

# GÜVENLİK TEKNOLOJİLERİ NEREYE GİDİYOR

**Tarık YILDIZ**

tarikyildiz@tekofaks.com.tr

TEKOFAKS A.Ş.

Gürsel Mah. Sevilen Sok. No:65 Kağıthane/İstanbul

Tel: 0212-210-69-00 (211)

## ÖZET

*Bugünün dünyasında gelişen ve değişen güvenlik gereksinimleri , gerek akademik çevreleri, gerekse de endüstri aktörlerini ,daha yüksek çözünürlüklü video temin , bu videonun çoklu alıcılara daha dar bant genişlikleriyle iletimi ve iletilen video üzerinde yapay öğrenme bazlı içerik analiz yöntemleri geliştirmeye zorluyor.*

CCTV teknolojileri endüstrisinde 1996 yılı itibariyle ilkel örnekleri, 2000 yılı başları itibariyle daha gelişmiş örnekleri, dijital video sinyali üretebilen kameralar olarak ortaya çıkan “Network ağları üzerinden takip ve kumanda edilebilen” güvenlik amaçlı görüntü teknolojisi, başlarda TCP/IP Protokolü üzerinden lokal bir ağın (LAN) ya da geniş alan bir ağın (WAN) herhangi iki noktası arasında güvenlik görüntüleri iletişiminin kolaylıkla sağlanabilmesini amaçlarken (1), günümüzde dijital video sinyali konsepti çerçevesi içinde megapiksel çözünürlüğün artırılarak geliştirilmesinin öncül amaç haline geldiğini görülmektedir. 2008 yılı içerisinde 5,8 ve nihayetinde 10 megapiksel dijital video network güvenlik kameralarının lansmanlarına tanık olunmuştur. Bugün hemen hepimizin hayatına giren, digital fotoğraf makineleri ve cep telefonları ile 1,3-10 Megapiksel aralığında çözünürlük ifade eden değerleri sıkça duyulmaya başlanmıştır.

Dijital video çözünürlüğünün, görüntüleme çerçevesinin piksel bazında sabit kaldığı halde, bu çerçeve içerisinde beslenen dijital video sinyalinin çözünürlüğü arttıkça, görüntü üzerindeki daha ince detayların daha keskin görülebilir hale geldiğini, elde edilen görüntünün birkaç kademe optik olarak yakınlaştırılması durumunda bile, görüntüyü oluşturan en küçük birim olan

piksellerin gözle fark edilir hale gelmediğini görüyoruz.



Konvansiyonel görüntüleme teknolojileri ile TV standartlarına uygun olarak üretilen 752x582 piksel çözünürlüğüne sahip görüntünün (yaklaşık 0,44 MP), bugün averaj standart haline gelen 1280x960 piksel çözünürlük boyutlarına sahip bir monitör üzerinde ancak yatay ve dikey olarak kopyalanarak sunulabildiğini, bu nedenle, optik yakınlaştırma yapılmadan bile görüntü üzerinde piksellerin belirgin hale geldiğini, dolayısıyla güvenlik açısından ince detayların kaybedildiğini görmekteyiz. Aynı 1280x960 piksel çözünürlüklü monitörde, 2592x1944 (yaklaşık 5MP) çözünürlük boyutlarında görüntü sinyali ile beslendiğini düşündüğümüzde ise yatayda ve dikeyde görüntü optik olarak 2 kat yakınlaştırılsa dahi hiçbir bozulma yada piksellerin ortaya çıkmasından kaynaklanan minimal karecikler belirmeksizin en ince detayların fark edilir olması sağlanabilmektedir (2).



