

Kodlanmış Video Verisinin Gizlilik Gereksinimleri ve Video Şifreleme Algoritmaları

Gül Boztok-Algın, E. Turhan Tunalı

Ege Üniversitesi Uluslararası Bilgisayar Enstitüsü, 35100, Bornova - İzmir
gul.boztok@ege.edu.tr, turhan.tunali@ege.edu.tr

Özet: Günümüz koşullarında, eğlence dünyasından tıbbi çalışmalara kadar birçok alanda kendine yer edinmiş olan kodlanmış video, kullanım alanları genişleyip çoğaldıkça daha çok önem kazanmakta ve içeriğinin güvenliğini sağlamak da başlı başına bir çalışma alanı haline gelmektedir. Gerek boyut gerekse yapısal özellikler bakımından düz metin verisinden farklı olan video verisinin güvenlik gereksinimleri de farklılık göstermektedir. Bu çalışmamızda, video verisinin güvenlik söz konusu olduğunda ortaya çıkan ihtiyaçlarına değinilmiş; üzerinde geliştirilebilecek yöntemlerin tespiti için yapısal özellikleri incelenmiş ve şimdiye kadar yapılmış içerik gizliliğini sağlamaya yönelik çalışmalar listelenmiştir.

Anahtar Kelimeler: Video Sıkıştırma, Video Şifreleme, Çoklu Ortam, Güvenlik.

Security Requirements of Encoded Video Data and Video Encryption Algorithms

Abstract: Encoded video has found application in many fields including entertainment and medical studies. As the number of encoded video applications increase, security of encoded video has become an important research area. Since the size and structural properties of encoded video data is quite different from plain text, its security requirements also considerably differ from that of plaintext. In this study, security requirements of encoded video data are reviewed together with examination of structural properties for development of procedures. A survey of related work is also given.

Keywords: Video Compression, Video Encryption, Multimedia, Security.

1. Giriş

Günümüz koşullarında, çoklu ortam öğelerinin popülerliği artmakta, buna bağlı olarak da çoklu ortam öğelerini kullanan uygulamalar günlük hayatımızda daha çok yer ve önem kazanmaktadır. Bu öğelerden biri olan video verisinin etkin aktarımı için pek çok teknik geliştirilmiştir. Bu tekniklerden beklenen ortak özellik, video verisinin gecikmeye karşı duyarlılığını göz önünde tutarak hızlı kodlama yapabilmeleri, yüksek sıkıştırma oranları sağlayarak verinin boyutunu küçültebilmeleri ve kullanılan bant genişliğine göre uyarlama yapabilmeleridir.

Video verisi aktarımında ortaya çıkan bir diğer ihtiyaç da içerik bilgisinin güvenliğinin sağlanmasıdır. Aktarımı yapılan verinin gönderici-alıcı kimliği doğrulanması yapılması, veriye erişimin tamamen ya da seviyeli olarak engellenmesi ve erişim yetkileri düzenlenmesi gibi ihtiyaçlar var olan tekniklere güvenlik eklemeleri yapılarak sağlanabilir. Bu eklemeler sırasında dikkat edilecek hususlar; video kodlayıcısının kodlama hızını yavaşlatmamak, sağladığı sıkıştırma oranını düşürmemek ve olabildiğince az ek veri kullanarak zaten büyük olan video verisinin boyutunu daha da büyütmemektir.

Bu çalışmamızda amacımız, bahsi geçen konuda şimdiye kadar yapılmış çalışmaları ve üzerinde çalışılan verinin ihtiyaçlarını inceleyerek bir çatı altında toplamaktır. Makalenin genel yapısı şu şekildedir: bölüm 2’de genel olarak video sıkıştırma işleminden ve H.264 SVC kodlayıcısından bahsedilecektir; bölüm 3’te video verisinin şifreleme ihtiyaçlarına değinilecektir; bölüm 4’te şimdiye kadar video verisi üzerinde geliştirilmiş şifreleme yöntemleri incelenecektir; bölüm 5’te ise sonuç ve tartışma yer alacaktır.

