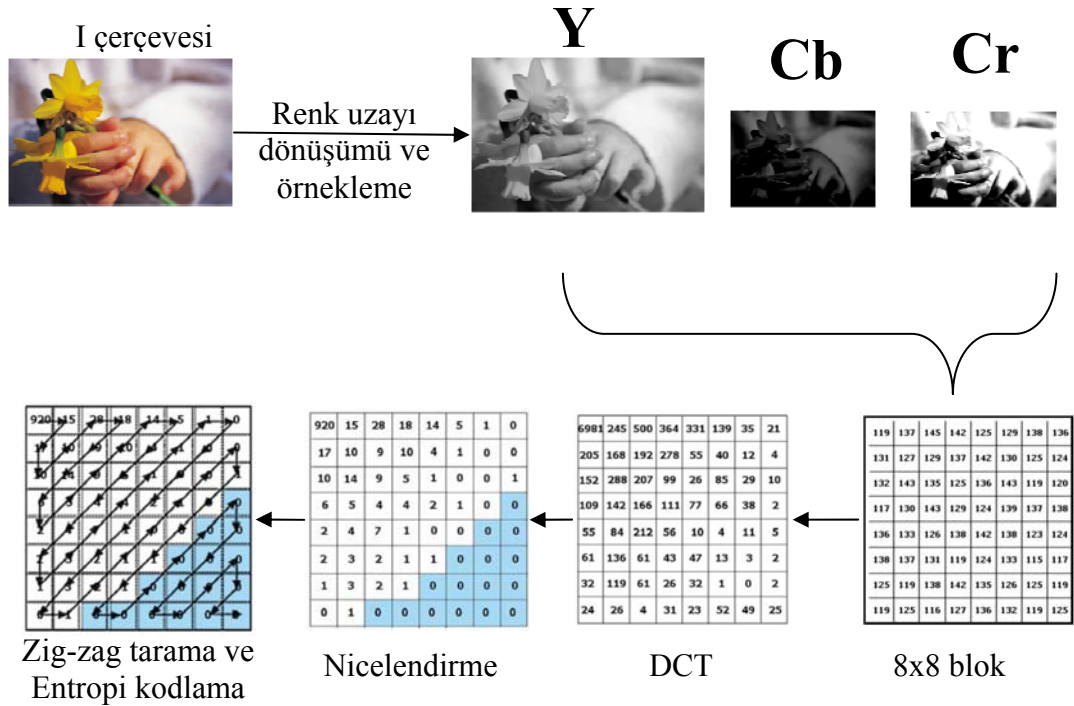
Sıkıştırılmamış video dosyalarının aksine MPEG yöntemi ile sıkıştırılmış video dosyalarında 3 farklı çerçeve tipi vardır. Bu sayede birbirini takip eden çerçeveler arasında az bir görsel fark olması durumunda çerçevenin tamamı dosyaya aktarılmaz. Ara-çerçeve tahmini, ardıl çerçevelerdeki benzerlikleri avantaj olarak kullanmaktadır. Öncelikle tam bir referans çerçeve seçilmekte ve ardından gelen çerçeveler bu referans çerçeve ile olan farklılıklar kodlanmak suretiyle ifade edilmektedir. Referans çerçeveye *iç-kodlanmış çerçeve* ya da *I-çerçevesi* denilmektedir. I-çerçevesi, P ve B tipi çerçeveleri tahmin etmek için kullanılmaktadır. Şekil 3.1 MPEG çerçeve tipleri ve çerçeveler arasındaki ilişkileri göstermektedir.



Şekil 3.1. Mpeg çerçeve tipleri

3.2. I Çerçevesi

I çerçevesi, gösterilebilmesi için başka bir resme ihtiyaç duyulmayan tam bir video resmidir. Bu yüzden en çok veriyi kapsamaktadır. Diğer çerçevelerden bağımsız olduğu için ayrı bir resim gibi düşünülebilir. I çerçevesi bir önceki çerçeve ile çok fazla farklılıkların olduğu durumlarda kullanılmaktadır. Bu çerçeve renk uzayı dönüşümü, örnekleme ve iç-çerçeve sıkıştırma metodu kullanılarak kodlanmaktadır. Şekil 3.2 I çerçevesinin sıkıştırılması sırasında kullanılan yöntemleri göstermektedir.



Şekil 3.2. I çerçevesinin kodlanması

3.2.1. Renk uzayı dönüşümü ve örnekleme

Daha önceki bölümlerde anlatıldığı gibi sayısal video akımlarında, genellikle RGB renk uzayı kullanılmamaktadır. İnsan gözü, bir noktadaki parlaklık değişikliğini

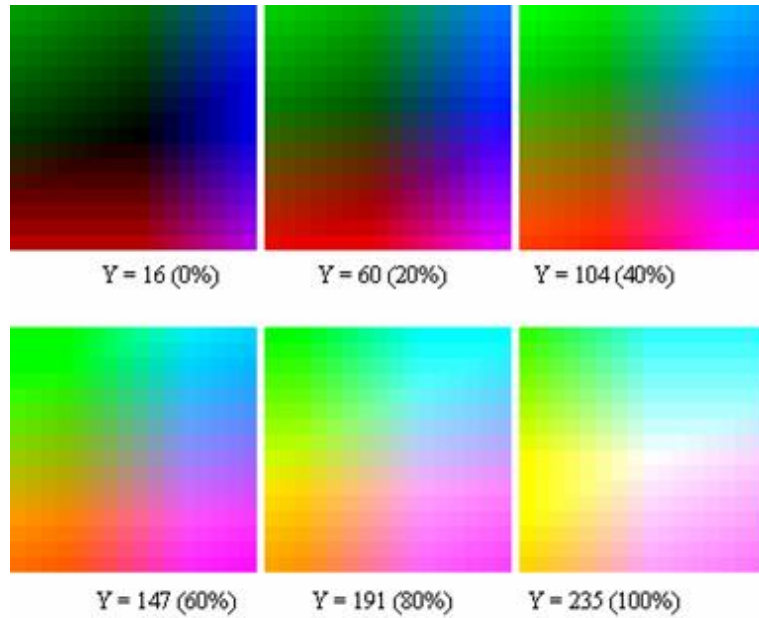
renk deęişikliğine göre daha çok fark etmektedir. MPEG sıkıştırma metodu, RGB renk uzayını YCbCr renk uzayına dönüştürmektedir. Bu dönüştürme,

$$Y \text{ (Parlaklık-Intensity)} = + 0.299R + 0.587G + 0.114B$$

$$Cb \text{ (Mavi/Sarı)} = + 0.492(B - Y) = - 0.147R - 0.289G + 0.436B$$

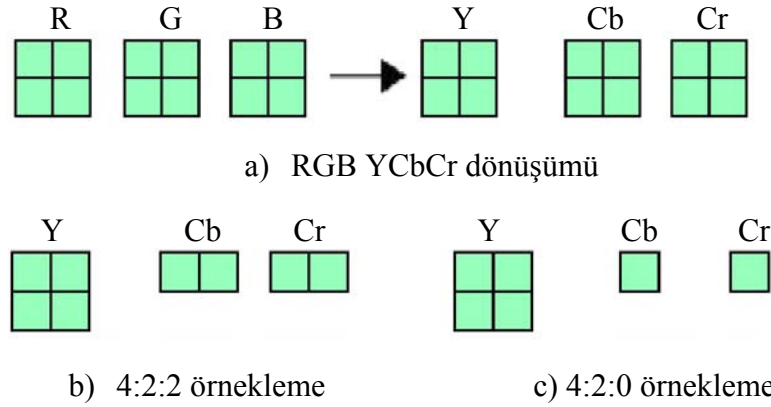
$$Cr \text{ (Kırmızı/Yeşil)} = + 0.877(R - Y) = + 0.615R - 0.515G - 0.100B$$

formülleri ile yapılmaktadır (Jack, 1995). Şekil 3.3 deęişik Y deęerlerine karşılık CbCr tonlarını göstermektedir.



Şekil 3.3. Deęişik Y deęerlerine karşılık CbCr tonları

Örnekleme işleminde, *Cb*, *Cr* ile temsil edilen renkleri daha az yer kaplayacak şekilde daraltılmakta, *Y* ile temsil edilen parlaklık deęerleri ise insan gözünün parlaklık deęişikliklerine olan yüksek hassasiyetinden dolayı deęiştirilmemektedir.



Şekil 3.4. Renk uzayı dönüşümleri ve örnekleme

Renk uzayının dönüşümü ve yeniden örneklendirilmesi, kayıplı bir sıkıştırma sağlamaktadır. Bu sıkıştırma işlemi MPEG video görüntülerinde birbirine yakın piksellerde daha az ton değişikliğinin olmasına ve iç-çerçeve sıkıştırma verimliliğinin artmasına olumlu etki sağlamaktadır. Şekil 3.4 renk uzayı dönüşümü ve örnekleme işlemlerini göstermektedir.

3.2.2. İç-çerçeve sıkıştırma

İç-çerçeve sıkıştırma, video çerçevesindeki düz alanlarda bulunan benzer renklerin oluşturduğu grupları farklı şekilde kodlayarak sıkıştırma sağlamaktadır. Örnek olarak mavi gökyüzü arka planına sahip bir video görüntüsünde, birçok sütundan oluşan benzer mavi pikseller bulunmaktadır. Uzaysal kodlama, bu piksel grubundan sadece bir pikseli ve ardından diğerlerinin birbirine benzer olduklarını belirterek kodlamaktadır. Böylece bit akımından büyük oranda fazlalık veri atılmaktadır.

İç-çerçeve sıkıştırma işlemi

1. Ayrık kosinüs dönüşümü,
2. Nicelendirme,
3. Zig-Zag Tarama,
4. Değişken uzunluklu kodlama

adımlarından oluşmaktadır.

Ayrık kosinüs dönüşümü, videoyu oluşturan çerçeveleri 8x8 bloklara bölmekte, ardından *katsayı* denilen, piksel renk ağırlıklarını frekans düzlemine geçirmektedir. Elde edilen sayılar seçilen kalite oranına göre bir tablo kullanılarak nicelendirilmektedir. Bu işlemden sonra uzaysal ve tekrarlayan artıklardan dolayı birçok katsayı sıfır ya da sıfıra yakın değerlerle sonlanmaktadır. Bunlar katsayı serisinden atılarak bir video çerçevesi çok az sayıda bit ile gösterilmektedir. Sonuçta insan gözünün fark edemeyeceği düzeyde birçok ufak detayı yok eden kayıplı bir sıkıştırma sağlanmaktadır.

3.2.2.a. Ayrık kosinüs dönüşümü

Dönüşüm kodlama, resim ve video işleme uygulamalarının çoğunda temel yöntem olarak kullanılmaktadır. Ayrık kosinüs dönüşümü ile değerler frekans uzayına dönüştürülmektedir. 8x8'lik piksel bloklarına uygulanan ayrık kosinüs dönüşümü (Ahmed v.d. 1974),

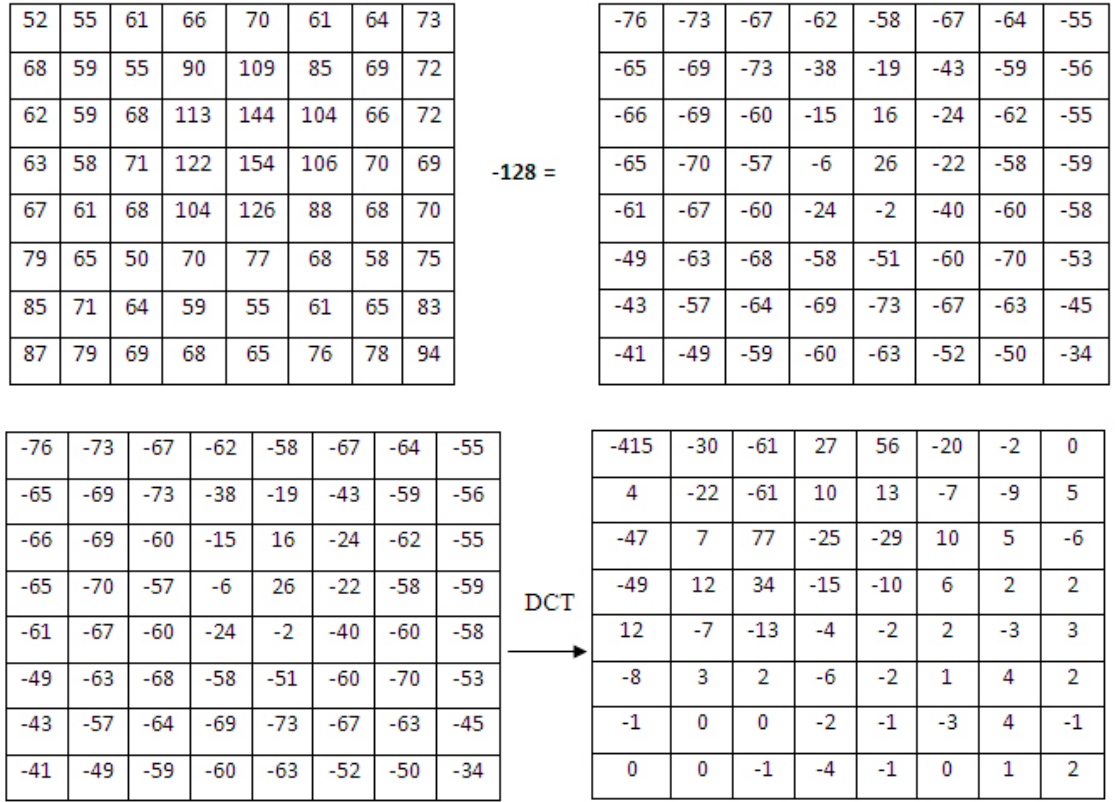
$$D(i, j) = 1 \frac{1}{\sqrt{2N}} C(i)C(j) \sum_{x=0}^{N-1} \sum_{y=0}^{N-1} \text{piksel}(x, y) \cos \left[\frac{(2x+1)i\pi}{2N} \right] \cos \left[\frac{(2x+1)j\pi}{2N} \right]$$

formunda verilmektedir. Burada kullanılan C fonksiyonu

$$C(x) = \begin{cases} \frac{1}{\sqrt{2}} & x = 0 \text{ ise} \\ 1 & x > 0 \text{ ise} \end{cases}$$

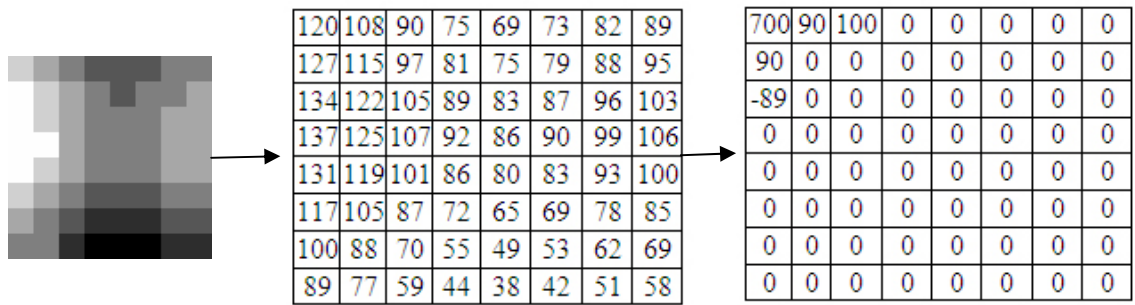
ile tanımlanır.

Ayrık kosinüs dönüşümü için girdi aralığının -128 ile +127 arasında olması gerekmektedir. Bu yüzden ayrık kosinüs dönüşümü yapılmadan önce piksel değerlerinden 128 çıkartılarak ayrık kosinüs dönüşümü yapılmaktadır. Örnek $N \times N$ matris için ayrık kosinüs dönüşümü sonucu şekil 3.5'te gösterilmektedir.



Şekil 3.5. Ayırık kosinüs dönüşümü

Şekil 3.6'daki ayırık kosinüs dönüşümü incelendiğinde, yöntemin sağlamış olduğu yüksek sıkıştırma görülebilmektedir.



Şekil 3.6. Örnek sıkıştırma

3.2.2.b. Nicelendirme

Nicelendirme, DCT işlemi sonucunda çıkan D matrisinin her bir elemanının nicelik matrisi Q ile bölünmesi işlemidir.

$$C(i,j) = \text{yuvarla}\left(\frac{D(i,j)}{Q(i,j)}\right)$$

MPEG sıkıştırma standardına göre 3 farklı tipte resim öngörülmektedir. İç-çerçeve sıkıştırma metoduyla kodlanan I çerçeveleri, iç-nicelik matrisi kullanılarak nicelendirilmektedir. P ve B çerçeveleri ise makro bloğun tipine bağlı olarak iç-nicelik matrisi veya iç-olmayan-nicelik matrisi kullanılarak nicelendirilir. Ayrıca kullanıcıya kendi nicelik matrisini kullanma şansı tanımaktadır (Ding ve Liu, 1995).

8	16	19	22	26	27	29	34
16	16	22	24	27	29	34	37
19	22	26	27	29	34	34	38
22	22	26	27	29	34	37	40
22	26	27	29	32	35	40	48
26	27	29	32	35	40	48	58
26	27	29	34	38	46	56	69
27	29	36	38	46	56	69	83

16	16	16	16	16	16	16	16
16	16	16	16	16	16	16	16
16	16	16	16	16	16	16	16
16	16	16	16	16	16	16	16
16	16	16	16	16	16	16	16
16	16	16	16	16	16	16	16
16	16	16	16	16	16	16	16
16	16	16	16	16	16	16	16

Şekil 3.7. İç-nicelik matrisi ve iç-olmayan-nicelik matrisi

Şekil 3.8'deki örnekte iç-nicelik matrisi kullanarak niceleme işlemi gerçekleştirilecektir. D matrisi sol alt köşesinde düşük sayısal değerlerin bulunduğu ve Q iç-nicelik matrisinin sol alt köşesinde büyük sayısal değerlerin olduğu dikkate alındığında; niceleme işlemi sonucunda C matrisinin sol alt köşesindeki birçok değerın sıfır olduğu görülmektedir.

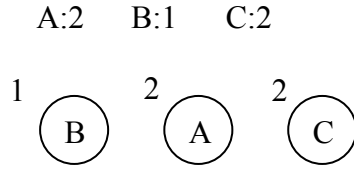
$$\begin{array}{c}
 D \qquad \qquad \qquad Q \\
 \begin{array}{|c|c|c|c|c|c|c|c|} \hline -415 & -30 & -61 & 27 & 56 & -20 & -2 & 0 \\ \hline 4 & -22 & -61 & 10 & 13 & -7 & -9 & 5 \\ \hline -47 & 7 & 77 & -25 & -29 & 10 & 5 & -6 \\ \hline -49 & 12 & 34 & -15 & -10 & 6 & 2 & 2 \\ \hline 12 & -7 & -13 & -4 & -2 & 2 & -3 & 3 \\ \hline -8 & 3 & 2 & -6 & -2 & 1 & 4 & 2 \\ \hline -1 & 0 & 0 & -2 & -1 & -3 & 4 & -1 \\ \hline 0 & 0 & -1 & -4 & -1 & 0 & 1 & 2 \\ \hline \end{array}
 \quad / \quad
 \begin{array}{|c|c|c|c|c|c|c|c|} \hline 8 & 16 & 19 & 22 & 26 & 27 & 29 & 34 \\ \hline 16 & 16 & 22 & 24 & 27 & 29 & 34 & 37 \\ \hline 19 & 22 & 26 & 27 & 29 & 34 & 34 & 38 \\ \hline 22 & 22 & 26 & 27 & 29 & 34 & 37 & 40 \\ \hline 22 & 26 & 27 & 29 & 32 & 35 & 40 & 48 \\ \hline 26 & 27 & 29 & 32 & 35 & 40 & 48 & 58 \\ \hline 26 & 27 & 29 & 34 & 38 & 46 & 56 & 69 \\ \hline 27 & 29 & 36 & 38 & 46 & 56 & 69 & 83 \\ \hline \end{array} \\
 \\
 C \\
 \begin{array}{|c|c|c|c|c|c|c|c|} \hline -52 & -2 & -3 & 1 & 2 & -1 & 0 & 0 \\ \hline 0 & -1 & -3 & 0 & 0 & 0 & 0 & 0 \\ \hline -2 & 0 & 3 & -1 & -1 & 0 & 0 & 0 \\ \hline -2 & 1 & 1 & -1 & 0 & 0 & 0 & 0 \\ \hline 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ \hline 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ \hline 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ \hline 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ \hline \end{array}
 \end{array}$$

Şekil 3.8. Niceleme işlemi

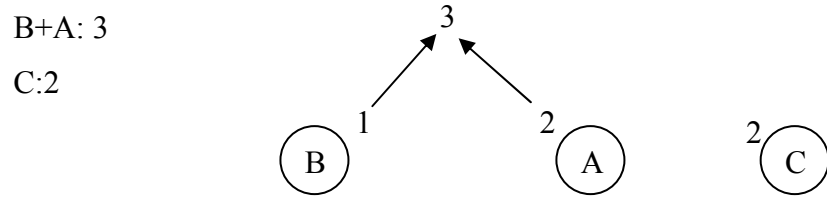
Kullanıcı tanımlı matrisler sıralama başlangıcından hemen sonra ya da nicelik matrisi uzantısında yüklenmektedirler. Video akımında akım sıralama başlangıç kodu bulunduğunda tüm nicelik matrisleri varsayılan olarak ayarlanmaktadır. Q matrisi 8 bit işaretli 64 değerden oluşmakta ve sıfır ile bölme işlemi olamayacağından sıfır değeri içermemektedir (Chun v.d., 1993).