Bugün konvansiyonel güvenlik teknolojilerini ile üretilen görüntü sinyallerinden elde edilen kayıt görüntüleri çözünürlük gereksinimleri sebebiyle ihtiyacı karşılayamaz hale gelmiştir. Güvenlik endüstrisinin lider üreticileri tüm ar&ge yatırımlarını daha yüksek çözünürlüklü dijital video sinyali üretimi üzerine yoğunlaştırdıklarını görüyoruz. Elde edilen çok yüksek band genişlikli sinyallerin (>10Mbit/s) ileri kodlama ve sıkıştırma yöntemleri ile daha düşük band genişliklerinde iletilebilmesi ve uç ünitelerde yüksek çözünürlükler ile kaydedilebilmesi ar/ge çalışmalarının en önemli hedefi olarak ortaya çıkıyor. Bunun belki de doğal bir sonucu olarak hybrid (MPEG iletim / JPEG kayıt) sıkıştırma metodu içeren kameralar da 2002 yılı itibariyle gerçek zamanlı sıkıştırma ve iletim amaçlı olarak denenmeye başlandılar (3). 2010 yılı sonu itibariyle 10-20 Mpiksel aralığında güvenlik kameralarının tanıtımlarını, bugün bilindik MPEG2-4 ve H264 gibi kodlama teknolojilerinin yerlerini, matematik modelleri 2004 sonları itibari ile başlanan ve günümüzde gerçek zamanlı testleri süren MPEG7, Theora, LZH vb başka teknolojilere aktardığını görmeye başlayacağız (4).

Böylelikle genellikle hollywood yapımı polisiye filmlerinde gördüğümüz kayıtlı görüntü üzerinde çok küçük bir ayrıntı çerçevesinin hiç bozulmadan 10-20 kademe optik yakınlştırılabilirdiği sahneler (hala hazırda yüksek çözünürlüklü broad-cast kameraların görüntülerinin, prodüksiyon hileleriyle kullanılması sayesinde bu görsellik sağlanmaktadır.), 2011 yılı itibariyle evlerimizin, işyerlerimizin ve

kurumlarımızın güvenliğinde kullandığımız cihazlarla hayatımıza girmeye başlayacak.



Network güvenlik teknolojisi, 11 Eylül'den sonra gelişen dönemde gelişen güvenlik anlayışı ve ihtiyaçların uygulama bazlı olarak daha da çeşitlenmesi ile birlikte sistem esnekliği ve yazılımsal algoritmalar ile desteklenme imkanları kısıtlı olan konvansiyonel güvenlik anlayışının yerini daha büyüyen bir ivme ile doldurmaya başladı. Konvansiyonel güvenlik teknolojisine nazaran, PC/Server düzlemlerine kolaylıkla aktarılabilir olması ve gelişen bilişim olanaklarıyla birlikte dijital video işlenebilir hale geldi. Günümüzdeki örneklerinde de görebileceğimiz, görüntü üzerinde korunan alanlar ve korunan alanlar arasında öncelik alanları oluşturabilmek, bazı alanları tamamiyle güvenlik önceliğinden çıkarabilmek, bu alanlardaki insani veya nesnel aktivasyonların tespit edebilmek artık sıradan yazılımsal özellikler olarak değerlendiriliyor. Kullanılan kameraların çözünürlüklerine bağlı olarak ışık şiddeti oldukça düşük ortamlarda, insan gözüyle fark edilmesi çok zor olan hareketliliğin tespiti ve görüntü üzerinde bu hareketliliğin farklı kontrastta veya renkte çizgiler ile takibi, normal trafik akışı veya park usul ve doğrultularına ters hareketliliğin tespiti, AVM lerde kaygan zeminde düşen insanların tespitine müteakip tehlikeli alan bildirimini, kapalı ve açık alanlarda sonradan bırakılan şüpheli paketlerin tespiti, kapalı ve açık alanlarda nesnelere kayıp / çalıntı tespiti, korunan alanda yangın durumunun tespiti, kapalı bir alana giren insan adetinin tespiti (özellikle AVM lerde) ve aniden aşırı derecede hızlanan insan ve araçların tespiti

gibi yazılımsal araçlar ise performans bakımından gelişim aşamasında sayılabilir.