2. Video Sıkıştırma ve H.264 SVC Kodlayıcısı

Video sıkıştırma işleminin amacı, veri bütünü içinde fazlalık olarak görülen, kodlanmaması durumunda verinin anlamsal bütünlüğünün bozulmayacağı parçaları video verisinden çıkararak, işlem görecektir toplam veri miktarını ve sonuçta da üretilecek çıktı boyutunu azaltmaktır. Fazlalık olarak adlandırılacak veri üç alanda tanımlanabilir: uzay, zaman ve SNR alanlar.

Video verisindeki piksellerin değerleri birbirlerinden bağımsız değildir. Aralarındaki ilişkiler kullanılarak bir piksel değeri diğerlerinden türetilir. Buradan yola çıkarak, aynı çerçevedeki komşu piksellerin ve komşu çerçevelerdeki ilgili piksellerin birbirleriyle ilişkileri kullanılarak uzaysal ve zamansal alandaki fazlalık verilerin temizlenmesi sağlanabilir. Özel alandaki fazlalıkların atılması ise diğer iki alandan farklı olarak kayıplı bir işlemdir. İnsan gözü, dijital olarak temsil edilebilen her detayı algılayamaz. Bu tarz insan algısı tarafından fark edilemeyen ancak görüntünün kalitesini etkileyen fazlalık veriler işleme tabi tutularak SNR yani kalite alanında sıkıştırma yapılmış olur.

Video kodlama işleminin belli başlı aşamaları sırasıyla: dönüştürme, nicelendirme, sıralama ve entropi kodlama işlemleridir. Dönüştürme işleminde, DCT vb yöntemler kullanılarak video görüntü-sünün piksel bazına düşen değerleri sayısal olarak katsayılarla ifade edi-

lebilecek şekle dönüştürülür. Oluşturulan bu katsayılar, diğerlerinden farklı olarak kayıplı olan nicelendirme işlemine iletilirler. Göze alınan kayıp eşik değerine göre nicelendirme seviyeleri tespit edilir ve elde edilen katsayılar bu seviyelerden sinyali kendine en yakın olana çekilir. Bu işlemin tersi gerçekleştirilirken kaybedilen sinyal seviyelerinin geri onarımı yapılamaz. Nicelendirme işlemi ertesinde genellikle karşılaşılan sonuç, düşük öneme sahip katsayıların sıfıra eşitlenmesi durumudur. Bu sıfır değeri alan katsayıların ard arda gelip kodlama kolaylığı sağlaması amacıyla sıralama işlemi devreye sokulur.

Nicelendirilmiş sıralanmış dönüştürme katsayıları entropi kodlama adı verilen işleme girdi olarak verilir. Entropi kodlama, girdi olarak aldığı verileri olabildiğince küçük boyutlarla temsil edecek şekilde işler. H.264 kodlayıcısı entropi kodlama aşamasında *CAVLC* ve *CABAC* yöntemlerini kullanmaktadır.

H.264 ve benzeri kodlayıcıların özelliği, video kodlaması sırasında hareket tahminleme ve dengeleme mekanizmalarını kullanmalarındır. Bu mekanizmalar, bir çerçevenin içeriğinin, kendinden önce ve/veya sonra kodlanmış/kodlanacak çerçeveleri kullanarak üretilebilmesi üzerine kuruludur. Bu şekilde kodlanan video birimlerine çerçeveler arası kodlanmış blok adı verilir. Tahminleme kullanmadan, hareket-siz resim gibi kodlanmış video birimlerine ise çerçeve içi kodlanmış bloklar adı verilir. Intra kodlanmış çerçevelerde verinin tamamı, inter kodlanmış çerçeveler de ise fark bilgileri kodlayıcıya verilerek sırasıyla yukarıda bahsedilen kodlama aşamalarından geçirilirler.

Kodlayıcı, yapısı içinde bir kod çözücü barındırmaktadır. Bu yapının amacı referans olarak kullanılacak çerçevelerin kod çözücü içinde şifre çözümünü sırasında kullanılacaklarla tamamen aynı olmasını sağlamaktır. Bu yapının kurulmaması durumunda, farklı çerçeveler kullanılarak yapılan tahminlemeler birbirlerinden farklı sonuçlar üreteceğinden kod çözücü tara-

finda elde edilecek video orijinalinden farklı olacaktır ve hata yayılması önlenemeyecektir.