3.2.2.c. Zig-Zag tarama

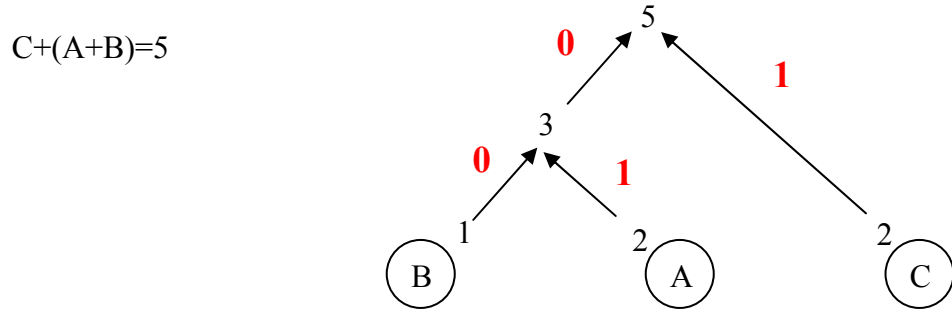
İki boyutlu olan C matrisi zig-zag tarama işlemi ile tek boyutlu bir dizi haline dönüştürülmektedir. Bu tarama ile dizinin son elemanlarının tümünün sıfır olması



şeklindedir. Ardından en küçük iki frekans toplanarak frekans tablosu yeniden düzenlenirse,



durumuna gelir. Bu işlem tek bir ağaç oluşturulana dek tekrarlandığında,



şekli elde edilmektedir. Ağacın dallarını oluşturan rakamlar kullanım sıklıklarını kırmızı rakamlar ise bit kodlarını göstermektedir. Oluşturulan ağaca göre bit haritaları,

B:00 A:01 C:1

gibi oluşmaktadır. Oluşturulan bit haritaları karakterlerin veri içersindeki konumlarına göre yerleştirildiğinde ortaya çıkan bit haritası sıkıştırılmış veri olmaktadır. Bu ise,

$$BAACC = 00\ 01\ 01\ 11 = 17h$$

şeklinde verilmektedir. Normal sabit uzunluklu kodlama ile her bir karakter 1 Byte yer kaplayacağından BAACC verisi toplam 5 Byte yer kaplamaktadır. Oysa veri Huffman sıkıştırma metoduyla sıkıştırıldığında 1 Byte yer kaplamaktadır.

Huffmann algoritması az sayıda karakter çeşidine sahip ve büyük boyutlardaki verilerde çok kullanışlı olmaktadır. Yöntemin en zayıf noktası, oluşturulan ağaçların sıkıştırılmış veriye eklenmesi zorunluluğudur. Ağaç yapısı veriye eklendiğinde bir miktar kayıp oluşmaktadır.

MPEG video sıkıştırma metodu, verinin kodlanması için kodun tamamında değişken uzunlukta kodlama yöntemini kullanmaktadır. Bununla beraber ağaç yapısının sıkıştırılmış veriye eklenmek zorunda kalınması dezavantajını aşmak için Ek-A'da bulunan sabit Huffman tabloları kullanılmaktadır.

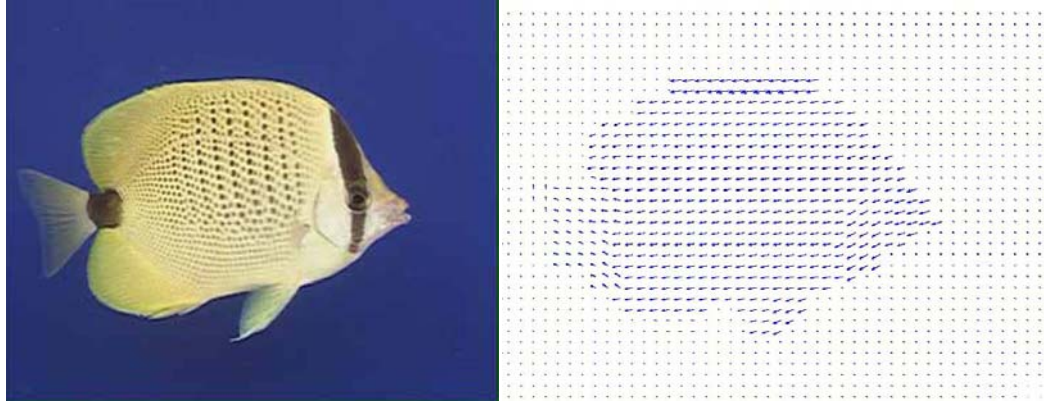
3.3. *P Çerçevesi*

P çerçevesi, bir önceki çerçevedeki farklılıkların tespit edildiği ve aradaki farklılıkların kodlandığı bir çerçevedir. Gösterilebilmesi için bir önceki I çerçevesine ihtiyaç duymaktadır. P çerçevesinde referans belirlemek için, 4 adet 8x8 bloğun birleşmesiyle meydana gelen makro bloklar kullanılmaktadır. Kodlayıcı P çerçevesindeki her bir makro blok için bir önceki P ya da I çerçevesinde arama yaparak uygun bir referans makro blok bulmaya çalışmaktadır. Referans makro blok ile oluşan küçük miktardaki farklılıklar da ayrıca kodlanarak iletilmektedir. Önceki çerçevede uygun bir referans makro blok bulunamaz ise o makro blok, I çerçevesi makro bloğu gibi kodlanmaktadır.

Bu tip sıkıştırmaya *ara-çerçeve sıkıştırması* denmektedir.

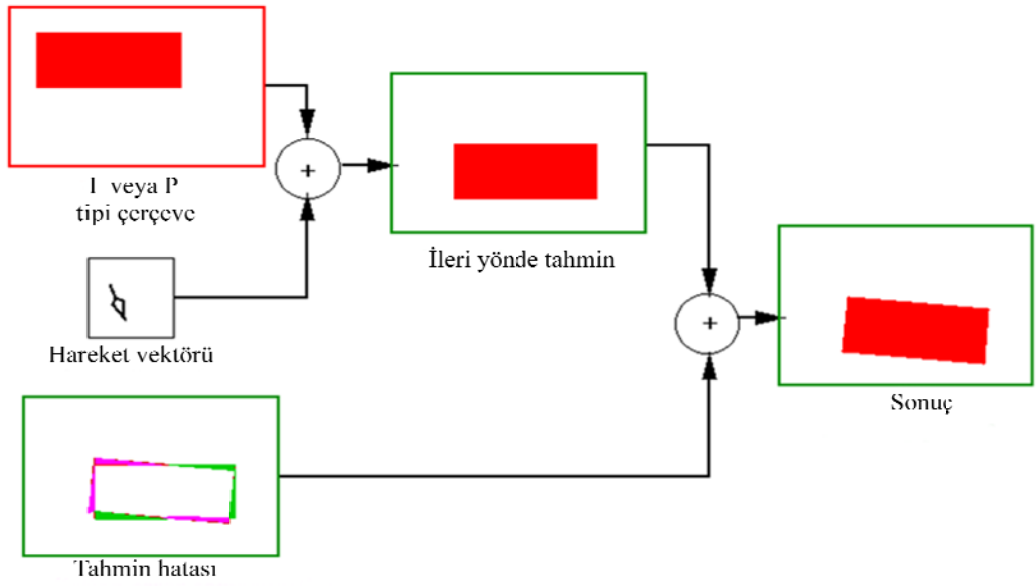
3.3.1. Ara-çerçeve sıkıştırması ve hareket kodlama

Bir hareketli resim dizisindeki iki komşu çerçeve genellikle birbirlerine çok benzerler. Resmin bazı kısımları çerçeveler arasında çok küçük miktarda yer değiştirmektedir. MPEG sıkıştırma metodu her yeni çerçeveyi uygun bir şekilde bölümlere ayırıp, bu bölümlerin nereden geldiğini belirlemek için bir önceki çerçeveyi araştırarak, meydana gelmiş olan zamansal fazlalıkları atmaktadır. Bir çerçevenin içeriğinin çoğu bir önceki çerçevede de bulunuyorsa, o çerçevenin tekrardan gönderilmesi depolama ve aktarım kaybı yaratmaktadır. Bütün çerçeveyi göndermek yerine, bir önceki çerçeve referans alınarak farklılıkların kodlanması akım hacmini düşürmektedir. Şekil 3.10, örnek bir çerçeve ve bu çerçeveye ait hareket vektörlerini göstermektedir.



Şekil 3.10. Örnek çerçeve ve hareket vektörleri

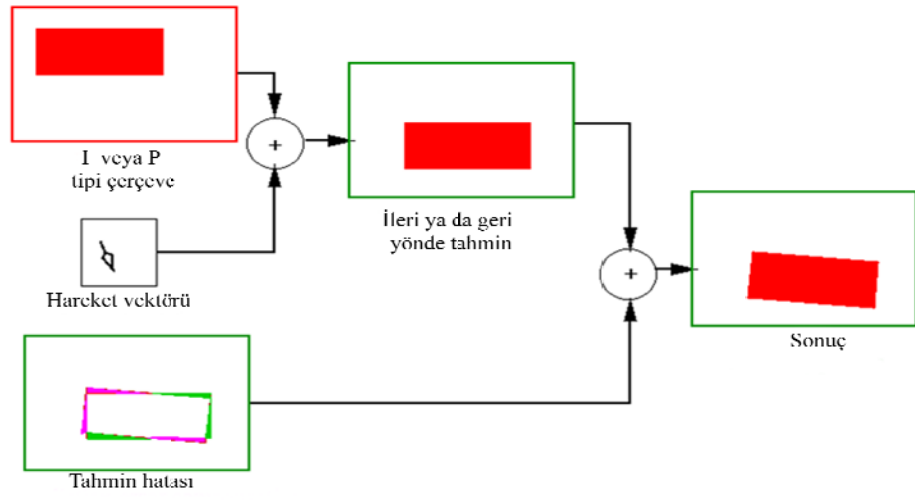
Nesnelerin ekrandaki konumları genellikle değişmekte iken, görünüşleri sabit kalmaktadır. Hareket tahmini bu benzerliğin avantajını, nesnelerin hareketlerini ölçerek kodlanması yoluyla kullanmaktadır. Video akımı çözülürken vektör şeklinde kodlanmış hareket kullanılarak, önceki çerçevelerdeki konumu kaydırılmakta ve takip eden çerçevedeki yeni yerine getirilmektedir. Bu yüzden hareket eden nesneler, sadece bir kez kodlanmakta ve gerektiğinde çerçeveler arasında hareket vektörleri yolu ile ifade edilmektedirler. Şekil 3.11 P çerçevesinin kodlanması aşamalarını göstermektedir.



Şekil 3.11. P çerçevesinin kodlanması

3.4. B Çerçevesi

Önceki çerçevede olmayan bir nesnenin I çerçevesinden sonra birdenbire ortaya çıkması durumunda, çerçevede uygun bir referans bulunamayacağından makro bloğun tamamının kodlanması gerekmekte ve bu sıkıştırma oranını düşürmektedir. Bu yüzden nesnenin var olduğu bir sonraki P veya I çerçevesini referans alan, üçüncü tip B çerçeveleri kullanılmaktadır. B çerçeveleri bir önceki ya da daha sonraki çerçevedeki farklılıkları kodlamaktadır. İleri ya da geri her iki yönde tahmin yapılabileceğinden en uygun tahmin kodlayıcı tarafından seçilmektedir. Şekil 3.12 B çerçevesinin kodlanması aşamalarını göstermektedir.



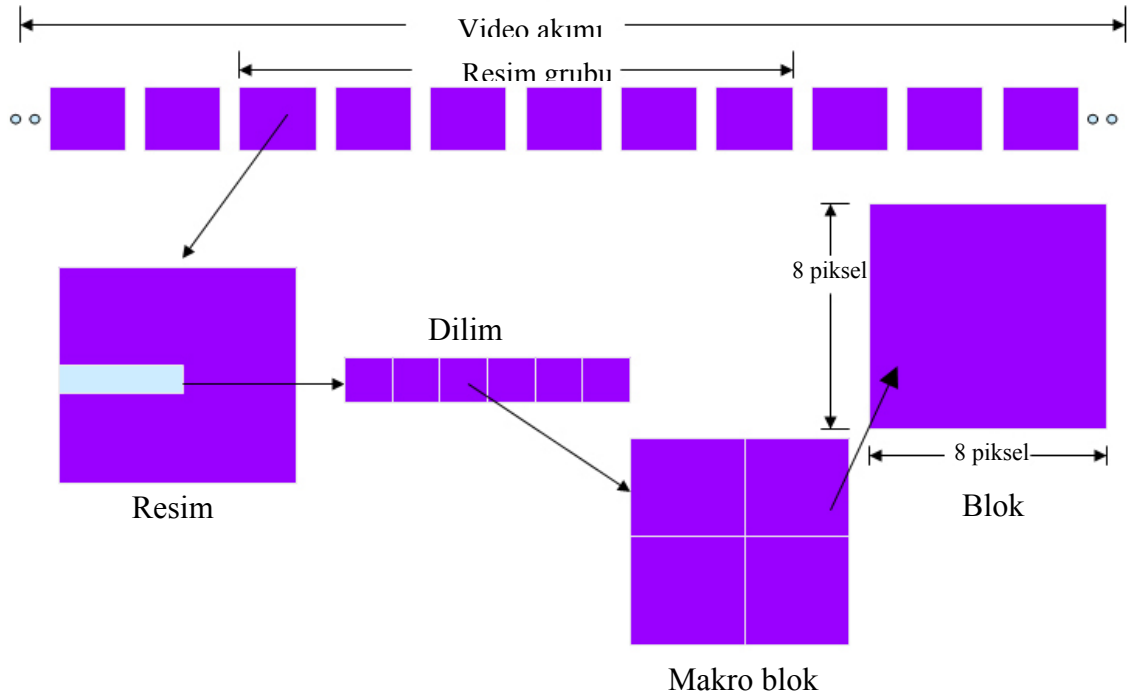
Şekil 3.12. B çerçevesinin kodlanması

BÖLÜM 4

MPEG AKIMININ ÇÖZÜLMESİ

MPEG sıkıştırma yöntemi, etkin bir sıkıştırma yöntemi olması ile birlikte dosya deseni bakımından da esnek bir yapıya sahiptir. Bir video bütününden kopartılan video parçacığı kendi başına izlenebilir, video parçacıkları birleştirilerek daha büyük video parçacıkları oluşturulabilir ve birleştirilmiş video parçalarının izlenebilmesi için ana video bütününe ihtiyaç duyulmaz.

Esnek dosya yapısı, MPEG sıkıştırma yönteminde değişken uzunlukta kodlama kullanılmasından ileri gelmektedir. Değişken uzunlukta kodlama, dosyanın belli bir desene sahip olmasını engellemektedir. Belli bir dosya kalıbı yerine MPEG video akımında, şekil 4.1’de görülen hiyerarşik bir katman yapısı öngörülmektedir (Taşkın v.d., 2007).



Şekil 4.1. MPEG video katman yapısı

Bir video akımının en küçük elementi, 8x8 büyüklüğünde, değişken uzunlukta kodlanmış biçimde piksel bilgilerini içeren bloklardır. 4 adet bloğun birleştirilmesi ile 16x16 büyüklüğünde, içinde hareket vektörlerinin de saklandığı makro bloklar oluşturulmaktadır. Dilim katmanı, makro blokların birleşmesi ile meydana gelmektedir. Dilim katmanının hataların kontrolü açısından önemli bir görevi bulunmaktadır. Eğer kod çözücü birim, bir dilimde hata belirler ise dilimin kalanını çözmeden diğer dilime atlamaktadır. Dilimlerin birleşmesi ile video akımının izleyici tarafından gözlenebilen tek katmanı olan resimler oluşmaktadır. Resimler, kodlayıcı ve kod çözücü tarafından kolay kontrol edilebilmesi amacıyla resim grupları halinde gruplandırılmaktadır. Resim gruplarının birleşmesi video akımını oluşturmaktadır.

4.1. *Başlangıç Kodları*

Belli bir dosya deseni bulunmayan MPEG video akımında, video katmanlarının belirlenmesi için akım içinde benzeri bulunmayan başlangıç kodları kullanılmaktadır. Bütün başlangıç kodları yirmi üç adet 0 ve bir adet 1'den oluşan 3 byte'lık bir ön ek almaktadırlar. Ön ekin ardından gelen byte, farklı başlangıç kodlarının kimliğini belirlemektedir. Mpeg akımında değişken uzunlukta kodlama yapıldığından, başlangıç kodları dışında buna benzer bir dizilime rastlamak mümkün değildir. Çizelge 4.1.'de bazı video başlangıç kodları verilmiştir.

Çizelge 4.1. Başlangıç kodları

Ön Ek 0000 0000 0000 0000 0000 0001	
Başlangıç kodu	Değeri
Resim grubu	1011 1000
Resim	0000 0000
Akım sonu	1011 0111
Akım hatası	1011 0100
Akım başlangıcı	1011 0011
Dilim 1	0000 0001
...	...
Dilim 175	1010 1111

Başlangıç kodları olmadan bir video akımının çözülmesi ve izleyiciye anlamlı görüntüler sunulması, alt katmanlara ayrılmış hiyerarşik MPEG video yapısı yüzünden imkânsızdır. Kod çözücü birim, katmanları blok tabakasına kadar çözmektedir. Kod çözücü birim, katman yapısına uymayan hatalı bir akım ile karşılaştığında o anda yaptığı işlemi kesip kodu çözmeye en başından başlamaktadır.

4.1.1. Akım başlangıç kodu

Bir video akımının çözülebilmesi için ilk olarak akım başlangıç kodunun bulunması gerekmektedir. Akım başlangıç kodu olmayan bir akım geçerli bir MPEG video akımı olarak algılanamaz. Akım başlangıç kodu, belli aralıklar ile tekrarlanmaktadır. Bu tekrarlar sayesinde akım ileri ya da geri sarıldığında, akım çözme işlemi hatasız gerçekleştirilmiş olmaktadır. Sadece tek akım başlangıç kodu olan görüntüler baştan sona izlenebilirler fakat ileri ya da geri alınamazlar.