Yazılımsal araçların sayılarındaki ve çeşitliliklerindeki artış, daha evvel aynı anda belki yüzlerce kamera görüntüsünü takip etmekte olan operatörlerin dikkat kabiliyetlerine olan bağımlılığı azalttı. Böylece her türlü yazılımsal araçla tespit edilen anormal durum otomatik olarak sesli ve görsel araçlarla operatör dikkatine sunulduğu gibi, daha üst seviye idarecilere de email yada telefon mesajlarıyla anormal durum alarm bildirimini otomatik olarak gerçekleştirilmeye başlandı. Network kamera teknolojisindeki çözünürlüğe bağlı gelişime paralel olarak, “anormal” olarak değerlendirilen aktivitelerin tespit edilebildiği minimum video alanı için bazı endüstriyel aktörler, kayıp çalıntı obje tespitinde aşgari 4x4, şüpheli nesne analizi için ise 10x10 piksellik video alanlarına kadar indirgediklerini iddia etmektedir (5).

Ancak bugün hala üretilen sonuçların doğruluk sıklığı (MTBF) bakımından kabul edilebilir ortalama görüntü alanı 30 \* 30 piksel olarak gösterilmektedir (6).



Bu yazılımsal araçların ters yönde hareketlilik, tehlikeli alan, kayıp/çalıntı ve şüpheli paket tespiti gibi dallarında basit düzeyde dahi olsa artificial neural network (“yapay sinir ağları”, “yapay zeka”), fuzzy membership matrices (bulanık üyelik fonksiyonu matrisi) vb modellemelerinin kullanılması, bu alandaki çalışmaların orta vadede operatör takibini tamamiyle ortadan kaldırabilecek şekilde otomatik tespit edebilecek ve önceden tanımlanan aksiyonları yürütebilecek yazılım platform-

larının geliştirileceği yönünde beklentileri artırmıştır. Hala hazırdaki yapay zeka algoritmaları ile düşük ve orta düzeydeki hareketliliğe sahip ortamlarda performansı, çözünürlük ve ortam ışığının homojenitesiyle doğru orantılı olarak yapay öğrenme gerçekleştirilebilmekte ve öğrenilen, hafızaya alınan görüntünün normal hali ile uyuşmayan anomali tespit edilebilmektedir. Yapılan tespitlerde toplam görüntü kalitesine veya görüntü üzerindeki toplam kompleksiteye bağımlı hataların da ayrıca tespiti ve müteakip tespitlerde hatanın tekrar edilmemesine yönelik “geri beslenebilen” daha üst düzey algoritmaların kullanımı bu yazılımsal araç uygulamalarındaki hataları da azaltacaktır (7).

## KAYNAKLAR

- (1) Douglas M. Grant MCSE SecurityWorld 2002
- (2) Sean A. Ahrens, CPP, CSC, Commercial Real Estate Council of ASIS International Facilitiesnet 2007
- (3) Zhezhou Yu; Yuchen Xie; Congying Lv; Chunguang Zhou; Faner Meng; Lei Liu - IEEE Transactions on Hybrid Information Technology, 2006
- (4) Takayuki Nishi, Chubu University - IEEE Transactions on Object-Based Video Coding Using Pikel State Analysis ,2004
- (5) Vista Scape Site IQ/ [www.buildingtechnologies.siemens.com/press/press\\_release/subchannel\\_press](http://www.buildingtechnologies.siemens.com/press/press_release/subchannel_press)
- (6) Dr. Dmitry Gorodnichy Video Technology for security, Rail and Urban Transit Security Workshop Montreal November 2007
- (7) L. Li, - IEEE Transactions on “Statistical Modeling of Complex Backgrounds for Fore-ground Object Detection” Image Processing 2004,

## FOTOĞRAFLAR

WV-NP304 – WJ-NT314 / I-Pro Series/2008/www.panasonic.net