Önceki standart olan MPEG-4 gibi görsel veri üzerinde çalışmasına rağmen, H.264 esneklik-tense etkinlik ve güvenilirliğe daha çok önem verir. Burada etkinlikten kasıt sıkıştırma ve iletim etkinlikleri iken esneklik farklı platformlara uygun veri üretebilme yetisidir.

H.264 ölçeklenebilir video kodlayıcı çalışmaları sonucu *Scalable Video Codec (SVC)* ortaya çıkmıştır. Bu yapıyla kodlayıcı katmanlı yapıya kavuşturulmuş-tur. Ölçeklenebilirlik, var olan kaynakların (ağ genişliği, donanım hızı, vb.) yeterliliği doğrultusunda gönderilecek veri miktarını dolayısıyla gönderilen videonun kalitesini ayarlayabilmek anlamına gelmektedir.

3. Videonun Güvenlik Gereksinimleri

Video verisinin doğası gereği gecikmeye duyarlılığı ve istemcilerin yüksek kalite beklentisinde olması video kodlayıcılarına bir dizi sorumluluk getirdiği gibi içerik gizlemeyi amaçlayan şifreleme algoritmalarına da sağlanması gereken koşullar yaratmaktadır.

Video kodlayıcılarının tasarımı sırasında ön planda tutulan amaç, olabilecek en yüksek kalitede veriyi olabildiğince küçük boyutlarla temsil edebilmektir. Görüntü kalitesinin istemcinin beklentileri doğrultusunda ayarlanması gerekirken, boyut ve aktarım parametreleri de var olan ağ altyapısının ya da depolama mekanizmasının imkanları doğrultusunda uyarlanmalıdır. Bu durum kalite ihtiyacı ve varolan kaynaklar arasında bir denge kurulması gereğini doğurmaktadır. Video kodlayıcıları, bu dengeyi bozmayacak şekilde, kaliteden ödün vermeden, üzerinde çalışılan verinin yapısal ve istatistiki özelliklerini kullanarak toplam dosya boyutunu azaltmaya çalışırlar.

Bir şifreleme algoritmasının, kodlayıcının getirdiği avantajları bozması için sağlaması gereken koşullar aşağıdaki gibidir:

- i. Verinin istatistiki yapısını bozmayarak kodlayıcının sağlayacağı sıkıştırma oranını koruması,
- ii. Hali hazırda çok büyük olan video verisine olabildiğince az eklenti veri katarak dosya boyutunu kontrol altında tutması,
- iii. İstemci tarafında gerçek zamanlı olarak gerçekleştirilen kod çözümü işlemini geciktirmeyecek şekilde hızlı ve düşük karmaşıklıkta, gerçek zamanlı kısıtlarına uygun olarak çalışması,
- iv. Şifre çözme sırasında kullanılacak, gösterim sıraları ile kod çözümü sıraları farklı olan, referans çerçevelere erişimde sıkıntı yaratmayacak bir şifreleme politikası izlemesi,
- v. Özellikle kayıplı sonuç üreten algoritmalar söz konusu ise, kodlayıcı içinde gömülü olan kod çözücü yapısını göz önüne alarak tasarlanmış olması,
- vi. İletimde oluşabilecek hata veya kayıp durumunda verinin zarar görmemiş kısımlarının şifre çözülmesine olanak sağlayacak şekilde senkronizasyon noktaları kullanılarak tasarlanmış olması, tercihen küçük bit hatalarını düzeltebilmesi, hata yayılmasını engellemesi ve kodlayıcının hata düzeltme mekanizmasını bozması,
- vii. İletim sırasında ihtiyaç duyulacak verilere erişimi engellememesi ve ara nodlarda verinin şifre çözülmesini gerektirmemesi,
- viii. Orijinal video kalitesinde düşüşe sebep olmaması,
- ix. Şifreleme birimlerini küçük ve birbirinden bağımsız tutarak sadece istenen bölümlere şifre çözümüleme yapılmasının sağlaması,
- x. İhtiyaç duyulan çeşitli güvenlik seviyelerinde video içeriğini ve hareketlerini gizlemesi.