Akım başlangıç kodu 00000000 00000000 00000001 10110011	Akım Bilgisi	Resim Grubu	Resim Grubu	Resim Grubu
---	---------------------	--------------------	--------------------	--------------------

Şekil 4.2. Akım başlangıç kodu ve akımın devamı

Şekil 4.2’de gösterildiği gibi akım başlangıç kodunun hemen ardından akım ile ilgili detaylı bilgiler gelmektedir.

Çizelge 4.2. Akım başlangıç kodu ve örnek akım ile ilgili bilgiler

Byte No	Bit7	Bit6	Bit5	Bit4	Bit3	Bit2	Bit1	Bit0	Değeri
0	0	0	0	0	0	0	0	0	0
1	0	0	0	0	0	0	0	0	0
2	0	0	0	0	0	0	0	1	1
3	1	0	1	1	0	0	1	1	179 (B3)
Akım başlangıç kodu									
4	0	0	0	1	1	0	0	0	384
5	0	0	0	0					

Yatay boyut									
5					0	0	0	1	288
6	0	0	1	0	0	0	0	0	
Dikey boyut									
7	0	0	1	0					0-0-1-0 = 3:4
Görünüş oranı									
7					0	0	1	1	0-0-1-1 = 25 Fps
Çerçeve oranı									
8	0	0	0	0	0	1	0	1	320 bps
9	0	0	0	0	0	0	0	0	
Bit oranı 4 bit sola kaydırılmıştır.									
10	1								1
İşaret biti her zaman 1'dir									
10		0	0	0	1	1	1	0	112
11	0	0	0						
VBV tampon boyutu									
11				0					
Zorunlu parametre bayrağı 0=Mpeg2 1=Mpeg1									
11					0				0
İç nicelik matrisi yükle? 0=yükleme, 1=yükle									
11						0			0
İç-olmayan nicelik matrisi yükle? 0=yükleme, 1=yükle									

Çizelge 4.2'de ele alınan örnek akımın, 384x288 çözünürlüğünde, 320 bit/s oranına sahip bir MPEG-2 videosu olduğu görülmektedir. Ters ayırık kosinüs dönüşümü için herhangi bir iç-nicelik matrisi içerip içermediği, takip eden bitlerle ifade edilecektir. Akım kodu çözüldükten sonra video akımı hakkında genel bilgiler kod çözücü tarafından belirlenmiş olmaktadır. Akımın çözümü açısından bu bilgiler önemlidir. Çünkü bir daha çerçeve boyutuyla ilgili akım içerisinde herhangi bir bilgi bulunmamaktadır. Kod çözücü birim bu bilgileri dikkatle değerlendirmek zorundadır.

4.1.2. Resim grubu başlangıç kodu

Video akımı başlangıç kodu belirlenerek, akımın karakteristiği hakkında bilgiler elde edilmektedir. Bu başlık kodundan sonra katman yapısına uygun biçimde resim grubu başlangıç kodu bulunmaktadır.

Resim grubu başlangıç kodu 00000000 00000000 00000001 10111000	Grup Bilgisi	Resim	Resim	Resim
---	-----------------	-------	-------	-------

Şekil 4.3. Resim gurubu başlangıç kodu

Şekil 4.3’de gösterildiği gibi resim grubu başlangıç kodunun hemen ardından resim grubu hakkında teknik bilgiler veren bit alanları bulunmaktadır. Çizelge 4.3 resim grubu başlangıcı ve örnek akım ile bilgileri göstermektedir.

Çizelge 4.3. Resim grubu başlangıcı ve örnek akım ile ilgili bilgiler

Byte No	Bit7	Bit6	Bit5	Bit4	Bit3	Bit2	Bit1	Bit0	Değeri
0	0	0	0	0	0	0	0	0	0
1	0	0	0	0	0	0	0	0	0
2	0	0	0	0	0	0	0	1	1
3	1	0	1	1	1	0	0	0	184(B8)
Resim grubu başlangıç kodu									
4	0								0
İşaret biti her zaman 0'dır									
4		0	0	0	0	0			0
Saat bilgisi									
4							0	0	0
5	0	0	0	0					
Dakika bilgisi									
5					1				1
İşaret biti her zaman 1'dir									
5						0	0	0	0
6	0	0	0						
Saniye bilgisi									
6				0	0	0	0	0	0
7	0								
Resim sayımı									
7		1							1
Kapalı resim grubu? 0=Açık 1=Kapalı									
7			0						0
Kırık bağlantı 0=Kırık değil 1=Kırık									
7				0	0	0	0	0	0
Doldurmak İçin fazlalık olarak 5 adet 0									

4.1.3. Resim başlangıç kodu

Resim başlangıç kodu resim grubunun hemen ardından gelmekte ve en çok sıfır değerini içermektedir.

Resim başlangıç kodu 00000000 00000000 00000001 00000000	Resim Bilgisi	Dilim1	Dilim 2	Dilim 3
--	----------------------	---------------	----------------	----------------

Şekil 4.4. Resim başlangıç kodu ve akımın devamı

Şekil 4.4’de gösterildiği gibi resim başlangıç kodunun hemen ardında, geçici referans numarası, çerçeve tipi gibi resim ile ilgili detaylı bilgilerin bulunduğu bir alan gelmektedir. Çizelge 4.4 resim başlangıcı ve örnek akım ile bilgileri göstermektedir.

Çizelge 4.4. Resim başlangıcı ve örnek akım ile ilgili bilgiler

Byte No	Bit7	Bit6	Bit5	Bit4	Bit3	Bit2	Bit1	Bit0	Değeri
0	0	0	0	0	0	0	0	0	0
1	0	0	0	0	0	0	0	0	0
2	0	0	0	0	0	0	0	1	1
3	0	0	0	0	0	0	0	0	0
Resim									
4	0	0	0	0	0	0	0	0	
5	0	0							
Geçici referans numarası									
5			0	0	1				1
Çerçeve tipi 001=I çerçevesi									
5						1	1	1	FFFF
6	1	1	1	1	1	1	1	1	
7	1	1	1	1	1				
Vbv gecikmesi =FFFF değişken bit kodlama (Mpeg2 için geçerli)									
7						0	0	0	0
Ekstra bit alanı =1 olduğu durumda 1 byte ekstra bilgi alanı karşımıza çıkar. Genelde 000 vardır									

Video akımının izlenebilir olması için aşılması gereken sorunlardan biri, MPEG video çerçevelerinin sıralanması işlemidir. MPEG akımında 3 tip çerçeve bulunmakta, B ve P tipi çerçevelerinin gösterilebilmesi için referans çerçevelere ihtiyaç

duyulmaktadır. Şekil 4.5.a'da örnek bir video akımı gösterilmektedir. Bu akımda yer alan 2. çerçeve olan B çerçevesinin gösterilebilmesi için 4. çerçeve olan P çerçevesine ihtiyaç duyulmaktadır. Kod çözücü birimin 2. çerçeveyi göstermesi esnasında 4. çerçeveye ait bilgileri de kullanmaktadır.

Sıra	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
Çerçeve Tipi	I	B	B	P	B	B	P	B	B	I	B	B	P	B	B	P

a) Gösterim sırası

Sıra	1	4	2	3	7	5	6	10	8	9	13	11	12	16	14	15
Çerçeve Tipi	I	P	B	B	P	B	B	I	B	B	P	B	B	P	B	B

b) Akım sırası

Şekil 4.5. Video gösterim ve akım sıraları

Bu sorunun aşılması için MPEG video akımında çerçevelerin gösterim sırası ile akım içindeki sıraları farklı tutulmakta ve kod çözücü birimin gösterim sıralarını tespit edebilmesi için, *geçici referans numarası* adı verilen 10 bitlik bir numara kullanılmaktadır. Kod çözücü birim akımdaki sıralara dikkat etmemekte ve izleyiciye birbirini takip eden referans numaralı resimleri göstermektedir.

Örnek video akımı dikkate alındığında kodu çözülmekte olan çerçevenin geçici referans numarası 0 olan bir I çerçevesi olduğu anlaşılmaktadır.

4.1.4. Dilim başlangıç kodu

Resim çerçevesi, gösterim sırası ve diğer özellikleri kod çözücü tarafından daha önceden belirlendiği halde henüz akım izlenebilir değildir. Kod çözücü birim, katman yapısını takip etmekte ve bir sonraki adım olan dilim başlangıç kodunu belirlemektedir. Şekil 4.6'da gösterildiği gibi dilim başlangıç kodu diğer başlangıç kodlarından farklı olarak 175 farklı seçeneğe sahiptir.

1.Dilim başlangıç kodu 00000000 00000000 00000001 00000001	Dilim Bilgisi	Makroblok 1	Makroblok 2	Makroblok 3
2.Dilim başlangıç kodu 00000000 00000000 00000001 00000010	Dilim Bilgisi	Makroblok 1	Makroblok 2	Makroblok 3
...				
175.Dilim başlangıç kodu 00000000 00000000 00000001 10101111	Dilim Bilgisi	Makroblok 1	Makroblok 2	Makroblok 3

Şekil 4.6. Dilim başlangıç kodları

Dilimlerin başlangıç kodları, resim çerçevesi içerisindeki konumları hakkında kod çözücü birimi bilgilendirmektedir. Her bir dilim resim çerçevesinin bir satırını tamamen kaplamak zorunda değildir. Ayrıca bir resim çerçevesinin oluşturulması için, MPEG sıkıştırma metodunun en fazla 175 adet çerçeveye izin verdiği açıkça görülmektedir. Çizelge 4.5 dilim başlangıcı ve örnek akım ile bilgileri göstermektedir.

Çizelge 4.5. Dilim başlangıcı ve örnek akım ile ilgili bilgiler

0	0	0	0	0	0	0	0	0	0
1	0	0	0	0	0	0	0	0	0
2	0	0	0	0	0	0	0	1	1
3	0	0	0	0	0	0	0	0	1
1 Numaralı dilim. dilim numarasına göre başlık değişiyor									
4	0	1	0	0	1				9
Nicelik Ölçeği									
4						0			
1 byte ilave bilgi alanı 0=Bilgi Yok 1=Bilgi var									

4.1.5. Makro blok ve blok başlangıcı

Makro blokların ve blokların herhangi bir başlangıç kodu bulunmamaktadır. Dilim bilgisinin hemen ardından makro blok ve kodlanmış bit dokusu şeklinde blok bilgisi gelmektedir. Şekil 4.7 makro blok ve takip eden alanları göstermektedir.

Dilim Bilgisi	Makro blok adres artım miktarı	Makro blok tipi	Nicelik ölçeği	Hareket Vektörü	Kodlanmış blok dokusu
---------------	--------------------------------	-----------------	----------------	-----------------	-----------------------

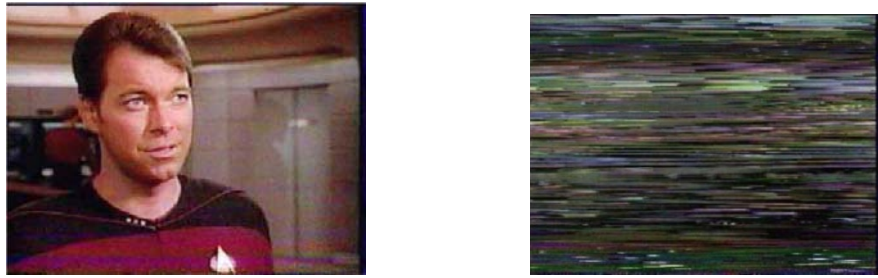
Şekil 4.7. Makro blok

BÖLÜM 5

İÇERİK KORUMA

Bir verinin içeriğinin istenmeyen şahısların eline geçmesini engellemek için anlamsız hale getirilmesi işlemine *içerik koruma* denilmektedir. İçerik koruma işlemi genellikle şifreleme kullanılarak sağlanmaktadır. Şifreleme işlemi ile verinin istenmeyen şahıslar tarafından değerlendirilmesi engellenmektedir. Gelişen teknoloji sonucunda sadece düz metin verileri dışında ses ve görüntü verilerinin de şifrelenmesi ihtiyacı duyulmaktadır. Video güvenliği genel olarak bir ya da daha fazla içerik koruma yöntemi kullanılarak sağlanmaktadır. Ağırlıklı şifrelemeye dayanan bu metotlar hem haberleşmede hem de saldırganlara karşı güvenliği sağlamaktadırlar.

Video verisi başlangıçta analog olarak kaydedilip işlendiğinden, öncü şifreleme metotları da analog sistemde çalışmaktadır. Analog sistemde şifreleme işlemi şekil 5.1’de gösterildiği gibi görsel bozukluğa dayanmaktadır. Görsel bozulmaya dayalı şifreleme sistemleri video verisini şifreledikten sonra, görüntü bozuk olarak gösterildiğinden izlenememektedir. Görsel olarak bozulmuş video verisi izleyiciye ulaştığında görüntüyü çözmeye yarayan özel kod çözücü cihazlar yardımı ile görüntü tekrar izlenebilir hale gelmektedir.



Şekil 5.1. Görsel şifreleme

Gelişen teknoloji ile birlikte, sayısal video ve video işleme gibi işlemler son kullanıcılara kadar ulaşmaktadır. Sayısal video güvenliği standart simetrik anahtarlı şifreleme yöntemleriyle sağlanabilir. Sayısal video ikili bir akım şeklinde ele alınarak

AES-DES gibi bir şifreleme sistemi kullanılmak suretiyle şifrelenebilir. Basit yaklaşım olarak adlandırılan bu yöntem video verisinin gerçek zamanlı olmadığı durumlarda kullanılmaktadır (Furt ve Socek, 2003). Gerçek zamanlılık gibi birçok zorunluluktan dolayı, akmakta olan bir video verisinin şifrelenmesi zor bir işlemdir. Akımın güvenliğini sağlamak DES veya AES gibi şifreleme algoritmaları kullanan bir uygulama kadar basit olmamaktadır. Akımın güvenliğini sağlamak video verisine en uygun şifreleme metodunu belirleme ve dikkatli bir analizi gerektirmektedir.

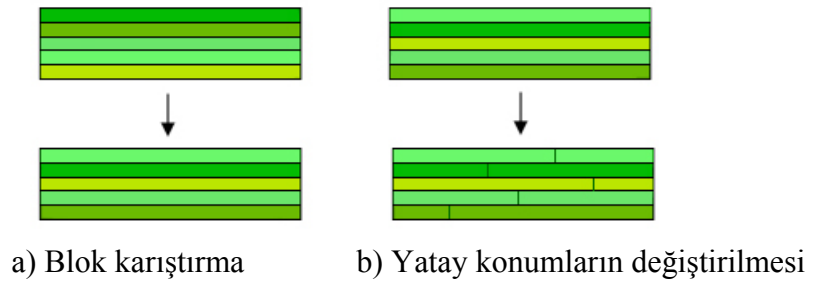
Özetle video verisinin şifrelenmesi için kullanılan yaklaşımlar,

1. Görsel şifreleme,
2. DES, RSA, AES gibi geleneksel şifreleme metotları,
3. Kısmi şifreleme algoritmaları,
4. Düzensiz haritalardır.

Bu yaklaşımlar sırası ile daha detaylı olarak incelenmektedir.

5.1. Görsel Şifreleme

Video verisi miktar olarak çok fazla yer kapladığından güvenliğinin sağlanmasında basit şifreleme metotlarına başvurulmaktadır. Görsel şifrelemenin en iyi örneği, yakın bir zamana kadar yayınlarını üyelerine ücretli olarak sunmak için Nagravizyon sistemini kullanan ulusal bir televizyon kanalı gösterilebilir. Nagra Kudelski tarafından geliştirilen Nagravizyon sistemi analog video verisi üzerinde çalışmaktadır ve PAL televizyon yayınlarında kullanılmaktadır.



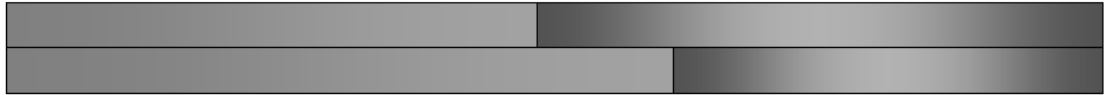
Şekil 5.2. Nagravizyon şifreleme aşamaları

Nagravizyon şifreleme metodu görüntüyü satırlara ayırmakta ve yerlerini bloklar halinde karıştırmaktadır. Bu karıştırma işlemi video görüntüsünü oluşturan her bir kareye aynı şekilde uygulanmaktadır. Şekil 5.2 Nagravizyon şifreleme aşamalarını göstermektedir.

Şifreyi kırmak isteyen saldırgan blok karıştırma sırasını bir kez çözdüğü takdirde, bu sıra hiç değişmediğinden, sistemi kolayca etkisiz hale getirebilmektedir. Bu yüzden Nagravizyon şifreleme sistemi ikinci bir şifreleme aşaması içermektedir. İzleyiciye üyelik sistemi tarafından sağlanan akıllı kart üzerinde bulunan ikinci bir şifreleme algoritması, blokların yatay konumlarını 256 farklı kesim noktasından birisini kullanarak değiştirmektedir. Saldırgan için tamamen rastlantısal sayılabilecek olan bu kesim noktaları akıllı kart olmadan belirlenememektedir.

Bu şifreleme sistemi günümüzde uygun şifre çözücü cihaz ve akıllı kart kullanılmadan yazılım ile gerçek zamanlı kırılabilir. Çok fazla karmaşıklık içermeyen şifreleme sistemi yine 2 adımda kırılmaktadır. Sistemin en zayıf olduğu nokta, yerleri değiştirilen blokların yer değiştirilme sırasının sabit olmasıdır. Bu sabit dizilim deneme yoluyla belirlenmektedir.

Fakat sistemin ikinci adımında gerçekleştirilen blokların kendi arasında yatay konumlarının kesilerek değiştirilmesi akıllı kart tarafından gerçekleştirilmektedir. Saldırgan, elinde akıllı kart olmadan 256 farklı değerden birisini tespit etmek için bloğun parlaklık değerlerini bir üst bloğun parlaklık değerleriyle karşılaştırmaktadır. Birbirine çok yakın parlaklık değerleri elde edildiğinde blokların yatay konumları kolaylıkla belirlenmektedir. Şekil 5.3 blokların örnek parlaklık değerlerini göstermektedir.



Şekil 5.3. Örnek blok parlaklık değerleri

Nagravizyon şifreleme sistemi, görsel bozulmaya dayanan ve çıktığı yıllarda son derece güvenli sayılan fakat son yıllarda resim işleme metotları kullanılarak anahtar bilgisi olmadan kırılabilen bir şifreleme sistemi olarak anılmaktadır (Markus, 1998).

5.2. Geleneksel Şifreleme

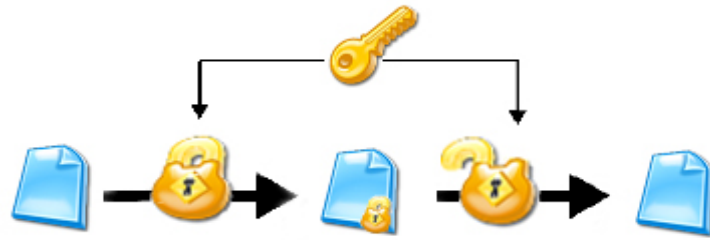
Şifreleme, matematik kullanarak veriyi gizleme ve çözme bilimidir. Şifreleme, değeri yüksek bilgiyi saklama ve güvensiz yollarda iletimi sırasında istenilen kişi dışında başka kişiler tarafından okunmasını engellemektedir. Herhangi bir yöntem kullanılmadan doğrudan okunabilen metne *açık metin*, açık metnin içeriğini gizleme yöntemine *şifreleme* denilmektedir. Açık metnin anlamsız ve okunamayacak haline *şifrelenmiş metin* denmektedir. Açık metin şifrelenerek, istenilen kişi dışında birisi tarafından okunamaz hale getirilmektedir. Şifreli metinden, orijinal açık metne dönüştürme işlemine *şifre çözme* denilmektedir. Şekil 5.4, bu işlem basamaklarını göstermektedir.



Açık metin Şifreleme Şifreli metin Şifre çözme Açık metin

Şekil 5.4. Geleneksel şifreleme

Şifreleme algoritmaları, simetrik ve asimetrik olmak üzere iki ana kategoriye ayrılmaktadır. *Simetrik şifreleme algoritmaları*, şifreleme ve çözme işlemleri için bir tek anahtar kullanmaktadır. Geniş bir kullanım alanına sahip DES şifreleme algoritması simetrik şifreleme algoritmalarına örnek olarak gösterilebilir. Şekil 5.5 simetrik şifreleme algoritmalarının nasıl çalıştığını göstermektedir.



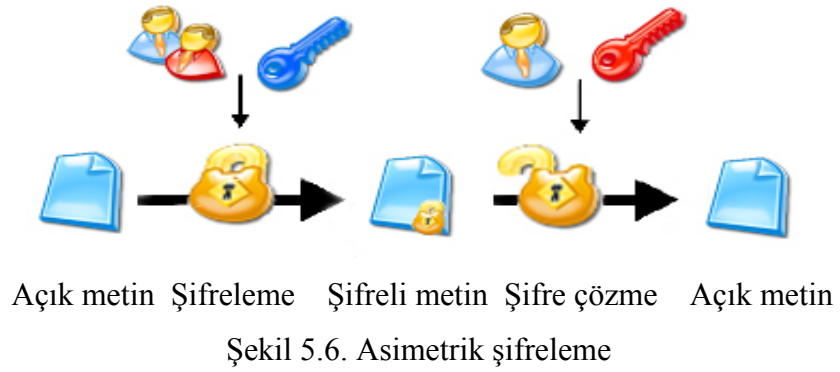
Açık metin Şifreleme Şifreli metin Şifre çözme Açık metin

Şekil 5.5. Simetrik şifreleme

Sayısal video akımını oluşturan bitler DES şifreleme algoritması kullanılarak metin gibi şifrelendiğinde bu yaklaşımın üç önemli açığı bulunmaktadır.

1. Görüntü bitlerinin dağılımları rastlantısal değildir ve genellikle birbirine yakın bitler birbirinin aynısıdır. Bu şifreyi kırmak isteyen saldırgana açık noktalar bırakmaktadır
2. DES şifreleme algoritmasının çıktısı rastlantısaldır. Bu yüzden şifreleme sonucunda oluşan şifrelenmiş görüntüye sıkıştırma işlemi yapılamaz.
3. DES şifreleme algoritması gerçek zamanlı video akımını şifrelemek için yeterince hafif bir şifreleme algoritması değildir.

Asimetrik şifreleme algoritmaları ise, simetrik şifreleme algoritmalarından farklı olarak bir yerine iki anahtar kullanılmaktadır. Açık metin, açık anahtar denilen anahtar kullanılarak şifrelenmektedir. Alıcı, şifreli metni gizli anahtar kullanarak çözmektedir. Açık anahtarın korunmasına gerek kalmadan gizli anahtar korunarak güvenlik sağlanmaktadır. Açık anahtara sahip herhangi bir kişi, gizli anahtarı olan kişinin okuyabileceği metinler üretmekten öteye gidemez. Şifreli metinden açık metne dönüşüm işlemi sadece gizli anahtara sahip olan kişi tarafından gerçekleştirilmektedir. RSA şifreleme algoritması, asimetrik şifreleme algoritmalarına örnek olarak gösterilebilir



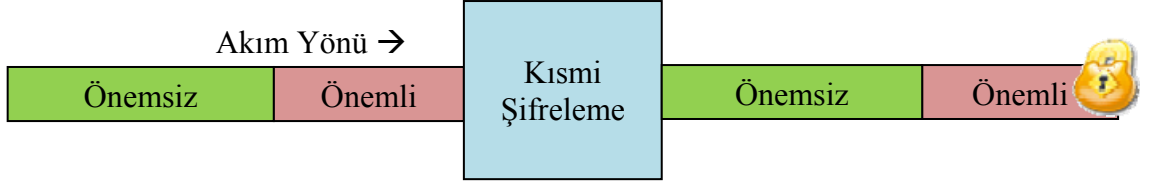
Sayısal video akımını oluşturan bitler RSA şifreleme algoritması kullanılarak metin gibi şifrelendiğinde bu yaklaşımın dört önemli açığı bulunmaktadır.

1. Görüntü bitlerinin dağılımları rastlantısal değildir ve genellikle birbirine yakın bitler birbirinin aynısıdır. Bu şifreyi kırmak isteyen saldırgana açık noktalar bırakmaktadır
2. RSA şifreleme algoritmasının çıktısı rastlantısaldır. Bu yüzden şifreleme sonucunda oluşan şifrelenmiş görüntüye, sıkıştırma işlemi yapılamaz.
3. RSA şifreleme algoritması gerçek zamanlı video akımını şifrelemek için yeterince hafif bir şifreleme algoritması değildir.
4. RSA şifreleme algoritması gücünü büyük anahtar değerinden alır. Anahtar değeri ne kadar büyük olursa güvenlik o derece artmaktadır. Fakat büyük anahtar değeri seçildiğinde şifreli dosya o derece büyümektedir.

5.3. *Kısmi Şifreleme*

Günümüz araştırmaları, var olan şifreleme algoritmalarının video verisinin gerçek zamanlılık ihtiyaçlarını karşılayacak şekilde yeniden düzenlenmesi ya da yeni şifreleme algoritmaları geliştirilmesini hedef almaktadır. Bu araştırmalardan büyük bir kısmı, veri biçimine has özellikleri kullanarak güvenliği sağlamaya dayalıdır. Bu tip yaklaşımlara *kısmi şifreleme* denilmektedir. Kısmi şifreleme, veri bütünü bir kısmını işleyerek veri bütünüün tamamının güvende olmasını sağlamaktadır. Kısmi şifrelemede boyut olarak küçük fakat akımın izlenebilirliği için önemli olan parçalar şifrelenmekte, geriye kalan büyük kısım ise şifrelenmemektedir. Şekil 5.7 kısmi şifreleme algoritmalarının temel çalışma mantığını göstermektedir.

Sayısal video boyut olarak çok yer kapladığından kısmi şifreleme algoritmaları sıkıştırılmış video dosyalarına uygulanmaktadır. Sıkıştırılmış video en düşük düzeyde veri tekrarı içermekte ve akımdaki ufak bozukluklardan büyük tahribat görmektedir.



Şekil 5.7. Kısmi şifreleme

5.4. Düzensiz Haritalar Kullanarak Şifreleme

Düzensizlik ve şifreleme arasındaki yakın ilişkiden dolayı düzensiz haritalar kullanılarak şifreleme sistemleri geliştirilmiştir. Genel olarak 2 boyutlu düzensiz haritalar kullanılarak sayısal resim ve video üzerinde gizli permütasyonlar oluşturulmaktadır. Düzensiz haritalar kullanılarak şifreleme işlemi sonucunda genellikle gürültüye benzer resimler elde edilmektedir.

Düzensiz haritalar kullanarak şifreleme işlemi

1. $M \times N$ boyutunda 2 boyutlu bir düzensiz harita belirleme,
2. 2 boyutlu düzensiz harita resmin tümünü kaplayacak şekilde itere etme,
3. Bir yerine koyma algoritması (şifreleyici) kullanarak, tüm piksel değerlerini resim histogramını bozacak şekilde değiştirme,
4. Permütasyon ve yerine koyma algoritmaları k kez tekrarlayarak şifreli resim elde etme

basamaklarından oluşmaktadır.

Saldırılardan korunmak açısından yerine koyma algoritması içeriğe uygun seçilmeli ve küçük değişiklikler yapmalıdır. Düzensiz haritalara örnek olarak,

$$B(x, y) = \begin{cases} \left(2x, \frac{y}{2}\right) & 0 \leq x < 1/2 \\ \left(2x - 1, \frac{y}{2} + \frac{1}{2}\right) & 1/2 \leq x < 1 \end{cases}$$

formunda gösterilen Baker haritası verilebilir (Furth ve Socek, 2003).

BÖLÜM 6

VIDEO ŞİFRELEME KONUSUNDA DAHA ÖNCE YAPILMIŞ ÇALIŞMALAR

Görüntü dosyaların şifrelenmesi ile ilgili yapılan yurt içi ve yurt dışı çalışmalar incelenerek aşağıda sunulmaktadır.

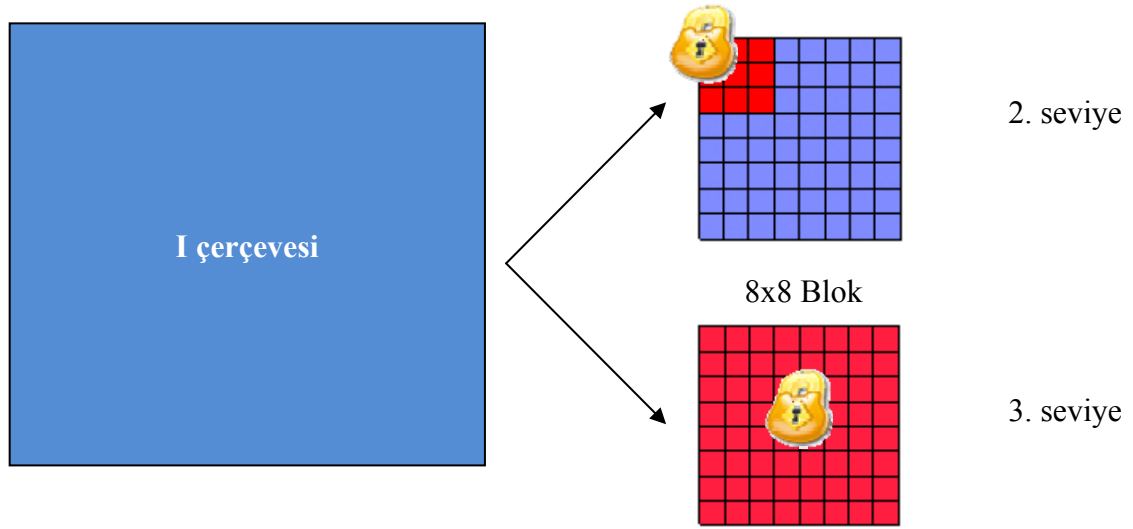
6.1. *SECMPEG*

1995 yılında Meyer ve Gadegast MPEG video standardı için SECMPEG adında kısmi bir şifreleme metodu geliştirmişlerdir. SECMPEG, 4 farklı güvenlik seviyesi sunmaktadır. Birinci seviyede SECMPEG sıralama tabakasından dilim tabakasına kadar tüm başlıkları şifrelemektedir. DCT bloklarını ve hareket vektörlerini ise şifrelememektedir. Şekil 6.1 SECMPEG video şifreleme metodunun birinci seviyesinde şifrelediği alanları göstermektedir (Meyer ve Gadegast, 1995).

Akım başlangıç kodu 00000000 00000000 00000001 10110011	Akım Bilgisi	
Resim grubu başlangıç kodu 00000000 00000000 00000001 10111000	Grup Bilgisi	
Resim başlangıç kodu 00000000 00000000 00000001 00000000	Resim Bilgisi	
1.Dilim başlangıç kodu 00000000 00000000 00000001 00000001	Dilim Bilgisi	

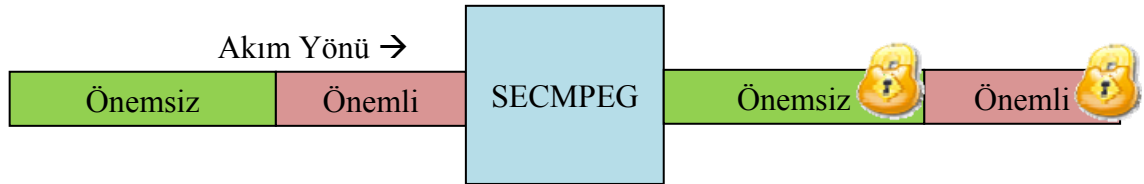
Şekil 6.1. SECMPEG video şifreleme metodu birinci seviye

İkinci seviyede I çerçevesine ait en önemli parçalar birinci seviye ilave olarak şifrelenmektedir. Üçüncü seviyede ise I çerçevesine ait tüm bloklar da şifrelenmektedir. Şekil 6.2 SECMPEG video şifreleme metodunun ikinci ve üçüncü seviyelerini göstermektedir.



Şekil 6.2. SECMPEG video şifreleme metodu ikinci ve üçüncü seviye

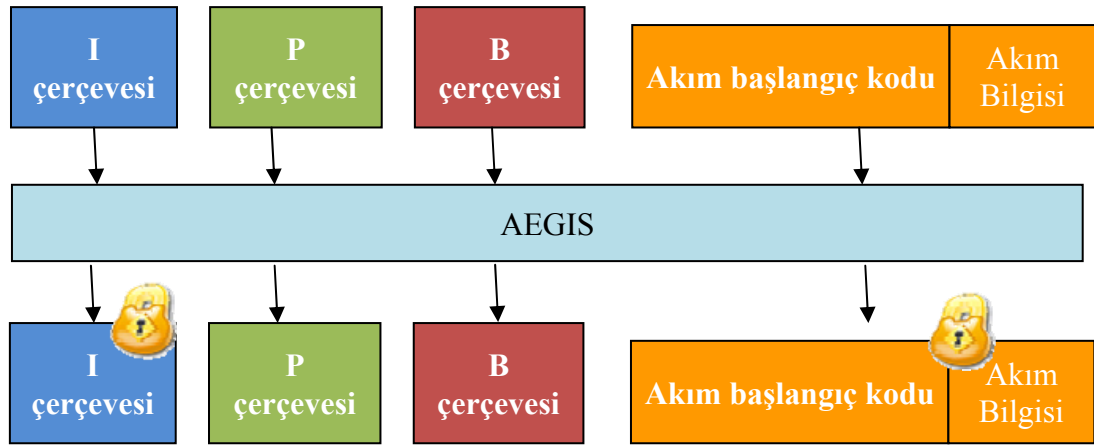
Son olarak dördüncü seviyede ise MPEG akımının tamamı şifrelenmektedir. Yazarlar, yoğun bir kullanıma sahip olduğundan şifreleme işlemi için DES simetrik şifreleme algoritmasını kullanmışlardır. Şekil 6.3 SECMPEG video şifreleme metodunun dördüncü seviyesini göstermektedir. Bu yaklaşım sadece depolama güvenliğini sağlamakta, gerçek zamanlı görüntülerde kullanılmamaktadır.



Şekil 6.3. SECMPEG video şifreleme metodu dördüncü seviye

6.2. AEGIS

MPEG video akımının kısmi şifrelenmesi temeline dayanan AEGIS, 1995 yılında Maples ve Spanos tarafından geliştirilmiştir. AEGIS, MPEG video akımı için özel olarak tasarlanmıştır. Bu şifreleme metodu tüm MPEG grupları içinden I çerçevelerini şifrelemekte, B ve P çerçevelerini ise olduğu gibi bırakmaktadır (Maples ve Spanos, 1995).



Şekil 6.4. AEGIS şifreleme metodu

AEGIS'e ek olarak resim boyutu, çerçeve oranı, bit oranı, tampon boyutu gibi birçok bilgiyi içeren video akımı başlangıç kodunu da şifrelemektedir. Şekil 6.4 AEGIS şifreleme metodunu göstermektedir. Sonuç olarak şifreli MPEG akımı, kod çözücü birim tarafından izlenebilir hale getirilememektedir. AEGIS'in tüm bunların arkasında kullandığı şifreleme metodu DES'tir. AEGIS, SECMPPEG'in üçüncü seviye güvenliğine benzer bir yaklaşımdır ve doğal olarak SECMPPEG'in dezavantajlarını da almaktadır.

6.3. Zig-Zag Permütasyon Algoritması

Tang'e ait zig-zag permütasyon algoritması şifreleme işlemini, video akımı sıkıştırılırken gerçekleştirmektedir. MPEG sıkıştırması sırasında nicelendirilmiş 8x8

Şifreli metin saldırısında ise 8x8 boyutundaki blokların sabit olan dağılım yoğunlukları kullanılmaktadır. DCT katsayıları içeren matrisin sol üst köşesi sıfırdan farklı elemanlar, sağ alt köşesi ise sıfır olan elemanlar içermektedir. Birden fazla şifreli blok incelendiğinde permütasyon listesi yine elde edilebilmektedir.

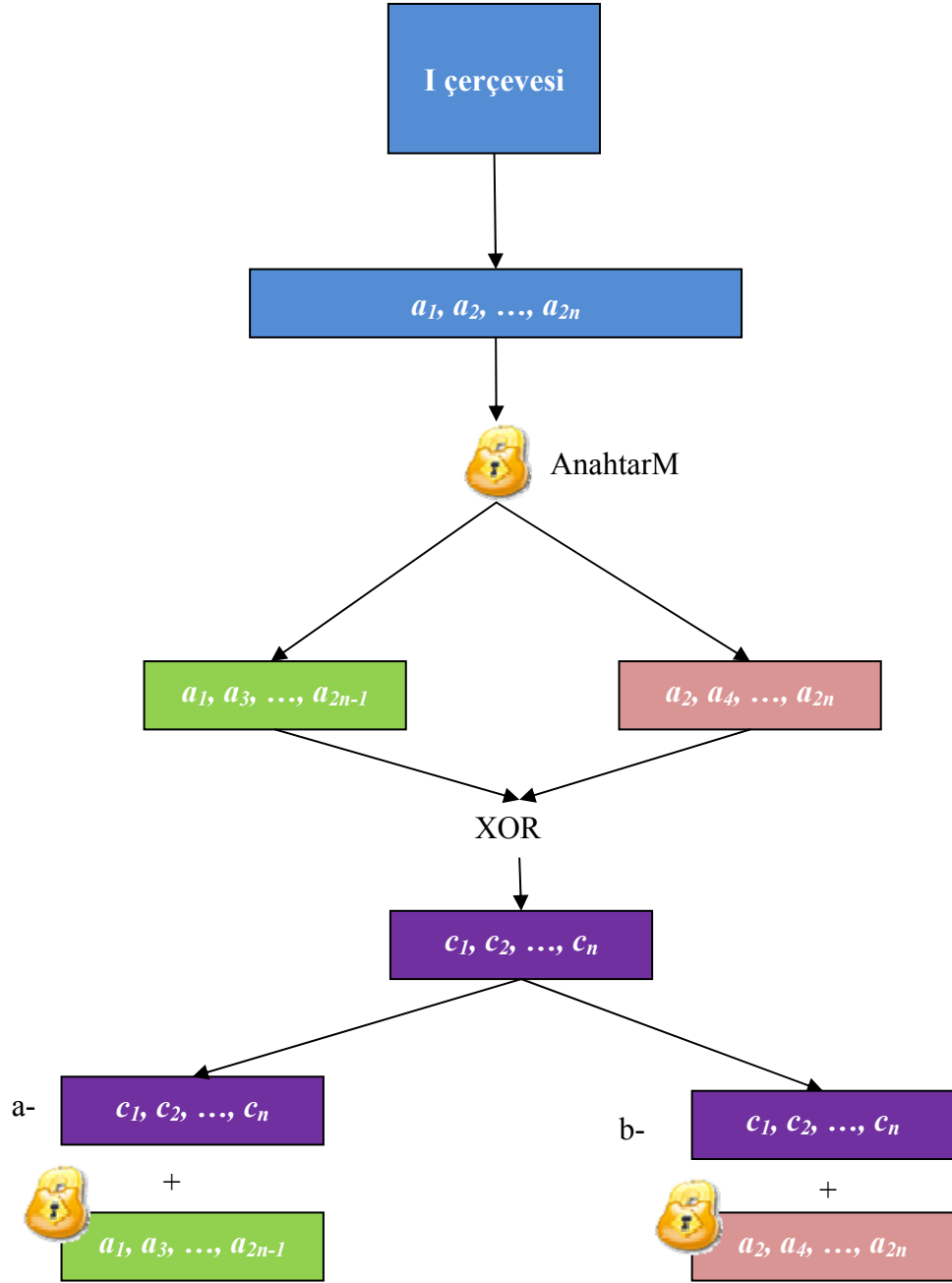
MPEG sıkıştırma yönteminin sıkıştırma oranının yüksek olmasında büyük rol oynayan zig-zag tarama stiline bozulması, şifrelenmiş akımın büyüklüğünü arttırmaktadır. Saldırgan, düşük sıkıştırma oranına sahip şifrelenmiş bir akımı belirlediğinde, şifreleme sistemi hakkında da yorum yapma şansına sahip olmaktadır.