4. İlgili Çalışmalar

Bölüm 3'te anılan ihtiyaçlar doğrultusunda geliştirilen yöntemlerin kendilerine göre artı ve eksi yönleri bulunmaktadır. Hedef, video verisinin kendine has özelliklerinden faydalanmak yoluyla şifrelemenin etkinliğini artırıp masrafını düşürmektir.

Bu konuda şimdiye kadar yapılmış çalışmalar-
dan literatürde öne çıkmış olanları incelenirse,
video yapısını kullananların yanı sıra videoyu
düz metin verisiymiş gibi ele alan algoritmaların
da varlığı görülür. Bunlardan ilki *Naive Al-
gorithm* adı verilen çalışmadır. MPEG bit akı-
şını, herhangi bir özelliğinden yararlanmadan,
normal metin verisiymiş gibi ele alarak çıkış
akışını DES algoritmasını kullanarak şifreler
[1]. Bu yöntemin performans açısından kötü
sonuç vermesinin sebebi video verisinin çok
büyük olmasıdır. İşlem zamanı ve karmaşıklığı
yüksek olacaktır. Bu şekilde tasarlanan bir diğer
algoritma ise *Random Rotation in Partitioned
Bit Streams* yöntemidir. Son adımında entropi
kodlama yapılan her türlü sıkıştırılmış çoklu
ortam bit akışına uygulanabileceği söylenen
yöntem, çıktı verisini rasgele uzunluklarda par-
çalara bölerek, her parçaya kendi içinde rasgele
sayıda rotasyon uygulamaktan ibarettir [15].

Şifrelenecek veri miktarını azaltmak isten-
diğinde, video verisinin yapısal özelliklerini
kullanmak faydalı olacaktır. Bu doğrultuda
yapılan çalışmalar genel olarak “seçimli şif-
reme” algoritmaları (*selective encryption*)
olarak anılabilir [9]. Bu yöntemlerden ilki I, P
ve B tipi çerçevelerin birbirlerini referans al-
malarına dayanarak sadece I tipi çerçevelerin
üzerinde kurulmuştur [7]. Daha sonra yapılan
çalışmalarla da kanıtlandığı üzere bu yöntem
yeterli seviyede gizlilik sağlamamaktadır. Bu-
nun asıl sebebi P ve B tipi çerçevelerin içinde
şifrelenmemiş olarak kalan I kodlanmış blokla-
rın varlığıdır [1]. Görülen bu açıkları gidermek
adına önerilen yöntemlerden biri, I kodlanmış
çerçevelerin yanı sıra P ve B tipi çerçevelerin
içindeki I kodlanmış blokların da şifrelenmesi-
dir. Bir diğer yöntem ise, şifrelenmesi önerilen
bu alanlara ek olarak P ve B tipi çerçevelerin
başlık bilgilerinin de şifrelenmesini uygun gö-
rür. Her iki yöntemde de seçilen alanlar DES
algoritması kullanılarak şifrelenmiştir [2].
Aynı grubun ilerleyen çalışmalarında üç yeni
seçimli şifreleme yöntemi geliştirilmiştir. Bun-
ların ilki her I blok yerine her *n.inci* I bloğun
şifrelenmesini; ikincisi tahminlenen (P ve B)

makroblokların başlık bilgileri ile *n.inci* I mak-
robloğun video verilerinin şifrelenme-sini; so-
nuncusu ise *n.inci* I makrobloğu video verileri
ile *n.inci* tahminlenen makrobloğun başlık bil-
gilerinin şifrelenmesini önerir. Bu yöntemlerin
işlem maliyetlerinin diğerlerine göre daha az
olduğu öne sürülmektedir. Yine şifreleme algo-
rması olarak DES kullanılmaktadır [3].

Önerilen bir başka seçimli şifreleme yöntemi
“SEC-MPEG” adı verilen yöntemdir. Şifrele-
necek veri alanları istenen gizlilik seviyesine
göre değişiklik göstermektedir. Yöntem DES
ve RSA algoritmalarını kullanarak güvenilirli-
ği sağlar. Seçilebilecek 4 güvenlik seviyesine
göre şifrelenen alanlar sırasıyla şu şekildedir:
1)Tüm başlık bilgileri, 2)Tüm başlık bilgileri,
DC katsayıları ve I blokların düşük frekanslı
AC katsayıları, 3) I tipi çerçeveler ve P ve B
tipi çerçevelerin içerdiği I kodlanmış bloklar,
4) Tüm video verisi. İçerik bütünlüğü ise CRC
kullanılarak kontrol edilir [8].