6.4. VEA Video Şifreleme Algoritması

Vea video şifreleme algoritması 4 adımdan oluşan MPEG video akımını şifrelemeye yönelik bir yaklaşımdır.

1. $a_1, a_2, a_3, \dots, a_{2n}$ $2n$ uzunluğunda bir byte akımını göstermek üzere bir I çerçevesinin büyük bir kısmını oluştursun
2. Çift ve tek olmak üzere $(a_1, a_3, a_5, \dots, a_{2n-1})$ ve $(a_2, a_4, a_6, \dots, a_{2n})$ listeleri oluşturulsun
3. İki liste, XOR işlemine tabi tutularak n byte uzunluğunda üçüncü bir $(c_1, c_2, c_3, \dots, c_n)$ listesine aktarılsın
4. Belli bir şifreleme sistemi E 'yi kullanarak, *AnahtarE* anahtarı kullanılmak suretiyle tek ya da çift listelerden birisi şifrelensin. Bu durumda şifreli metinler $c_1, c_2, \dots, c_n E.AnahtarE(a_1, a_3, a_5, \dots, a_{2n-1})$ yada $c_1, c_2, \dots, c_n E.AnahtarE(a_2, a_4, \dots, a_{2n})$ olacaktır.

Görüldüğü gibi *AnahtarE* anahtarına sahip bir kişi şifrelenmiş listeyi açıp c dizisi ile XOR işlemine tabi tutarak listenin kalan kısmını da kolayca elde edebilmektedir (Qiao ve Nahrstedt, 1997).



Şekil 6.7. Video şifreleme algoritması (VEA) ikinci yaklaşım

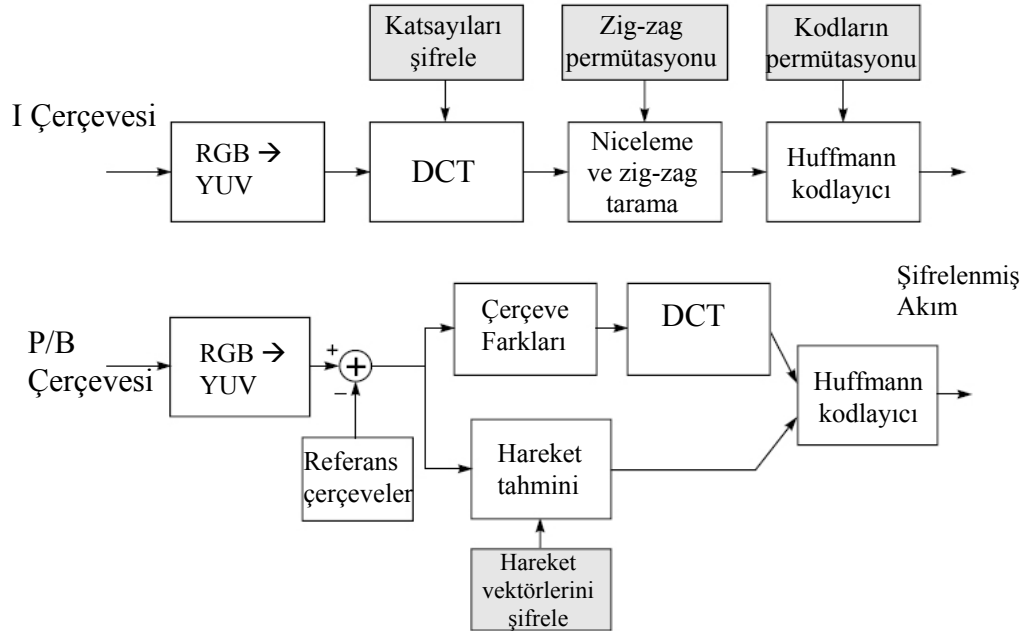
Sistemin güvenlik seviyesi seçilen şifreleme algoritmasına bağlı olmasının dışında saldırgan tek ya da çift listelerden herhangi birisini ele geçirdiğinde sistemi tamamen çözebilmektedir. Bu yüzden yazarlar, listeyi tek ve çift olmak üzere ikiye bölmek yerine *AnahtarM* denilen ikinci bir anahtar kullanarak ikiye bölmeyi önermektedirler. Bu eşit sayıda 0 ve 1 içeren, 64 veya 128 bit uzunluğunda bir anahtardır. *AnahtarM* anahtarının değeri gizli tutulduğu takdirde saldırganın alt listeleri

çözmesi çok uzun zaman almaktadır. Bu yüzden *AnahtarM* anahtarının alıcıya güvenli bir şekilde ve akım çözme işlemine başlamadan önce gönderilmesi gerekmektedir. Şekil 6.7 VEA algoritmasının ikinci yaklaşımını göstermektedir.

Bu algoritmanın hızı basit yaklaşımın yarısı kadardır ve gerçek zamanlı uygulamalar için hala yüksek sayılabacak sayıda hesaplama gerektirmektedir.

6.5. Video Şifreleme Algoritmaları

Shi, Wang ve Bhargava, daha önceden gerçekleştirmiş oldukları çalışmaları Algoritma I, Algoritma II (VEA), Algoritma III (MVEA) ve Algoritma IV (RVEA) olmak üzere 4 grupta toplamışlardır. Bu algoritmaların temel prensipleri şekil 6.8’de gösterildiği gibi MPEG dosyalarında DCT katsayı matrislerinin kısmi şifrelenmesine dayanmaktadır (Shi v.d., 1999).



Şekil 6.8. Video şifreleme algoritmaları

6.5.1. Algoritma I

Birinci algoritma, I çerçevelerindeki Huffman kod kelimelerinin permütasyonu işlemine dayanmaktadır. Algoritmanın gizli kısmı, MPEG sıkıştırma metodunda sabit olarak kullanılan Huffman tablolarını karıştıran π permütasyon değeridir. Sıkıştırma miktarını bozmamak için Huffman tablosunun permütasyonu alınırken aynı bit uzunluğuna sahip kodların değiştirilmesine dikkat edilmektedir. Ayrıca orijinal tablo ile şifrelenmiş tablo arasındaki farkın, kullanıcı tarafından belirlenmiş, şifre kalite parametresi β 'dan büyük olması beklenmektedir.

Algoritma I'in güvenliği, bilinen açık metin ve şifreli metin saldırılarına oldukça açık olduğundan çok iyi değildir. Bazı şifresiz video çerçeveleri bilinir ise (siyah boş ekran, program girişleri) orijinal ve şifreli çerçeveler karşılaştırılarak π permütasyonu kolaylıkla belirlenebilmektedir.

Bunun dışında Algoritma I, şifreli metin saldırılarına da hedef olmaktadır. Aynı bit uzunluğundaki kodları karıştırdığından ve Huffman kodlamasına göre en düşük bit uzunluğuna sahip kodlar sık kullanılan karakterler için kullanıldığından uzun kodlu permütasyonlar göz ardı edilerek, kayıplı da olsa orijinal görüntüye çok yaklaşık sonuçlar elde edilebilmektedir.

6.5.2. Algoritma II (VEA)

İkinci algoritma MPEG video akımında bulunan DCT katsayılarının işaret bitlerini m bitlik gizli $AnahtarK=k_1, k_2, \dots, k_m$ ile XOR işlemine tabi tutarak şifrelemektedir. Bu yaklaşımın etkisi olarak DCT katsayılarının işaret bitleri $AnahtarK$ 'nın bit dağılımına göre rasgele değişmesidir. Eğer k_i biti 0 ise işaret biti değişmeden kalmaktadır k_i biti 1 ise işaret biti değişmektedir. K anahtarı her zaman sabit kaldığından Şekil 6.9'da gösterilen algoritma II, bilinen açık metin saldırılarına karşı zayıf kalmaktadır.

```

Algoritma II: VEA(
int m, /* Anahtar uzunluğu */
bit key[m], /* Gizli anahtar */
char *mpeg_video, /* Girdi dosyası */
char *vea_sifreli_video) /* Çıktı dosyası */
{
int n; /* Tampon boyutu */
bit video[n]; /* Girdi tamponu */
file in; /* Girdi */
file out; /* Çıktı */
int k,l,i=0;
in=open(mpeg_video,"r");
out=open(vea_sifreli_video,"w");
while(!eof(in)) {
    l=read(video,n,in); /* Bir bit oku */
    for(k=0;k<l;k++){
        switch(video[k]) {
            case(GOP başlangıcı): i=0;break;
            case(DCT işaret biti):
                video[k]=video[k] XOR key[i];
                i++ mod m;
                break;
        }
    }
    write(video,l,out); /* Bir bit yaz */
}
Close(in);close(out);
}

```

Şekil 6.9. VEA şifreleme algoritması

6.5.3. Algoritma III(MVEA)

İkinci algoritmanın güçlendirilmiş şeklidir. Algoritma II'ye ilave olarak P ve B çerçevelerine ait hareket vektörlerinin işaretlerinin rastgele şekilde değiştirilmesini öngörmektedir. Hareket vektörlerinin işaretleri değiştirildiğinde yönleri de değiştiğinden, bu tip bir eklenti video'yu gösterim sırasında daha rastlantısal ve izlenemez hale getirmektedir. Şekil 6.10'da gösterildiği gibi, algoritma ek olarak hareket vektörlerindeki değişim miktarını da arttırarak görüntüyü tamamen izlenemez

kılmaktadır. Bu algoritmada da Algoritma II’de olduğu gibi m bitlik K anahtarı kullanılmaktadır. Bu yüzden Algoritma II’de bulunan güvenlik sorunları bu algoritmaya taşınmaktadır.

```

Algoritma III: MVEA(
int m, /* Anahtar uzunluğu */
bit key[m], /* Gizli anahtar */
char *mpeg_video, /* Girdi dosyası */
char *mvea_sifreli_video) /* Çıktı dosyası */
{
int n; /* Tampon boyutu */
bit video[n]; /* Girdi tamponu */
file in; /* Girdi */
file out; /* Çıktı */
int k,l,i=0;
in=open(mpeg_video,"r");
out=open(mvea_sifreli_video,"w");
while(!eof(in)) {
    l=read(video,n,in); /* Bir bit oku */
    for(k=0;k<l;k++){
        switch(video[k]) {
            case(GOP başlangıcı): i=0;break;
            case(DCT işaret biti):
                video[k]=video[k] XOR key[i];
                i++ mod m;
                break;
            case(hareket vektörü işaret biti):
                video[k]=video[k] XOR key[i];
                i++ mod m;
                break;
        }
    }
    write(video,l,out); /* Bir bit yaz */
}
Close(in);close(out);
}

```

Şekil 6.10. MVEA şifreleme algoritması

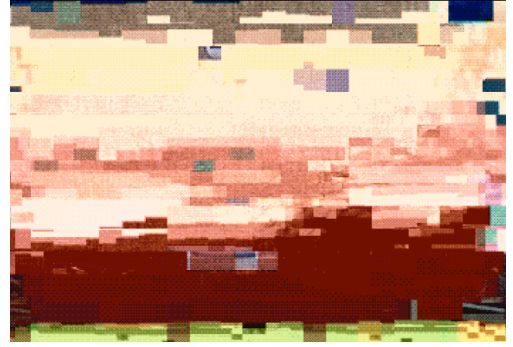
6.5.4. Algoritma IV(RVEA)

Yazarların geliştirdiği dördüncü algoritmaya göre MPEG akımından DCT katsayılarının işaretleri ve hareket vektörleri belirlenmekte ve AES gibi geleneksel bir şifreleme metoduyla şifrelenmektedir. Bunun etkileri, bazı işaret bitlerinin değiştiği önceki algoritmalara (VEA/MVEA) benzemektedir. Yazarlar hesaplama zamanının kısılması için şifrelenecek bit sayısını 64 ile sınırlı tutmaktadırlar.

RVEA, MPEG akımının sadece %10'luk bir kısmını DES, IDEA, AES gibi geleneksel metotlar ile şifrelemekte ve basit yaklaşıma göre %90 gibi bir hesaplama zamanı tasarrufu sağlamaktadır (Shi v.d., 1999). Şekil 6.11 video şifreleme algoritmaları kullanılarak şifrelenmiş örnek videoları göstermektedir.



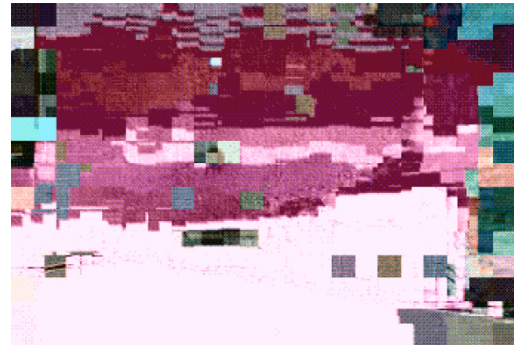
a) Orijinal görüntü



b) VEA ile şifrelenmiş görüntü



c) MVEA ile sadece hareket vektörleri şifrelenmiş görüntü



d) RVEA ile şifrelenmiş görüntü

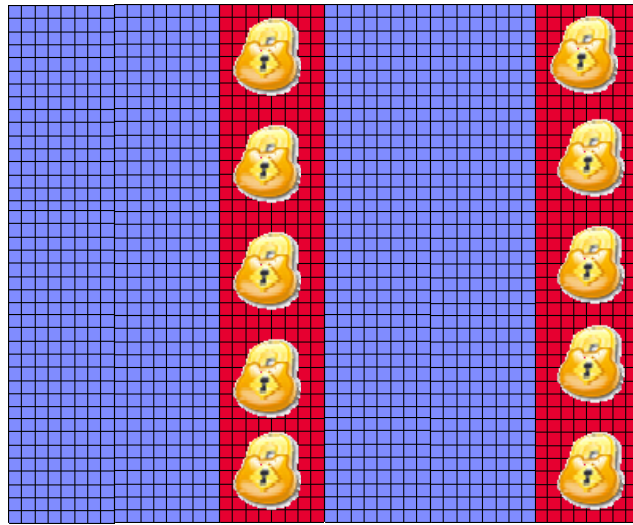
Şekil 6.11. Orijinal görüntü ve şifrelenmiş görüntü sonuçları

6.6. Video Şifreleme Metotları

1999 yılında Alattar, Al-Regip ve Al-Semari DES şifreleme sistemine dayanan Metot I, Metot II ve Metot III diye adlandırdıkları 3 farklı yöntem sunmaktadırlar. Bu geliştirilen 3 metot, temelde yazarların daha önce yapmış oldukları Metot 0'dan yola çıkılarak tasarlanmıştır. Metot 0'a göre I çerçevesinde bulunan tüm makro bloklar DES şifreleme sistemiyle şifrelenmektedir. Bu yaklaşım MPEG akımının %40 ile %79 oranı arasında değişen büyük bir kısmını şifrelediği için başarı olarak benzerlerini geçememektedir.

Metot I, MPEG akımına ait her I çerçevesinin n . makro bloğunu DES şifreleme algoritması kullanılarak şifrelemektedir. Bunun dışında kalan veriler ise şifrelenmemektedir. n değeri için özel bir rakam belirtilmemiş, uygulama ve güvenlik gereksinimlerine göre seçimlik bırakılmıştır. $n=2$ olduğunda I çerçevesini oluşturan makro blokların yarısı şifrelenmekte ve güvenlik düzeyi yüksek olmaktadır. Diğer yandan n değeri büyütüldüğünde hesaplama kazançları artmakta, güvenlik düzeyleri düşmektedir. Şekil 6.12 $n=3$ için I çerçevesinin şifrelenen alanlarını göstermektedir. Burada önemli olan kısım I çerçevesine ait şifrelenmemiş olarak bırakılan makro blokların önemsiz olma zorunluluğudur (Furth ve Kirovsky, 2004).

I Çerçevesi



Şekil 6.12. $n=3$ için metot 1 şifreleme

Birinci metodun güvenliğini artırılması için yazarlar B ve P çerçevelerine ait tüm makro blok başlık bilgilerinin DES şifreleme algoritması kullanılarak şifrelenmesini öngörmektedirler. DES 64 bitlik bloklar üzerinde çalışan bir blok şifreleme algoritması olduğundan makro blok başlıkları 64'lü gruplar halinde şifrelenmektedir. Metot II, metot 0'dan hızlı olmasına rağmen metot I'den yavaş çalışmaktadır.

Son olarak yazarlar Metot II'nin hesap yükünü azaltmak için B ve P çerçevelerine ait tüm makro blok başlık bilgilerini şifrelemek yerine tüm çerçevelerdeki n . makro bloğun başlık bilgilerini şifrelemeyi öngörmektedir.

6.7. *MHT Şifreleme Metodu ve MSI kodlayıcısı*

Wu ve Kua 2000-2001 yıllarında MPEG video akımını şifrelemek için MHT şifreleme metodu ve MSI kodlayıcısı adında iki farklı yöntem önermektedirler.

MHT şifreleme metodu, standart Huffman tablolarının gizli bir anahtar yardımıyla değiştirilmesini öngörmektedir. Daha önce incelenen Shi, Wang ve Bhargava'nın Algoritma I yöntemi de benzer bir yaklaşımı öngörmekteydi, fakat farklı Huffman ağaçları üretmeye dayalı bu yöntem 3 adımda gerçekleşmektedir.

1. 0'dan 2^k-1 'e kadar 2^k adet Huffman tablosu oluştur
2. 0'dan 2^k-1 'e kadar k bitlik p_i değerleri alan rastlantısal $P=(p_1, p_2, p_3, \dots, p_n)$ vektörünü oluştur
3. Video akımını sıkıştırırken Huffman kodlama aşamasında i . Sembol için $P_{(i-1 \pmod n)+1}$ numaralı Huffman tablosunu kullan.

Diğer yöntemlerden farklı olarak bu yöntem sıkıştırma oranının etkilenmemesi için çok rastlantısal tablolar yerine şekil 6.13'te gösterildiği gibi değişime uğramış Huffman tabloları kullanmaktadır. Deneysel çalışmalar göz önüne alındığında çoklu Huffman tablolarının kullanılması sıkıştırma oranlarını fark edilir düzeyde düşürmemektedir (Furth ve Kirovsky, 2004).

1. Bit karıştırma
2. Blok karıştırma
3. Blok döndürme

Algoritmaya göre her bir I çerçevesi, her biri makro bloklardan oluşan bölümlere ayrılmaktadır. Her bir bölümdeki aynı dereceli DCT katsayıları karıştırılmakta ve her bir katsayının işaret bitleri şifrenmekte ya da gizli bir anahtara göre yer değiştirmektedir. Yazarlar ayrıca P ve B çerçevelerine ait hareket vektörlerinin de şifrenmesini öngörmektedir (Furth ve Kirovsky, 2004).

BÖLÜM 7

SIKIŞTIRILMIŞ VIDEO AKIMININ DÜZENSİZ HARİTALAR VE BAŞLANGIÇ KODLARINA DAYALI ŞİFRELENMESİ

Televizyon, internet, video konferans, tıbbi ve askeri görüntüleme gibi birçok sayısal video tabanlı sistem, saklama ve veri iletimi sırasında tutarlı bir güvenliğe ihtiyaç duymaktadır.

1976 yılından günümüze uzanan simetrik şifreleme algoritması DES ve diğer geleneksel şifreleme algoritmaları halen birçok güvenlik uygulamalarına temel teşkil etmektedirler. 1990'lı yıllardan bu yana video ve resim şifreleme ile ilgili birçok çalışma yapılmıştır. Metin tabanlı şifreleme yöntemleri hala popülerliğini korurken, video görüntülerinin güvenliğini sağlayacak, dönüm noktası sayılabilecek bir güvenlik yöntemi henüz geliştirilmemiştir.

Sıkıştırılmış video akımını şifrelemeye yönelik yeni bir yöntem geliştirme sürecinde yapılan çalışmalar aşağıda sunulmaktadır.

7.1. MPEG Akımında Başlık Şifreleme

MPEG olarak sıkıştırılmış bir video akımı, mevcut şifreleme algoritmaları kullanarak şifrelenebilir. Mevcut güvenliğin arttırılması amacıyla şifreleme ve açma anahtar uzunlukları büyütülebilmektedir. Fakat bu işlem şifreleme ve çözme işlemlerinin süresini arttırmaktadır.

MPEG akımının çözülmesi işleminin adımları incelendiğinde, videonun tekrar izlenebilir hale gelebilmesi için, MPEG başlıklarının ne kadar hayati bir önem taşıdığı görülmektedir. Şekil 7.1'de örnek bir çerçeveye ait dilim başlangıcı ve dilime ait bazı kodlar verilmektedir.

00	00	01	01	4A	BB	D1	40	04	E0	0F	50
10	FF	E4	60	22	80	27	40	9A	00	6D	F1
C7	11	45	EB	9D	4D	3F	32	9D	83	60	43
7E	98	C6	F8	11	1A	AF	B0	AA	3F	8C	21
36	9A	16	D1	1A	B7	80	00	72	24	02	50
08	30	90	C4	00	E4	48	04	BE	98	48	6D
EC	CD	6A	1A	D6	DF	34	00	E4	48	04	BE

Şekil 7.1. 1 Numaralı dilim

Dikkat edildiğinde “00 00 01 01” byte dizisi 1 numaralı dilimin başlangıcını belirtmektedir. Bu başlık değeri dışında bu verinin birinci dilime ait olduğunu gösteren başka bir işaret bulunmamaktadır. Eğer başlık değeri akımdan çıkartılır ise veya başlık değeri kasıtlı biçimde bozulur ise video akımının yeniden izlenmesi imkânsızdır.

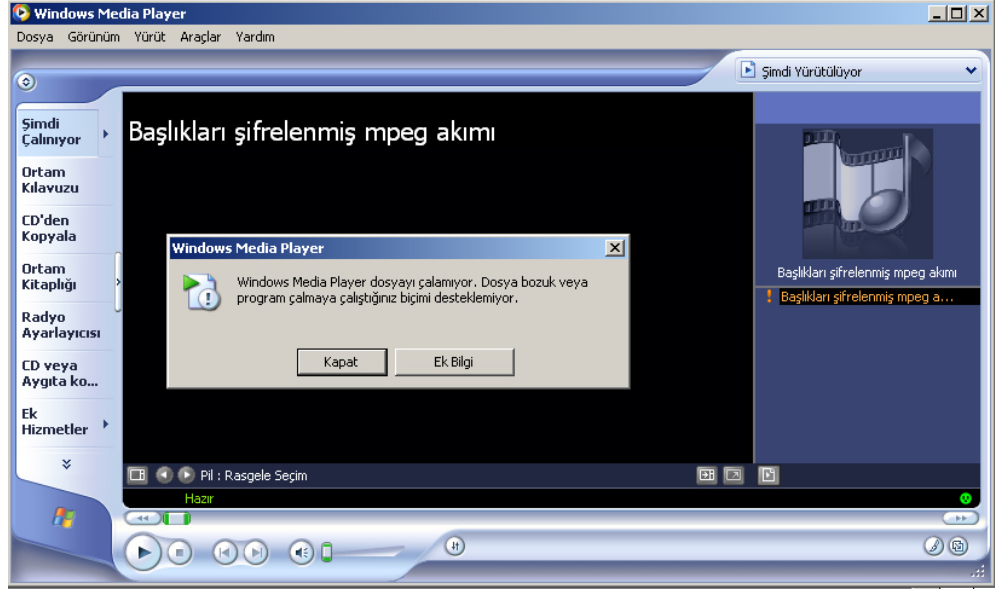
Bu yöntemde, şifreleyici bir yazılım yardımıyla izlenebilir MPEG akımındaki tüm başlık değerleri rastlantısal değerlerle değiştirilmektedir. Şifreleme işlemi sonucunda akımın orijinal başlıkları farklı bir anahtar dosya içine kaydedilmektedir. Anahtar dosya olmaksızın şifrelenmiş video akımını izlemek hiçbir şekilde mümkün değildir. Şifre çözücü yazılım kısmında, anahtar dosyada bulunan başlık değerleri şifreli video dosyasındaki yerlerine yazılarak video akımı yeniden oluşturulmaktadır. Şekil 7.2 orijinal ve şifrelenmiş video akımlarını göstermektedir.

00	00	01	01	4A	BB	D1	40	04	E0	0F	50
W	X	Y	Z	4A	BB	D1	40	04	E0	0F	50

Şekil 7.2. Orijinal ve şifrelenmiş MPEG akımları

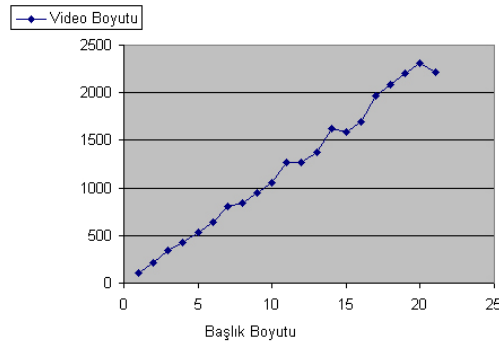
Başlık verileri tahrip edilmiş bir MPEG dosyasının izlenmesi mümkün değildir. Başlıkları bozulmuş bir video akımını izlenebilir kılan henüz bir metot geliştirilmemiştir. Bu avantajları kullanarak yöntem çok küçük bir veriyi şifreleyerek bir veri bütününe anahtar dosya olmadan, anlamsız ve kullanılamaz hale getirmiştir (Taşkın v.d., 2007).

Anahtar dosya mevcut şifreleme metotları kullanılarak şifrelendiğinde güvenlik son derece sağlam hale gelmektedir. Anahtar dosya şifrelenmediği durumda dahi anahtar dosyanın deseni bilinmediğinden şifre çözme işlemi gerçekleştirilemeyecektir. Şekil 7.3, yöntem kullanılarak şifrelenmiş dosyanın izlenmek istenmesi durumunda ortaya çıkan hatayı göstermektedir.



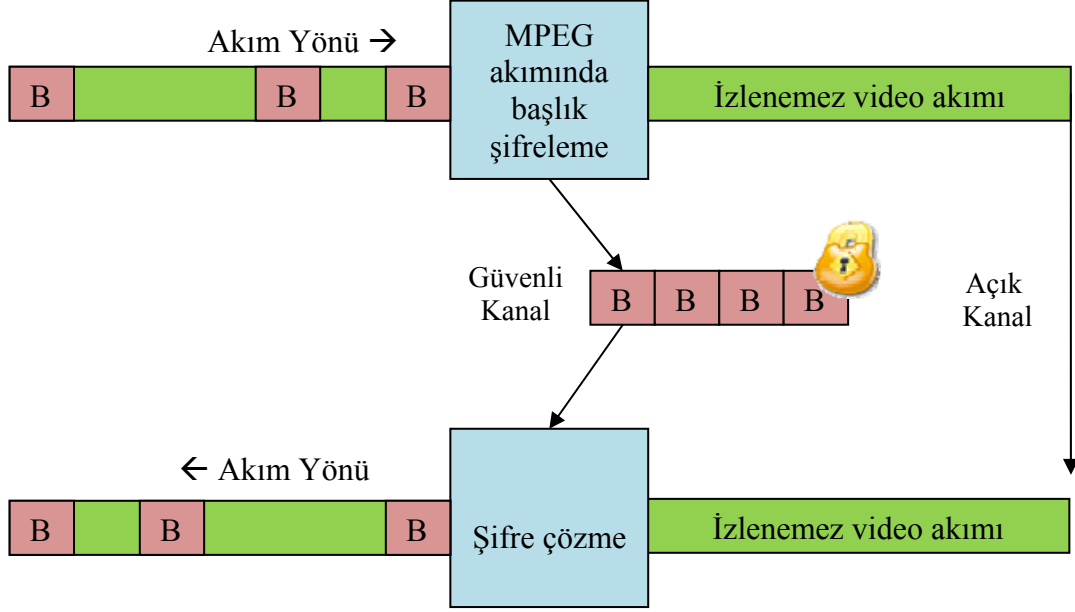
Şekil 7.3. Şifrelenmiş akım izleme hatası

Video boyutuna bağlı olarak başlıkların kapladığı toplam boyut da artmaktadır. Bu şifrelenecek veri miktarında da artışa neden olmaktadır. Buna rağmen başlık boyutları toplam video boyutunun yaklaşık %1 eşdeğeridir. Şekil 7.4'te videoların kapladıkları dosya boyutlarına göre sistem başlıklarının kapladıkları alanlar verilmiştir.



Şekil 7.4. Video boyutuna göre toplam başlık boyutları

Şekil 7.5 MPEG akımında başlık şifreleme metodunu göstermektedir.



Şekil 7.5. MPEG akımında başlık şifreleme metodu

7.2. MPEG Akımında Operatör İşlemlerinin Kısıtlanması Yoluyla İçerik Koruma

Video dosyalarında içeriğin bütünlüğünün korunması açısından, ileri geri alma gibi operatör işlemlerinin engellenmesi ve video bütününden belli bir parçanın kopyalanmasının engellenmesi önemlidir. Bu amaçla, akımın çözülmesi işlemi detaylı bir şekilde incelenmiştir. Akımda yapılacak değişiklik akımın tümünden bozulmasına neden olmamalıdır.

Yapılan çalışmalarda,

- Bir sıralama başlangıcı her zaman en azından bir resim grubu tarafından takip edilmekte
- Bir video akımında birden fazla sıralama başlangıcı bulunmakta

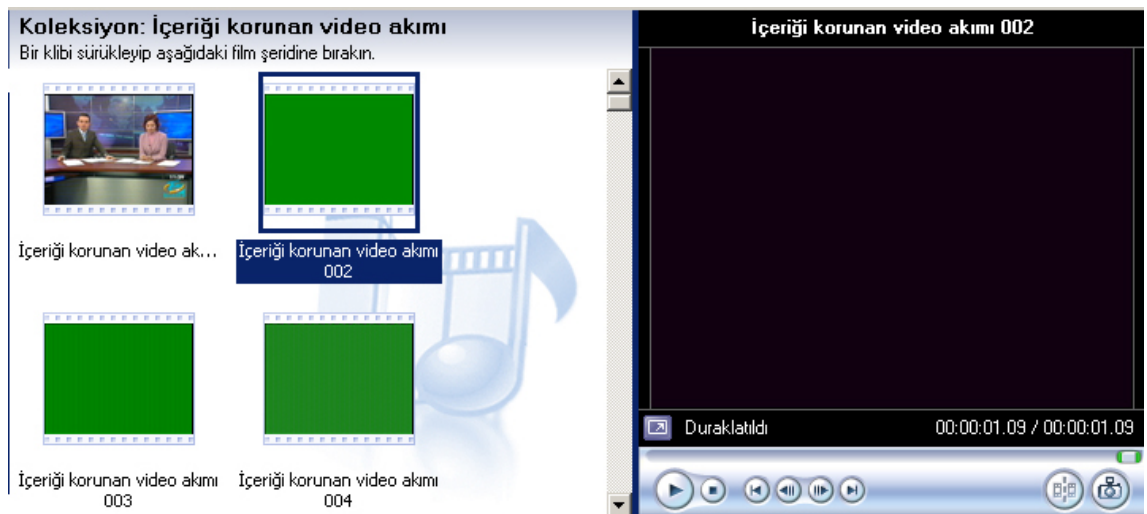
c) Bir video gösterici birimin, ileri sarma ya da geri sarma işlemleri için, video akımı çözme basamaklarını yinelemekte

olduğu belirlenmiştir.

Bu durumda video gösterici birimin ileri ya da geri sarma işlemleri sırasında, akım içerisinde birden fazla bulunan, sıralama başlangıcı kodunu bulması gerekmektedir. Eğer bir video akımında bir tek sıralama başlangıcı kodu bulunursa, akım içerisinde operatör işlemlerini uygulamak mümkün olmayacaktır. Ayrıca bir sıralama başlangıcı her zaman resim grupları tarafından takip edileceğinden, video baştan sona izlenirken başka sıralama başlangıcı koduna ihtiyaç duyulmayacaktır (Taşkın v.d., 2007).

Örnek video görüntüsü içinden ilk sıralama başlangıç koduna müdahale edilmemekte, diğerlerine ise rastlantısal veriler girilmektedir. Sıralama başlangıçları yerine, rastlantısal verilerin konması akımın çözülmesi işlemine herhangi bir etki etmemektedir. Bu sayede video akımı, mevcut kullanılan donanım ve yazılım birimleri ile izlenmektedir.

Değişiklik yapılan video akımı, yazılım ve donanım tabanlı video çözücü birimler tarafından test edilmiş ve akım içerisinde ileri ya da geri sarma operatör işlemlerinin gerçekleştirilemediği gözlemlenmiştir. Şekil 7.6'da görüldüğü gibi, video işleme işlemleri için kullanılan Movie Maker yazılımı, korunmuş video akımlarından izlenebilir video parçacıkları çıkarmayı başaramamıştır.



Şekil 7.6. Movie Maker yazılımı ve korunmuş video akımı

7.3. *Sıkıştırılmış Video Güvenliği*

İçerik güvenliği ve erişim kontrolü genellikle şifreleme ile sağlanmaktadır. Eşsiz bir yapıya sahip MPEG sıkıştırılmış video akımı geleneksel metotlar kullanılarak şifrelenebilmektedir. Bu çalışmada, asimetrik şifreleme algoritması kullanılarak şifrelenen video verilerinin açık noktalarına değinilmiştir. Düz metni şifrelemek için kullanılan bu algoritmalarda, gizli metinden anahtar değeri bilmeden açık metni elde etmek için yeterli sayıda açık metin-şifreli metin ikilisine ihtiyaç duyulmaktadır. Şifreli metinden elde edilebilecek sızıntı, kelime boyları ve harf kullanım yoğunlukları olmaktadır. Bu özellikleri kullanarak açık metin-şifreli metin ikilileri elde etmek için sözlük kullanılmaktadır. Geleneksel metotlar, deneme yanılma sayısının çok olması ve kırma işleminin çok uzun sürmesi açısından kırılmaz olarak nitelendirilmektedirler.

MPEG sıkıştırılmış video akımının düşman saldırılara açık olduğu en zayıf noktası başlık değerleridir. MPEG akımının sabit bir dosya deseninin bulunmamasından dolayı akımın çözülmesinde MPEG video başlıkları birincil rol oynamaktadır. Bütün başlangıç kodları yirmi üç adet 0 ve bir adet 1'den oluşan 3 byte'lık bir ön ek almaktadırlar ve yüksek sıkıştırma oranlarından dolayı MPEG video akımında başlık bilgileri dışında böyle bir dağılıma rastlamak mümkün değildir. Doğal olarak böyle bir bit diziliminin şifrelenmiş hali de tekrarlı olacağından kolayca fark edilebilir.

Saldırgan, elinde bulunan şifreli video akımı içersinde birbiri ardına sıralanmış iki adet aynı değerli sayı tespit ettiğinde, bunun bir başlık bilgisi olduğunu öngörerek anahtar değeri tespit edebilir. Saldırgan şifrelenmiş akımdaki sadece basit birkaç karşılaştırma işlemi sonrasında, başlık bilgilerini kullanarak birçok açık metin-şifreli metin ikilisi elde etmektedir.

Prensip olarak, sayısal video verisi bir bit akımına dönüştürülerek geleneksel veri gibi şifrelenebilir. Sayısallaştırılmış ve sıkıştırılmış video verisinin alfa-sayısal biçimde ele alınıp şifrelenmesi görüldüğü gibi hatalı bir yaklaşımdır. Video verisinin eşsiz yapısından dolayı “ya hep-ya hiç” koruma mantığına sahip geleneksel şifreleme yöntemleri video verisinin güvenliği için uygun olmamaktadır. Anahtar bilinmeden, şifreli metin incelenerek elde edilen açık noktalar kullanılarak şifre kırma işlemi yapılmaktadır. Tüm bu noktalar dikkate alındığında akım bütününün şifrelenmesi saldırıya şifreyi kırması için yeterli bilgiyi sağlamaktadır. Akımın bütününün yerine

belli bir kısmının şifrelenmesinin daha fazla güvenlik sağlayacağı açıkça görülmektedir. Bu sebeple saldırıya yeterince açık metin-şifreli metin ikilisi sağlayan başlık bilgilerinin şifrelenmemesi öngörülmektedir. Başlık bilgileri dışında MPEG akımında birbirini tekrarlayan veri bulunmamaktadır. Bu yüzden başlık bilgileri dışındaki bit akımı, şifreleme işlemine tabi tutulmaktadır ve şifreli dosyada işleme alınan tekrarlı bilgi bulunmamaktadır. Bu da şifreli dosyanın kırılmasını büyük oranda zorlaştırmaktadır. Başlık bilgileri dışındaki verinin şifrelenmesi saldırıya açık nokta bırakmamaktadır. Şekil 7.7 açık ve öngörülen yöntemle şifrelenmiş video akımlarını göstermektedir (Taşkın v.d., 2007).

95 46 DB 6E BD 70 00 00 01 B8 44 00 04 92 F4 01
 00 9C 43 F8 9A 1E 01 E0 07 EC 81 98 00 DA 3D 98
 8F 7A 59 4D B6 87 5C 92 C0 F2 8F B6 C3 92 0D 6A
 C5 BC CC ED F2 65 CB 36 17 64 9A 1E 74 19 0B 28
 B1 8D 67 F7 9C 99 9B 7A 8B 22 52 E5 45 DA B0 28

Resim grubu başlık bilgisi

a) Açık video akımı

90 43 DE 6B B8 75 00 00 01 B8 41 05 01 97 F1 04
 05 99 46 FD 9F 1B 04 E5 02 E9 84 9D 05 DF 38 9D
 8A 7F 5C 48 B3 82 59 97 C5 F7 8A B3 C6 97 08 6F
 C0 B9 C9 E8 F7 60 CE 33 12 61 9F 1B 71 1C 0E 2D
 B4 88 62 F2 99 9C 9E 7F 8E 27 57 E0 40 DF B5 2D

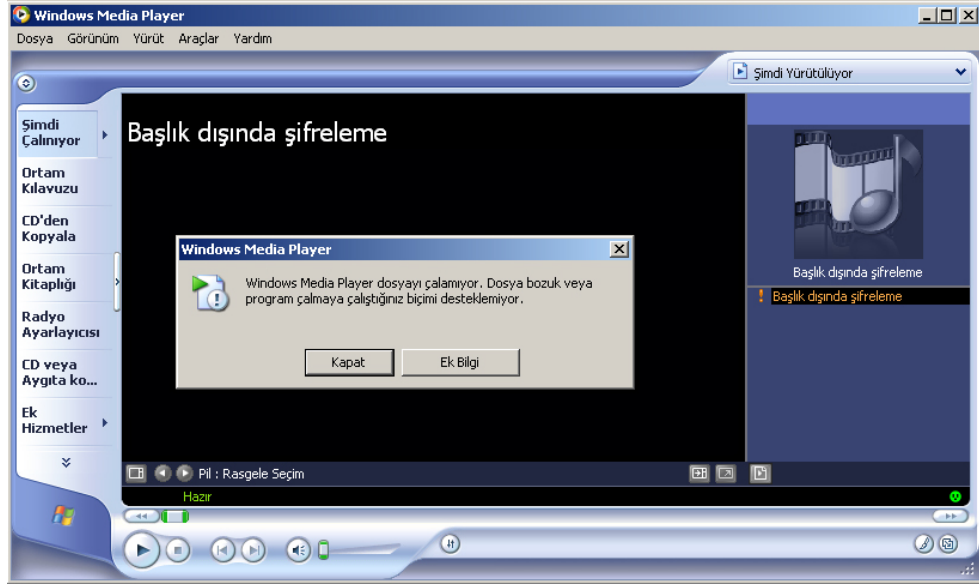
Resim grubu başlık bilgisi

b) Şifreli video akımı

Şekil 7.7. Açık ve öngörülen yöntemle şifrelenmiş video akımları

MPEG video akımında başlık bilgilerinin kapladığı alan, veri bütününe %1'lik miktarını oluşturmaktadır. Toplam veri miktarına göre çok düşük bir alan kaplayan başlık bilgileri, şifre kırma işlemi için çok değerli bilgiler sızdırmaktadır.