Uygulama karmaşıklığı düşük bir yöntem ola-
rak geliştirilen *Zig Zag Permutation Algorithm*,
entropi kodlamadan önce transformasyon kat-
sayılarının sıralanması aşamasında uygulanan
zig zag sıralama yerine rasgele sıralamalar
yapmak suretiyle gerçekleştirilir. Algoritma,
uygulanan rasgele sıralama listesini anahtar
veri olarak kullanır. Bu çalışma için yapılmış
iyileştirme çabaları içinde, diğer katsayılarla
göre daha belirgin olan DC katsayısını sakla-
maya yönelik girişimler görülmektedir [12].

MPEG üzerinde yapılmış bir başka şifreleme
çalışması da “*Video Encryption Algorithm*”
(VEA)’dir. Sadece Intra kodlanmış çerçeveler
üzerinde dilim seviyesinde byte-byte çalışan
algoritma, veriyi tek sayılılar ve çift sayılılar
olmak üzere iki akış haline ayırmaktadır. Her
iki akışı birbiriyle XORlamak suretiyle bir tür
“tek kez kullanılan şifreleme” işlemi yapmış
olur. Buna ek olarak çift sıra numaralı byteların
oluşturduğu akışı DES’den geçirerek çıktı ve-
risinin ikinci bölümünü de yaratmaktadır. Böy-
lece DES’den geçecek veri miktarı azaltılır.

Ancak bilinen metinlerle şifre kırma saldırısı yapıldığı takdirde bu yöntemin zayıf kalacağı kanıtlanmış ve iyileştirme çalışmaları dahilinde anahtarlı versiyonlar geliştirilmiştir [9]. Aynı grubun, çalışmaları sırasında bulunduğu video verisine ait istatistikî bilgiler doğrultusunda geliştirdiği bir diğer yöntem "sade karıştırma" (*Pure Premutation*) yöntemidir. Video verisinin byte desenlerinde ikili tekrarları-na çok seyrek rastlanmasından yola çıkılarak bytelerin rasgele permütasyon işlemine sokulmasının yeterli güvenliği getireceği düşünülmüştür ancak bu yöntemin bilinen metin saldırısına karşı zayıf olacağı açıktır [9].

DCT katsayıları ile çalışan bir başka yöntem olan *Scalable Partial Encryption* yönteminde ise bir n parametre değeri seçilerek ard arda gelen video veri bloklarının ilk n katsayısının şifrenmesi sağlanmaktadır. Yöntem DCT katsayıları-nın azalan önem seviyesinde sıralanması gerçeği üzerine kurulmuştur. Hareket tahminleme problemlerine karşı güçlü olduğu söylenen bu yöntemin JPEG tabanlı tüm video sıkıştırma algoritma-larında uygulanabileceği belirtilmiştir. [5]

Ölçeklenebilir video kodlayıcıları için tasarlanan şifreleme yöntemlerinde düşülen genel bir yanlış da, aynı Intra kodlanmış çerçeveleri şifrelemenin yeterli olacağını düşünülmesi gibi, sadece temel katman verilerinin şifrenmesinin yeterli olacağı düşüncesidir. Bu şekilde şifrelenmiş bir video şifre çözümü yapılmadan izlendiğinde görüntü içindeki objelerin ana hatlarıyla belirgin olarak seçilebildiği görülmüştür. Bizim çalışmamız da bu tespiti doğrular sonuçlar üretmiştir. Bu durumu önlemek için önerilen yöntem, temel katmanı ihtiyaca bağlı olarak seçimli ya da tümünden şifrelemek, geliştirme katmanlarını ise seçimli olarak şifreleme işlemine tabi tutmak yönündedir. [16]