Bu yöntem, MPEG kodlama yapısına özel geliştirildiğinden, veri bütününe şifrelenmesi gereken kısımlarını kendisi belirlemektedir. Belirlenen zayıf noktalar şifrelenmeyerek verinin güvenliği arttırılmaktadır. Şekil 7.8, bu yöntem kullanılarak şifrelenmiş dosyanın izlenmesi durumunda ortaya çıkan hatayı göstermektedir.

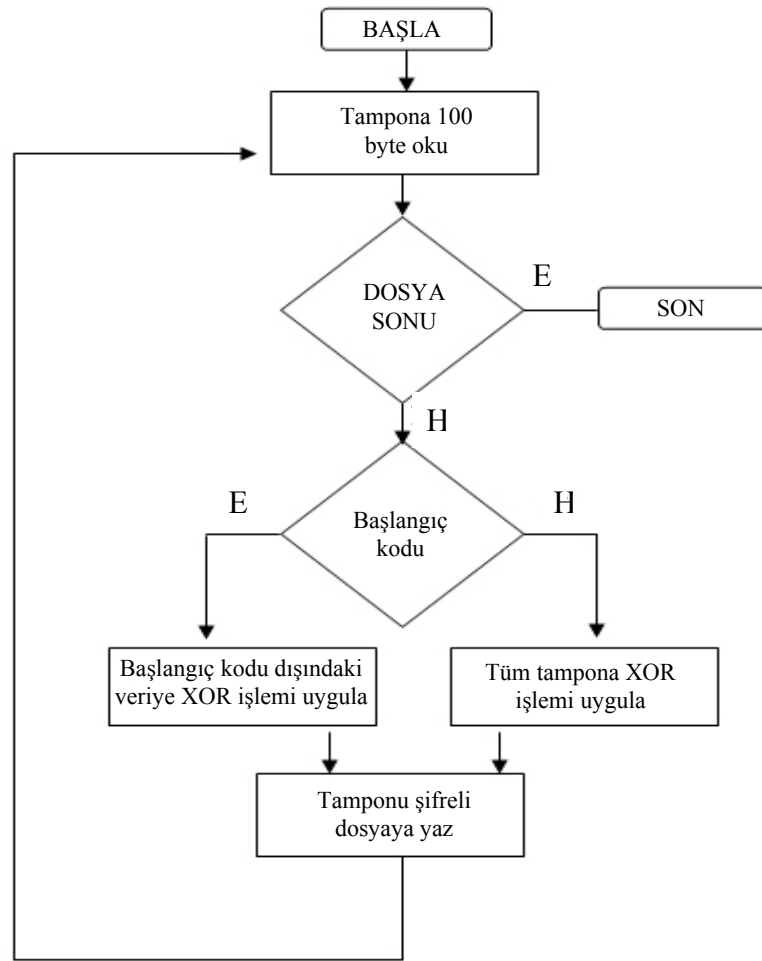


Şekil 7.8. Şifrelenmiş akım izleme hatası

7.4. Seçimli XOR İşlemi İle MPEG Video Akımını Koruma

Mpeg video akımının çözülmesi, akımın kodlanması işleminin tam tersi şeklinde yapılmaktadır. Akım çözücü videoyu izleyiciye göstermek için başlangıç kodlarını kullanmaktadır. Başlangıç kodlarının, videoyu oluşturan çerçevelerin içerikleriyle doğrudan bir bağlantısı bulunmadığından şifrelenmemektedirler. Bu yaklaşımda ikili video akımı XOR işlemi kullanılarak korunmaktadır (Taşkın v.d., 2007).

Geliştirilen uygulama, video akımını açarak 100 byte'ını tampon belleğe okumaktadır. Tampon bellekte başlangıç kodu dışında kalan kısım XOR işlemine tabi tutulmaktadır. Video akımını şifreleyen bu basit yaklaşım zaman açısından çok uygundur ve dosya boyutunu değiştirmektedir. Bu metot ile video şifreleme için kullanılan ağır hesaplamalara ihtiyaç kalmamıştır. Şekil 7.9 seçimli XOR işleminin akış şemasını göstermektedir.



Şekil 7.9. Seçimli XOR işlemi

7.5. Byte Dağılımını Değiştirerek MPEG Video Akımını Koruma

MPEG akımının izlenebilir olması için başlangıç kodlarının doğru olması gerekmektedir. Başlangıç kodları kod çözme işlemi için önemli bilgiler içermektedir. Bu yaklaşımda MPEG video dosyasındaki başlangıç kodları, onları takip eden 4 byte ile yer değiştirilmektedir (Taşkın v.d., 2007).

Video akımını şifreleyen bu basit yaklaşım zaman ve dosya boyutu açısından çok uygundur. Bu metot ile video şifreleme için kullanılan ağır hesaplamalara ihtiyaç kalmamıştır. Şekil 7.10, byte dağılımı değiştirme işlemi için geliştirilmiş program kodunu göstermektedir.

```

#define INPUTFILE "c:\\open.mpg"
#define OUTPUTFILE "c:\\secure.mpg"

int main ()
{
    unsigned char buf[100];
    unsigned char tmp[4];
    const void *ptr=(void *) buf;
    FILE *input;
    FILE *output;
    interval=time(NULL);

    input=fopen(INPUTFILE,"rb");
    output=fopen(OUTPUT,"wb");
    while((nn=fread(ptr,sizeof(char),100,input))==100){
        for(i=0;i<96;i++){
            if(buf[i]==0 && buf[i]==0 && buf[i]==1) {
                tmp[0]=buf[i];tmp[1]=buf[i+1];tmp[2]=buf[i+2];tmp[3]=buf[i+3];
                buf[i]=buf[i+4];buf[i+1]=buf[i+5];buf[i+2]=buf[i+6];buf[i+3]=buf[i+7];
                buf[i+4]=tmp[0];buf[i+5]=tmp[1];buf[i+6]=tmp[2];buf[i+7]=tmp[3];
            }

            fwrite(ptr,sizeof(char),100,output);
        }

        for(i=0;i<nn-4;i++){
            if(buf[i]==0 && buf[i]==0 && buf[i]==1) {
                tmp[0]=buf[i];tmp[1]=buf[i+1];tmp[2]=buf[i+2];tmp[3]=buf[i+3];
                buf[i]=buf[i+4];buf[i+1]=buf[i+5];buf[i+2]=buf[i+6];buf[i+3]=buf[i+7];
                buf[i+4]=tmp[0];buf[i+5]=tmp[1];buf[i+6]=tmp[2];buf[i+7]=tmp[3];
            }

            fwrite(ptr,sizeof(char),nn,output);
        }

        fclose(input);
        fclose(output);

        printf("%d",time(NULL)-interval);
        printf("\noperation Successful");getch();

    }

    return 0;
}

```

Şekil 7.10. Byte dağılımı değiştirme

7.6. Önerilen Yöntem

Yöntemin geliştirilmesi aşamasında incelenen bilimsel yayınlar ve yapılan çalışmalar göstermiştir ki,

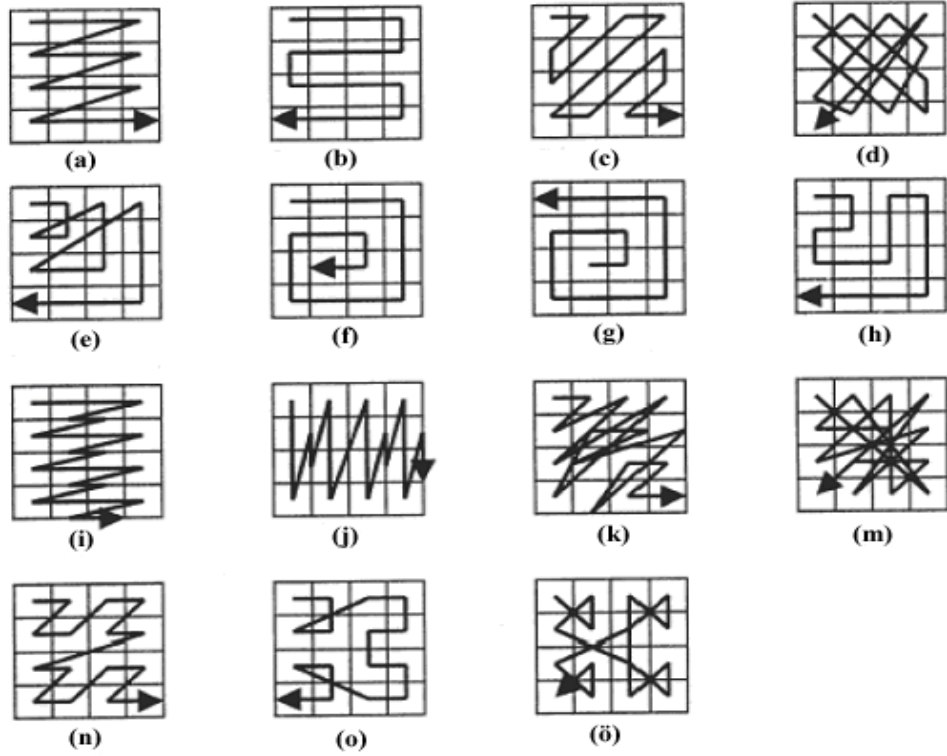
1. Video akımının tümünün geleneksel şifreleme metotlarıyla şifrlenmesi uygulanabilirlikten uzak ve güvenilir değildir.
2. Analog olarak görsel şifreleme metotlarıyla şifrlenmiş akım, video işleme metotları kullanılarak kırılabilir.
3. Videonun sıkıştırılmadan önce şifrlenmesi mümkün değildir. Sıkıştırma işlemi videonun görsel özelliklerine bağlı olduğundan şifrlenmiş görüntüdeki birçok bilgi sıkıştırma esnasında kaybolmakta ve akımın şifresinin çözülmesi imkânsız hale gelmektedir.

4. Çerçeve bazında şifreleme yapan kısmi şifreleme algoritmaları, program giriş tanıtımları, televizyon logoları gibi videoya has görüntüler yüzünden, bilinen açık metin saldırılarına karşı savunmasızdır.
5. Kısmi şifrelemede, şifrelenecek veri miktarının çok düşük tutulması güvenlik seviyesini düşürürken, yüksek tutulması ise şifreleme zamanını arttırmaktadır.
6. Video akımının izlenebilirliğinden çok, verinin tamamını şifrelemeye yönelik metotlar, video kodlama yönünden yapılan çalışmalar ile kırılmaktadırlar.

Tüm bu durumlar göz önüne alınarak, geliştirilen metodun güvenlik ve hız açısından dengeli bir yapıda olmasına dikkat edilmiştir. Sıkıştırılmış video akımının düzensiz haritalar ve başlangıç kodlarına dayalı kısmi şifrelenmesi, daha önce geliştirilen ve gerçek zamanlılıktan uzak DES, AES ve RSA gibi klasik şifreleme metotlarını içermemektedir. Metot, düzensiz haritaların piksel bazında kullanılması yaklaşımını değiştirerek, kısmi şifreleme mantığıyla özdeşleştirmektedir. Şifreleme güvenliğini arttırmak için yöntem iki aşamalı olarak tasarlanmaktadır.

7.6.1. Aşama I

Yönteme göre öncelikle MPEG akımını oluşturan çerçevelerin referans numaraları satır öncelikli yerleşim mantığı ile 4x4'lük matrise aktarılmaktadır. MPEG akımındaki referans numaraları 0 ile 30 arasında değişmektedir. Bu değerlerin bozulması için ayrıca matristeki tüm değerlere ϵ ilave edilmektedir. Ardından şekil 7.11'de verilen temel tarama desenlerinden birisi harita olarak belirlenmektedir.



Şekil 7.11. Temel tarama desenleri

Şifreleme metodunun ilk aşaması sonucunda referans numaraları tahrip edilmiş bir video akımı elde edilmektedir ve hatalı referanslara sahip hareket vektörleri ortaya çıkmaktadır. Diğer yaklaşımlar hareket vektörlerini veya hareket vektörlerinin işaretlerinin şifrelenmesini öngörmektedirler. MPEG video katmanları dikkate alındığında hareket vektörlerinin ve işaretlerinin değiştirilebilmesi için akımın blok seviyesine kadar çözülmesi gerekmektedir. Bu da akımın neredeyse tamamen elden geçmesi anlamına gelmektedir. Geliştirilen yöntem, akımı resim katmanına kadar incelemekte ve hareket vektörlerinin şifrelenmesi işlemini, hatalı referanslar yaratarak temelden çözmektedir. Referans numaralarının tahribi için ağır şifreleme algoritmaları kullanılmamış ve hafif denilebilecek temel tarama desenlerinden biri kullanılmıştır.



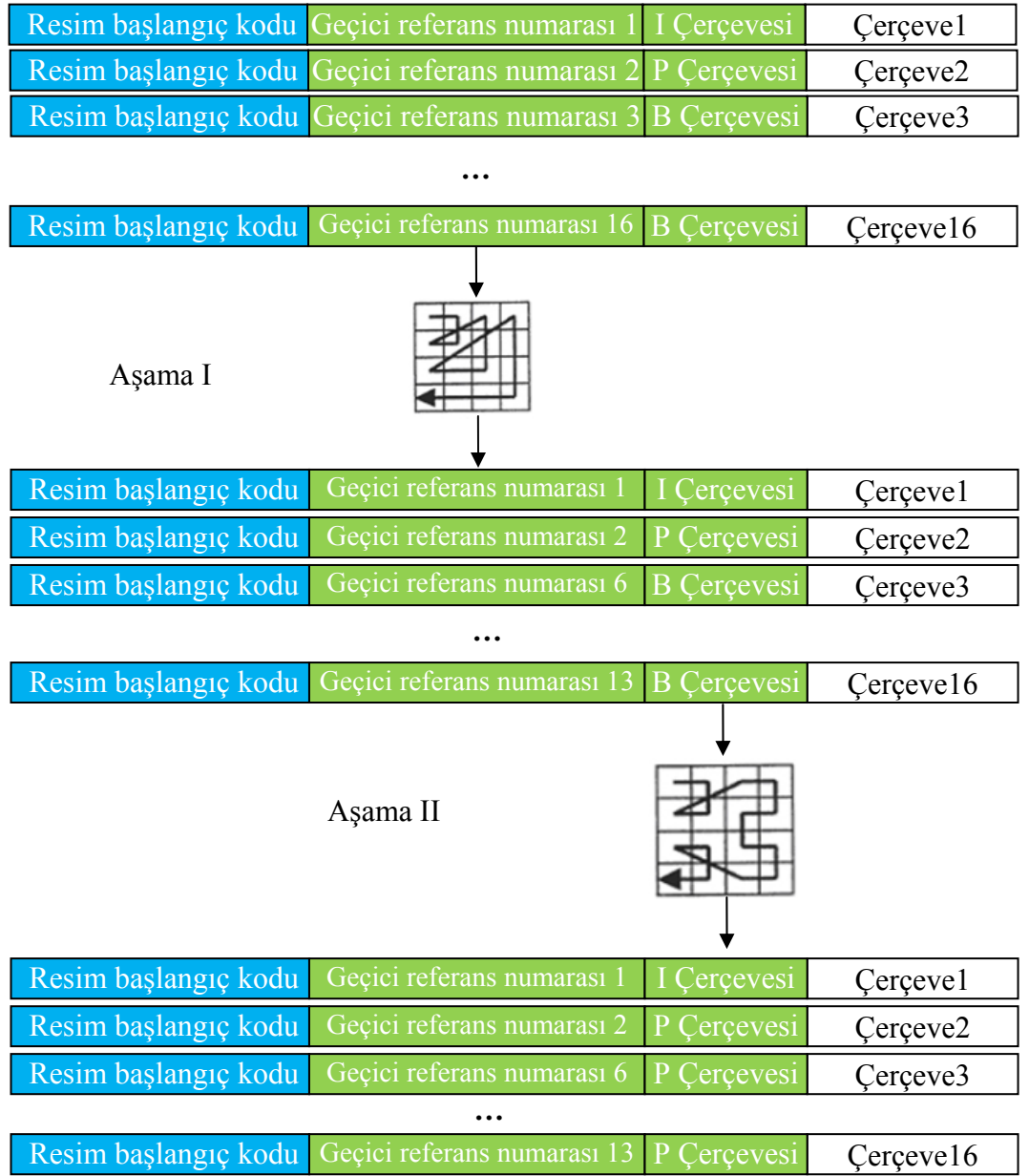
Şekil 7.12. Örnek video akımı ve şifrelenmiş görüntü

Referans numarası dışında başlangıç kodu tahrip edilmediği için MPEG akımının yapısında büyük bir bozulma olmamaktadır. Geliştirilen yöntem başlangıç kodlarını değiştirerek şekil 7.12’de gösterildiği gibi görsel bir bozulma yaratmaktadır. Akım, görsel olarak bozuk da olsa izlenebilmekte, ses paketlerine müdahale edilmediğinden sese bozulma olmamaktadır.

7.6.2. Aşama II

Yöntem ikinci seviye olarak yine resim başlangıç kodu seviyesinde ulaşılabilen çerçeve tipi bilgisini şifrelemeyi öngörmektedir. Çünkü I çerçeveleri boyut olarak akımda en büyük yeri kaplamaktadırlar ve referans çerçeveler olmadan gösterilebilmektedirler. İkinci aşamada, öncelikle çerçevelerin tiplerini satır öncelikli yerleşim mantığı ile 4x4’lük matrise aktarılmaktadır. Ardından temel tarama desenlerinden birisi harita olarak belirlenmekte ve çerçeve tipleri karıştırılmaktadır. Yeni çerçeve tipleri şifrelenmiş akıma aktarılmaktadır.

Ayrıca geliştirilen yöntem iç-çerçeve bazında şifreleme yapmadığından, bilinen açık metin saldırılarına karşı daha dayanıklıdır. Daha önce incelenen yöntemler karıştırma işlemlerini çerçeve bazında yaptıklarından bilinen şifresiz video görüntüleri kullanılarak (televizyon logosu gibi) tarama desenleri kolaylıkla belirlenmektedir. Şekil 7.13 geliştirilen yöntemin aşamalarını göstermektedir.



Şekil 7.13. Sıkıştırılmış video akımının düzensiz haritalar ve başlangıç kodlarına dayalı kısmi şifrelenmesi

BÖLÜM 8

SONUÇ

Bu tez çalışmasında video akımını şifrelemek için kullanılan yöntemler incelenmiş, yöntemlerin açık noktaları belirlenerek alternatif bir şifreleme yöntemi geliştirilmiştir. Geliştirilen alternatif yöntem, diğer yöntemlerden farklı olarak DES, RSA, AES gibi zaman alıcı klasik şifreleme metotlarını içermemektedir. Video verisi gibi yüksek veri oranlarına sahip bilginin şifrelenebilmesi için önerilen yöntem kısmi şifreleme mantığı ile bağdaşmaktadır. Kısmi şifreleme yapan bir yöntem olması, gerçek zamanlı şifreleme yapabilmesini sağlamaktadır.