MPEG video şifreleme üzerine çalışan bir başka grubun önerdiği bir dizi algoritma bu alandaki çalışmalar arasında önemli yer tutmaktadır [4]. *Algorithm 1* isimli ilk algorit-

malarında, standartta kullanılan Huffman tablosu yerine gizli anahtar görevi de görececek başka bir tablo kullanarak gizliliği sağlamayı amaçlamışlardır. Ancak üretilecek her tablo istenilen sıkıştırma oranını sağlamayacağı için anahtar uzayının sınırlı kalması yöntemi zayıf kılar [4]. Bu zayıflığın üzerine grup *VEA* adını verdikleri diğer algoritmalarını geliştirmişlerdir. Algoritma DC ve AC katsayıları üzerinde gizli anahtar uyarınca işaret değiştirme işlemi yapmaktadır. Algoritma video akışı üzerinde senkronizasyon noktaları yaratmaktadır. Bu alanlar gizli anahtarın ilk bitinden itibaren tekrar kullanılmaya başlandığı noktalardır. Senkronizasyon noktalarının faydası, ağdan kaynaklanan kayıp ve gürültü durumunda sağlam kalan video parçalarının şifrelerinin çözülebilmemesini mümkün kılmasıdır. Benzer şekilde ileri/geri hızlı sarmalarda ya da videonun sadece belirli parçalarının şifresinin çözülmesi istendiğinde de bu noktalardan yararlanılacaktır. Belirtilen sakıncalara çözümler; uzun anahtar kullanılması, anahtarın sıkça değiştirilmesi ve başlık verilerinin, tahmin edilebilirliğinden dolayı, şifrenmemesidir. [4]

Geliştirilen üçüncü algoritma VEA algoritmasının değiştirilmiş bir versiyonu olan *MVEA (Modified VEA)* algoritmasıdır. Çalışmada, I bloklara ait DC katsayılarının yanı sıra B ve P çerçevelerine ait hareket vektörlerinin de işaret bitlerinin değiştirilmesi önerilmektedir. Yine her GOP'un başlangıcı senkronizasyon noktası olarak işaretlenir. Elde ettikleri sonuçlara göre, hareket vektörlerinin diferansiyel kodlanması, işaret bitlerindeki değişimin vektörün yönüyle birlikte büyüklüğünü de etkilemesine sebep olmaktadır ve bu sebeple hareket vektörlerinin şifrenmesi yeterince güçlü bir gizlilik sağladığından B ve P çerçevelere ait DCT katsayılarının şifrenmesini gereksiz kılmaktadır. Algoritmada, VEA'den farklı olarak sadece I bloklara ait DC katsayıları şifrenmektedir. Bunun sebebi video verisi açısından DC katsayılarının AC'lere göre daha etkili olmasıdır. Ancak aralarındaki ilişkiden dolayı AC katsayıları kullanılarak DC katsayısının

elde edilebi-leceği düşünülürse, yüksek önem taşıyan videolarda ilk birkaç AC katsayısının da şifrelemeye tabi tutulması önerilir [4].

Önerilen dördüncü yöntem *RVEA (Robust VEA)* adı verilen diğer iki çalışmanın üzerine geliştirilmiş bir algoritmadır. Diğer iki algoritmanın bilinen metin saldırısına açık olması sebebiyle bu yöntem geliştirilmiştir. Yine MPEG kodlanmış video verilerinin DCT ve hareket vektörleri işaret bitleri üzerinde gizli anahtar kullanarak çalışan algoritma seçilen bu alanları şifrelemek için herhangi bir şifreleme algoritmasını (ör. DES, IDEA) kullanabilmektedir. Dilimler bazında çalışan RVEA, her makrobloktan önem sırasına göre en fazla 64 işaret biti seçerek bunları şifreleme algoritmasından (ör. DES, IDEA) geçirdikten sonra orijinal yerlerine geri yerleştirir.

İşaret biti seçme aşamasında önem sırası DC katsayılarının AC katsayılarına göre ve parlaklık bloklarının krominans bloklarına göre daha etkili olmaları üzerine kurulur. RVEA algoritmasının kırılma zorluğunun alt planda kullanılan şifreleme algoritmasının kırılma zorluğuna eşit olduğu öne sürülmektedir [4].