Yöntem kullanılarak şifrelenmiş akımın yapısı büyük oranda sağlam kalmasına rağmen akımın izlenebilirliği bozulmaktadır. Resim çerçevesi bazında şifreleme yapan bir metot olmadığı için bilinen açık metin saldırılarına karşı daha güvenli bir metottur. Temel tarama desenleri pikseller yerine başlangıç kodları ile ilişkilendirildiğinden özgün bir yaklaşımdır.

Yeni geliştirilen yöntem MPEG kodlama yapısına özel tasarlandığından veri bütünüünün şifrelenmesi gereken kısımlarını kendisi belirlemektedir. Video akımının tamamı şifrelenmediğinden yöntemin kaynak ihtiyacı düşük olmaktadır. Çizelge 8.1’de geliştirilen yöntem ve diğer yöntemlerin şifreleme zamanları görülmektedir. Bu sonuçlara göre, önerilen yöntem geleneksel şifreleme algoritmaları içeren yöntemlerden hızlı fakat basit şifreleme aşamaları içeren kısmi şifreleme algoritmalarından bir miktar yavaştır. Geliştirilen yöntem iki aşamalı olarak çalıştığından bu daha önceden öngörülmüş ve kabul edilebilir bir sonuçtur. Ancak diğer yöntemlere göre güvenlik seviyesi daha yüksektir.

Çizelge 8.1. İncelenen yöntemlerin şifreleme hızları

Yöntem	Yöntem Türü	Dosya Boyutu	Şifreleme Zamanı (sn)	Hız (Mbit/s)
RSA (8 Bit anahtar)	Geleneksel	309MB	47.23	52
MPEG akımında başlık şifreleme	Kısmi	309MB	27.89	89
MPEG akımında operatör işlemlerinin kısıtlanması yoluyla içerik koruma	Kısmi	309MB	26.50	93
Başlık dışında şifreleme	Geleneksel + Kısmi	309MB	46.82	52
Seçimli XOR işlemi ile MPEG video akımını koruma	Kısmi	309MB	27.71	89
Byte dağılımını değiştirerek MPEG video akımını koruma	Kısmi	309MB	26.22	94
Önerilen yöntem	Kısmi	309MB	30.60	81

Çizelge 8.2’de görüldüğü gibi, önerilen yöntemin dosya boyutuna bağlı performansı incelendiğinde, küçük dosya hacimlerinde daha yüksek performans sergilediği görülmektedir.

Çizelge 8.2. Önerilen yöntemin dosya boyutuna bağlı performansı

Dosya Boyutu	Şifreleme Zamanı (sn)	Hız (Mbit/s)
30.98MB	2.68	92.48
61.96MB	5.46	90.78
92.94MB	9.57	77.69
123.92MB	11.54	85.91
154.90MB	15.18	81.63
185.88MB	17.34	85.35
216.86MB	21.60	80.32
247.84MB	24.90	79.63
278.82MB	27.75	80.38
309.80MB	30.60	80.99
619.80MB	61.70	80.34

Geliştirilen yöntem ile piksel değerlerinde bir değişiklik yapılmamasına rağmen görsel olarak bozuk bir video görüntüsü elde edilmektedir. Bu, akımın şifresini kırmak isteyen saldırganları yanlış yönlendirmektedir.

Geliştirilen yöntem iki aşama olarak uygulanmıştır. Sonraki yapılacak çalışmalarda aşama sayısını arttırmak mümkündür. MPEG başlık bilgileri dosyanın çok az miktarını kapsadıkları halde içinde önemli bilgileri barındırmaktadır. Bu bilgilere farklı yöntemler uygulanabilir. Geliştirilen yöntem resim başlangıç kodu seviyesinde şifreleme yapmaktadır. Farklı başlangıç kodları seviyesinde şifreleme metotları geliştirilebilir.

EK-A**DEĞİŞKEN UZUNLUKTA KODLAMA ÇİZELGELERİ**

Çizelge 1. Makro blok adres artım çizelgesi

Değişken uzunlukta kod	Artım değeri	Değişken uzunlukta kod	Artım değeri
1	1	0000 0101 10	17
011	2	0000 0101 01	18
010	3	0000 0101 00	19
0011	4	0000 0100 11	20
0010	5	0000 0100 10	21
0001 1	6	0000 0100 011	22
0001 0	7	0000 0100 010	23
0000 111	8	0000 0100 001	24
0000 110	9	0000 0100 000	25
0000 1011	10	0000 0011 111	26
0000 1010	11	0000 0011 110	27
0000 1001	12	0000 0011 101	28
0000 1000	13	0000 0011 100	29
0000 0111	14	0000 0011 011	30
0000 0110	15	0000 0011 010	31
0000 0101 11	16	0000 0011 001	32
		0000 0011 000	33
		0000 0001 111	Fazlalık
		0000 0001 000	Makro blok kaçış

Çizelge 2. I Çerçevesi için makro blok tipi

Değişken uzunlukta kod	Nicelik çarpanı	İleri yönde tahmin	Geri yönde tahmin	Makro blok dokusu	İç makro blok
1	0	0	0	0	1
01	1	0	0	0	1

Çizelge 3. P Çerçevesi için makro blok tipi

Değişken uzunlukta kod	Nicelik çarpanı	İleri yönde tahmin	Geri yönde tahmin	Makro blok dokusu	İç makro blok
1	0	1	0	1	0
01	0	0	0	1	0
001	0	1	0	0	0
00011	0	0	0	0	1
00010	1	1	0	1	0
00001	1	0	0	1	0
000001	1	0	0	0	1

Çizelge 4. B Çerçevesi için makro blok tipi

Değişken uzunlukta kod	Nicelik çarpanı	İleri yönde tahmin	Geri yönde tahmin	Makro blok dokusu	İç makro blok
10	0	1	1	0	0
11	0	1	1	1	0
010	0	0	1	0	0
011	0	0	1	1	0
0010	0	1	0	0	0
0011	0	1	0	1	0
00011	0	0	0	0	1
00010	1	1	1	1	0
000011	1	1	0	1	0
000010	1	0	1	1	0
000001	1	0	0	0	1

EK-B

KISALTMALAR

Kısaltma	İngilizce	Türkçe
CMYK	Cyan-Magenta-Yellow-Black	Camgöbeği-Eflatun-Sarı-Siyah
DCT	Discrete Cosine Transform	Ayrık Kosinüs Dönüşümü
DV	Digital Video	Sayısal Video
DVD	Digital Versatile Disk	Sayısal Çok Amaçlı Disk
HLS	Hue-Luminance-Saturation	Renk tonu-Parlaklık-Doygunluk
HSI	Hue-Saturation-Intensity	Renk tonu-Doygunluk-Yoğunluk
HSV	Hue-Saturation-Value	Renk tonu-Doygunluk-Değer
ISO	International Organization for Standardization	Uluslararası Standartlar Teşkilatı
MHT	Multiple Huffman Trees	Çoklu Huffman ağaçları
MPEG	Moving Picture Experts Group	Hareketli Resim Uzmanları Grubu
MVEA	Modified Video Encryption Algorithm	Değiştirilmiş Video Şifreleme Algoritması
NTSC	National Television Standards Committee	Ulusal Televizyon Standartları Komitesi
PAL	Phase Alternating Line	Faz Değişimli Hat
RGB	Red-Green-Blue	Kırmızı-Yeşil-Mavi
RVEA	Robust Video Encryption Algorithm	Güçlendirilmiş Video Şifreleme Algoritması
SECMPEG	Secure MPEG	Güvenli MPEG
VEA	Video Encryption Algorithm	Video Şifreleme Algoritması
XOR	Exclusive OR	Özel Veya
YIQ	Luma-Inphase-Quadrature	Parlaklık-Faz-Evre farkı
YUV	Luma-Chrominance	Parlaklık-Renk tonu

KAYNAKLAR

- Ahmet N., Natarajan T., Rao R., 1974, "Discrete Cosine Transform", IEEE Trans. Computers,
- Algın G. B., Tunalı E.T., 2007, "Kodlanmış video verisinin gizlilik gereksinimleri ve video şifreleme algoritmaları", Akademik Bilişim 2007, Kütahya.
- Benson B., 1986, "Television Engineering Handbook", McGraw-Hill
- Bhargava B., Changgui S., Wang S.Y., 2002, "MPEG video encryption algorithms", Kluwer Academic Publishers
- Brady N., 1999, "MPEG-4 standardized methods for compression of abritrarily shaped objects", IEEE Trans. Circuits and Systems-Video Technologies
- Brady N., Bossen F., Murphy N., 1997, "Context based arithmetic encoding of 2D shape sequences", IEEE Image Processsing Conference
- Chang S., Messerschmidt D., 1995, "Manipulation and composting of MC-DCT compressed video", IEEE Journal Selected Area Communications
- Chang S., 1995, "Compressed domain techniques for image/video indexing and manipulation", IEEE Conference-Image Processing
- Chang S., Sall S., Lee U., 1999, "Efficient video indexing scheme for content based retrieval", IEEE Trans. Circuits and Systems-Video Technologies
- Chen J., Lin D., 1997, "Optimal bit allocation for video coding video signals over ATM Networks", IEEE Journal Selected Area Communications
- Cheng H., Li X., 2000, "Partial encryption of compressed images and video", IEEE Trans. Signal Processing
- Chiang T., Zhang Y., 1997, "A new rate control scheme using quadratic rate-distortion modelling", IEEE Trans. Circuits and Systems-Video Technologies
- Chun K., Lim W., Cho H., Ra B., 1993, "An adaptive perceptual quantization algorithm for video coding", IEEE Trans. Consumer Electronics
- Clarke C.K.P., 1986, "Colour encoding and decoding techniques for line-locked sampled PAL and NTSC television signals", BBC Research Department Report BBC
- Coppersmith D., 1994, "The data encryption standard (DES) and its strenght against attacks", IBM journal of research and development.

- Cücioğlu İ., 2003, “Analog video temelleri”, www.eproje.com
- Daemen J., Rijmen V., 1999, ”AES proposal: rijndel, AES algorithm submission”, <http://www.nist.gov/CryptoToolkit>.
- Ding W., Liu B., 1995, “Rate-Quantization modelling for rate control of MPEG video coding and recording” , SPIE Digital Video Compression
- Ding W., Liu B., 1996, “Rate control of MPEG video coding and recording by rate-quantization modelling”, IEEE Trans. Circuits and Systems-Video Technologies
- Dipçin V., Pazarcı M., 2003, “Görsel bozulmaya dayalı sayısal video şifreleme”, Itu dergisi-Mühendislik, Cilt 2, Sayı 1
- Divakaran A., Sun H., 2000, “A descriptor for spatial distribution of motion activity”, Proc. Storage and Retrieval From Image and Video Databases, San Jose CA
- Drake M., Hoffmann H., Rabbah R., Amarasinghe S., 2006, “MPEG-2 Decoding in stream programming language”, 20th IEEE International Parallel & Distributed Processing Symposium
- Dufaux F., Moscheni F., 1995, ”Motion estimation techniques for digital tv: a review and a new contribution”, Proc. Of IEEE, Vol. 83
- Erol B., Kossentini F., 2000, ”Automatic key video object plane selection using shape information in the MPEG-4 compressed domain”, IEEE Trans. Multimedia
- Eskicioglu A.M., 2003, “Protecting intellectual property in digital multimedia Networks”, IEEE Computer, (Vol. 36, No. 7), 39–45
- Fieury P., Reichel J., Ebrahimi T., 1996, ”Image quality prediction for bit rate allcation”, IEEE International Conferance Image Processing
- Fish M. M., Stögner H., Uhl A., 2004, “Layered encryption techniques for dct-coded visual data”, The European Association for Signal Processing
- Furth B., Socek D., 2003, “Multimedia security : encryption techniques”, IEC Comprehensive Report on Information Security, Chicago
- Furth B., Kirovsky D., 2004, “Multimedia security handbook”, CRC
- Gapalakrishnan S., Reiningner D., 1999, “Realtime MPEG system stream transcoder for heterogeneous Networks”, Packet Video Workshop, New York
- Geman S., Geman D., 1984, ”Stochastic relaxation, gibbs distributions, and the bayesian restoration on images” , IEEE Trans. Pattern Anal. Machine

Gilvarry J., 1999, 'Extraction of Motion Vectors from an MPEG Stream', Technical Report, Dublin City University

Howgrave-Graham N., Nguyen P., Pointcheval D., Proos J., Silverman J.H., Singer A., Whyte W., 2003, "The Impact of Decryption Failures on the Security of NTRU Encryption", Crypto 2003, Santa Barbara

Jack K., 1995, "Video Demystified", LLH Technology Publishing

Khayam S.A., 2003, "The discrete cosine transform (DCT): theory and application", Michigan State University

Kuhn M., 1998, "Analysis of nagravision video scrambling method", <http://www.cl.cam.ac.uk/~mgk25>

Li S., Chen G., 2007, "On the design of perceptual MPEG-video encryption algorithms", IEEE Transactions on Circuits and Systems for Video Technology

Li Y., Chen Z., Tan S., Campbell R. H., 1996, "Security enhanced MPEG player", IEEE First International Workshop on Multimedia Software Development (MMSD'96),

Liu X., Eskicioglu A.M., 2003, "Selective Encryption of Multimedia Content in Distribution Networks: Challenges and New Directions", IASTED International Conference on Communications, Internet and Information Technology (CIIT 2003), Scottsdale

Lookabaugh T., Sicker D.C., Keaton D.M., Guo W.Y., Vedula I., 2003, "Security Analysis of Selectively Encrypted MPEG-2 Streams", Multimedia Systems and Applications VI Conference

Mao Y., Wu M., 2004, "Security evaluation for communication-friendly encryption for multimedia", International Conference on Image Processing (ICIP 2004), Singapore

Maples T.B., Spanos G.A., 1995, "Performance Study Of Selective Encryption Scheme For The Security Of Networked Real-Time Video", 4th International Conference on Computer and Communications, Las Vegas

Markus K., 1998, "Analysis of the nagravision video scrambling method"

Meng J., Chang S., 1995, 'Tools for Compressed Domain Video Indexing and Editing', SPIE Conference on Storage and Retrieval

Meyer J., Gadget F., 1995, "Security Mechanisms for Multimedia Data with the Example MPEG-1 Video", Project Description of SECMPG, Technical University of Berlin

Mitchell J.L., Pennebaker W.B., Fogg C.E., Legal D.J., 1996, "Mpeg Video Compression Standard", Chapman and Hall

- Nemoto Y., Toyota Y., Sakazawa S., Zhao L., Yamamoto H., 2005, "A study on video scrambling considering inter-frame prediction", IEICE Technical Report- Image engineering
- Patel N., Sethi I., 1996, "Compressed Video Processing for Cut Detection", IEE Proceedings - Vision, Image and Signal Processing
- Podesser M., Schmidt H., Uhl A., 2002, "Selective Bitplane Encryption for Secure Transmission of Image Data in Mobile Environments", 5th Nordic Signal Processing Symposium, Hurtigruten, Norway
- Pommer A., Uhl A., 2003, "Selective encryption of wavelet-packet encoded image data", ACM Multimedia Systems
- Qiao L., Nahrstedt K., 1997, "A New Algorithm for MPEG Video Encryption", 1st International Conference on Imaging Science, Systems and Technology (CISST '97)
- Rivest R., Shamir A., Adleman L., 1978, "A method for obtaining digital signatures and public-key cryptosystems", Communications of ACM, ss:120-126.
- RSA Laboratories, 2000, "Frequently asked questions about today's cryptography"
- Seidel T., Socek D., Sramka M., 2004, "Parallel Symmetric Attack on NTRU using Non-Deterministic Lattice Reduction", Designs Codes and Cryptography, Kluwer Academic Publishers
- Shi C., Bhargava B., 1998, "A Fast MPEG Video Encryption Algorithm, 6th International Multimedia Conference, Bristol, U.K.
- Shi C., Wang S., Bhargava B., 1999, "MPEG Video Encryption in Real-Time Using Secret key Cryptography", International Conference on Parallel and Distributed Processing Techniques and Applications (PDPTA '99), Las Vegas
- Spanos G.A., Maples T.B., 1996, "Security for Real-Time MPEG Compressed Video in Distributed Multimedia Applications", Conference on Computers and Communications
- Stinson D.R., 2002, "Cryptography Theory and Practice", CRC Press, Boca Raton, FL
- Tang L., 1996, "Methods for Encrypting and Decrypting MPEG Video Data Efficiently", 4th ACM International Multimedia Conference, Boston,
- Taşkın D., Suçsuz N., 2006, "Sıkıştırılmış ortamda çerçeve tipine dayalı gerçek zamanlı sahne değişimi belirleme", IV. Bilgi teknolojileri Kongresi, Denizli.
- Taşkın D., Taşkın C., Suçsuz N., 2007, "MPEG akımında başlık şifreleme", Akademik Bilişim 2007, Kütahya.

- Taşkın D., Taşkın C., Suçsuz N., 2007, “MPEG akımında operatör işlemlerinin kısıtlanması yoluyla içerik koruma”, Akademik Bilişim 2007, Kütahya.
- Taşkın D., Taşkın C., Suçsuz N., 2007, “Sıkıştırılmış video güvenliği”, e-Journal of New World Sciences Academy, Volume: 2, Number: 3
- Taşkın D., Suçsuz N., Taşkın C., 2007, “MPEG video protection by changing byte alignment”, International Scientific Conference, Smolian, 2007
- Taşkın D., Suçsuz N., Taşkın C., 2007, “MPEG video protection by selective inverting”, International Scientific Conference, Smolian, 2007
- Tosun A. Ş., Feng W., 2000, “Efficient Multi-layer coding and encryption of MPEG video streams”, Multimedia and Expo, ICME 2000
- Van Droogenbroeck M., Benedett R., 2002, “Techniques for a Selective Encryption of Uncompressed and Compressed Images”, Advanced Concepts for Intelligent Vision Systems (ACIVS)
- Van Oorschot P.C., Menezes A.J., Vanstone S.A., 1997, “Handbook of Applied Cryptography”, CRC Press, Boca Raton, FL
- Yılmaz İ., 2002, “Renk Sistemleri, renk uzayları ve dönüşümler”, Selçuk Üniversitesi Jeodezi ve Fotogrametri Mühendisliği Öğretiminde 30. Yıl Sempozyumu, Konya

TEŞEKKÜR

Bu çalışmanın hazırlanmasında bana yol gösteren, destek ve yardımlarını esirgemeyen danışman hocam Yrd. Doç Dr. Nurşen SUÇSUZ'a, çalışmalarımda bana yardımcı olan Yrd. Doç Dr. Cavit TEZCAN, Yrd. Doç. Dr. Seyfettin DALGIÇ ve değerli hocalarıma, çalışma arkadaşlarıma ve aileme teşekkürlerimi sunarım.

ÖZGEÇMİŞ

30.04.1980’de Kırklareli’nde doğdum. İlk eğitimimi Babaeski/Kırklareli’de, orta eğitimimi Kırklareli Anadolu Lisesi’nde, lise eğitimimi Edirne Fen Lisesi’nde tamamladım. 1998-2002 yılları arasında Trakya Üniversitesi Bilgisayar Mühendisliği Bölümü’nde öğrenim gördüm. 2002 yılında Trakya Üniversitesi Fen Bilimleri Enstitüsü Bilgisayar Mühendisliği Anabilim Dalı’nda yüksek lisansa başladım. Aynı yıl Trakya Üniversitesi Mühendislik Mimarlık Fakültesi Bilgisayar Mühendisliği Bölümü’nde araştırma görevlisi olarak çalışmaya başladım. 2004 yılında Trakya Üniversitesi Fen Bilimleri Enstitüsü Bilgisayar Mühendisliği Anabilim Dalı’nda doktora eğitimime başladım. Halen Trakya Üniversitesi Mühendislik Mimarlık Fakültesi Bilgisayar Mühendisliği Bölümü’nde araştırma görevlisi olarak çalışmaktayım.