Aynı gruba ait bir başka çalışma olan *PVEA (Perceptual Video Encryption Algorithm)* yine seçimli olarak video verisinin sabit uzunluklu kodlarını (*FLC*) şifrelemek üzerine kuruludur. Değişken uzunluklu kod (*VLC*) elemanlarını şifrelemenin, sıkıştırma etkinliğini bozma riski çok yüksek olduğu için FLC elemanlarının seçildiği söylenmektedir. Çalışmalar süresince:

- i. *Intra DC katsayılarının* 8x8 blok seviyesinde videonun genel görüntü bilgisini taşıdığı bu sebeple şifrenmesinin düşük çözünürlükte genel görüntüyü etkileyeceği,
- ii. *AC ve Inter DC katsayılarının işaret bitlerinin* ve *ESCAPE DCT katsayılarının* videonun 8x8 bloklarında detayları temsil ettiği ve şifrenmesinin yüksek çözünürlükte detayları etkileyeceği,

- iii. *Hareket vektörlerinin değerleri* ve *işaret bitlerinin* hareket bilgilerini içeren görsel kaliteyi temsil ettiği ve şifrenmesinin zamansal hareketi etkileyeceği,

gözlemlenmiş ve algoritma bu üç başlık altında toplanmış anılan FLC elemanların üzerine kurulmuştur. İstenen çeşitli gizlilik seviyelerine karşılık verebilmek için bu alanlar değişik oranlarda şifrelenir [6].

Bütün bu algoritmaların etkin sonuç vermesinin sebeplerinden biri de üzerinde çalışılan işaret bitlerinin toplam video verisinin %10'u civarında olmasıdır [4].

Entropi kodlama sırasında kullanılan Huffman tabloları üzerine geliştirilen bir diğer şifreleme algoritması da *Multiple Huffman Tables (MHT)* yöntemidir. Temel algoritma, entropi kodlama aşamasında kullanılacak birden fazla Huffman tablosu oluşturmak ve bu tabloları değişik sıralarla her sembol için kullanmaktan ibaret. Bu yöntemde gizli tutulacak bilgiler: oluşturulan Huffman tabloları ve bu tabloların kullanılış sıralarıdır. Buradaki önemli nokta kullanılacak Huffman tablolarının sıkıştırma oranını bozmayacak şekilde uygun tablolar olmasıdır. Bunu da sağlamanın yolu her tabloyu genel resim özelliklerini bünyesinde barındıran değişik resim kümelerine uygun olacak şekilde üretmektir. Böylece her tablo birbirinden farklı olurken sıkıştırma açısından eşit uygunlukta olacaktır [14].

MHT yönteminde kullanılacak çok sayıda etkili Huffman tablosu üretme süreci zahmetli olacağından az sayıda tablo üretip bunları mutasyona uğratarak istenen sayıda tablo yaratma fikri ortaya atılmıştır [14]. Yine MHT yönteminin geliştiricileri tarafından ortaya atılan bu yöntem *Huffman Tree Mutation* olarak adlandırılmaktadır. Yöntem dahilinde genel resimlere uygun olabilecek 4 tablo ürettiklerini ve bu örnekleri mutasyona sokarak yeterli sayıda tablo elde edebildiklerini öne süren grup, ağacın ara nodlarına ait etiketleri verilen bir

tam sayı anahtarın bit değerlerine bağlı kalarak rasgele değiştirmektedir. Birden çok tablo kullanılması toplam kod uzunluğunda büyük farklılıklara sebep olmazken, farklı tabloların bir sembol için farklı uzunluklarda kod üretibilmesi semboller arası senkronizasyon sorunu yaratacağın-dan sadece şifrelenmiş metin saldırısı yaparak sembollerin tahminlemesini güçleştirecektir [14].

5. Sonuç

Bu çalışmada, bir çoklu ortam ögesi olan video verisinin yapısal özelliklerine değinilerek, veriye özel bir şifreleme algoritmasının yerine getirmesi gereken koşullar incelenmiştir. Video verisi içeriğini gizleme ve güvenliğini sağlamaya yönelik yapılan çalışmalar alınmıştır.

Şimdiye kadar bahsettiğimiz gereksinimler doğrultusunda, video verisinin içeriğini yeterli düzeyde gizleyen bir algoritma geliştirmiş durumdayız. Seçimli bir şifreleme yöntemi öneren ve ölçeklenebilir video yapısının özelliklerini kullanan algoritmamıza ait yöntem ve detaylı başarımlarını sonuçları [17]'de rapor edilmiştir.

6. Kaynaklar

[1] Agi, I., Gong, L., "An Emprical Study of MPEG Video Transmissions", *Proc. Internet Society Symposium on Network and Distributed System Security*, s. 137-144, San Diego, CA, (1996).

[2] Alattar, A.M., Al-Regib, G.I., "Evaluation of Selective Encryption Techniques for Secure Transmission of MPEG-Compressed Bit-Stream", *Proc. of the IEEE Int'l Symposium on Circuits and Systems*, Orlando, Florida, (1999).

[3] Alattar, A.M., Al-Regib, G.I., Al-Semari, S.A., "Improved Selective Encryption Techniques for Secure Transmission of MPEG Video Bit-Streams", *Proc. Int'l Conference on Image Processing (ICIP'99)*, (1999).

[4] Bhargava, B., Shi, C., Wang, S.-Y., "MPEG Video Encryption Algorithms", *Multimedia Tools and Applications*, vol. 24 no.1 s.57-79, (2004).

[5] Kunkelmann, T., Reinema, R., "A Scalable Security Architecture for Multimedia Communication Standards", *Proc. 4th IEEE Int'l Conference on Multimedia Computing and Systems*, Ottawa, Kanada, (1997).

[6] Li, S., Chen, G., Cheung, A., Bhargava, B., "On The Design of Perceptual MPEG-Video Encryption Algorithms", Cornell University Library, arXiv e-print, cs.MM/0501014, <http://arxiv.org/abs/cs.MM/0501014>, (2005).

[7] Maples, T.B., Spanos, G.A., "Performance Study of a Selective Encryption Scheme for the Security of Networked Real-time Video", *Proc. 4th Int'l Conference on Computer and Communications*, Las Vegas, NV, (1995).

[8] Meyer, J., Gadegast, F., "Security Mechanisms for Multimedia Data with the Example MPEG-1 Video", <http://www.gadegast.de/frank/doc/secmeng.pdf>, (1995).

[9] Qiao, L., Nahrstedt, K., "Comparison of MPEG Encryption Algorithms", *Int'l Journal on Computer & Graphics, Special Issue on Data Security in Image Communication and Network*, (1998).

[10] Reichel, J., Schwarz, H., Wien, M., "Joint Scalable Video Model JSVM-6 Draft Output Document from JVT", http://ftp3.itu.org/av-arch/jvt-site/2006_04_Geneva/JVT-S202.zip, JVT 19th Meeting, Geneva, İsviçre, (Nisan 2006).

[11] Richardson, I.E.G., *H.264 and MPEG-4 Video Compression*, Wiley Yayınları, 2003.

[12] Tang, L., "Methods for Encrypting and Decrypting MPEG Video Data Efficiently", *Proc. ACM Int'l Multimedia Conference*, Boston, MA, 1996.

[13] Wiegand, T., Sullivan, G. J., Bjontegaard, G., Luthra, A., ‘Overview of the H.264 / AVC Video Coding Standard’, *IEEE Transactions on Circuits and Systems for Video Technology*, July 2003.

[14] Wu, C.-P., Kuo, C.-C. J., “Design of Integrated Multimedia Compression and Encryption Systems”, *IEEE Transactions on Multimedia*, vol.7 no.5 s.828-839, Ekim 2005.

[15] Xie, D., Kuo, C.C.J., “Multimedia Data Encryption via Random Rotation in Partitioned Bit Streams”, *Int’l Symposium on Circuits and Systems*, Kobe, Japonya, 23-26 Mayıs 2005.

[16] Yuan, C., Zhu, B.B., Wang, Y., Li, S., Zhong Y., “Efficient and Fully Scalable Encryption for MPEG-4 FGS”, *Proc. IEEE Int’l Symposium on Circuits and Systems*, vol.2 s.620-623, Mayıs 2003.

[17] Boztok Algın, G., and Tunalı, T., “Ölçeklenebilir .264 Video Kodlayıcısı İçin Seviyelenendirilebilir Güvenlik Sağlayan Bir Video Şifreleme Çalışması”, Ege Üniversitesi Fen Bilimleri Enstitüsü Yüksek Lisans Tezi, (2007).