KODLANMIŞ VİDEO VERİSİNİN GİZLİLİK GEREKSİNİMLERİ VE VİDEO ŞİFRELEME ALGORİTMALARI

Gül BOZTOK ALGIN

E. Turhan TUNALI

İçerik

- Video Sıkıştırma
- H.264 Kodlayıcısı
- Video Verisinin Güvenlik Gereksinimleri
- İlgili Çalışmalar
- Sonuç

Giriş

Video verisinin kullanım alanları genişledikçe ihtiyaçları da farklılaşmaktadır. İçerik gizliliğinin sağlanması da bu ihtiyaçlardan biridir.

Bu çalışmamızda amacımız, bahsi geçen konuda şimdiye kadar yapılmış çalışmaları ve üzerinde çalışılan verinin ihtiyaçlarını inceleyerek bir çatı altında toplamaktır.

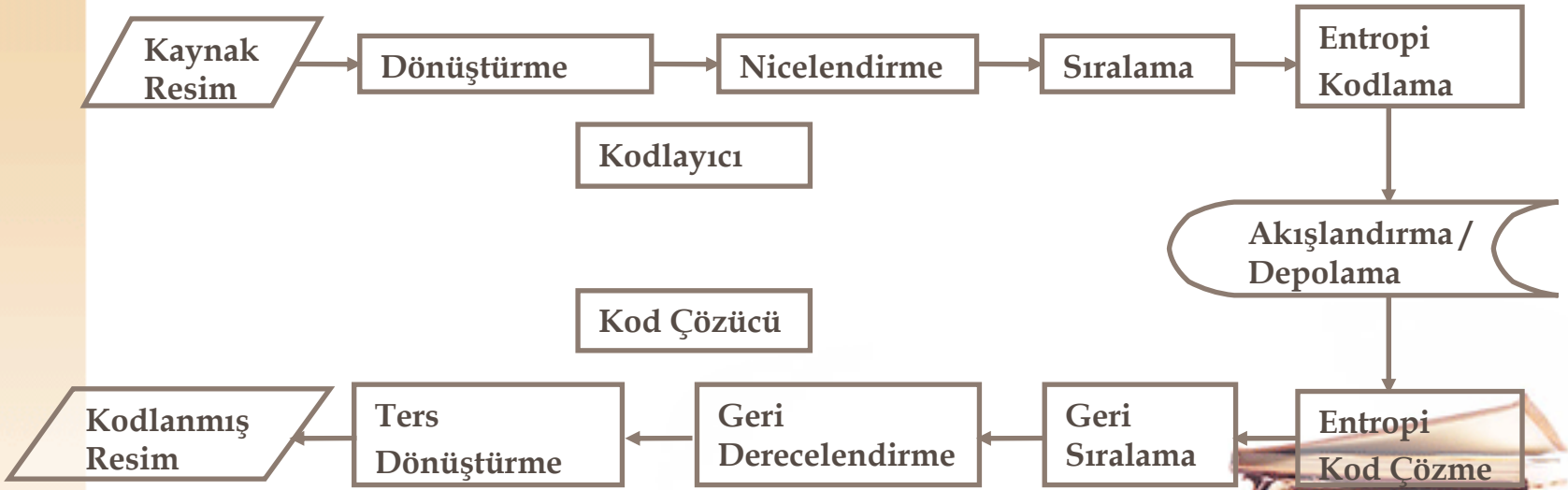
Video Sıkıştırma ve H.264

Video sıkıştırma (*compression*) işleminin amacı, fazlalık olarak görülen, kodlanmaması verinin bütünlüğünü bozmayacak parçaları çıkartarak, işlem görecek toplam veri miktarını ve üretilecek çıktı boyutunu azaltmaktır

Fazlalık olarak adlandırılabilecek veri üç alanda ele alınabilir:

- Uzay (*spatial*) alan
- Zaman (*temporal*) alan
- SNR alan

Video Sıkıştırma ve H.264 (devam)



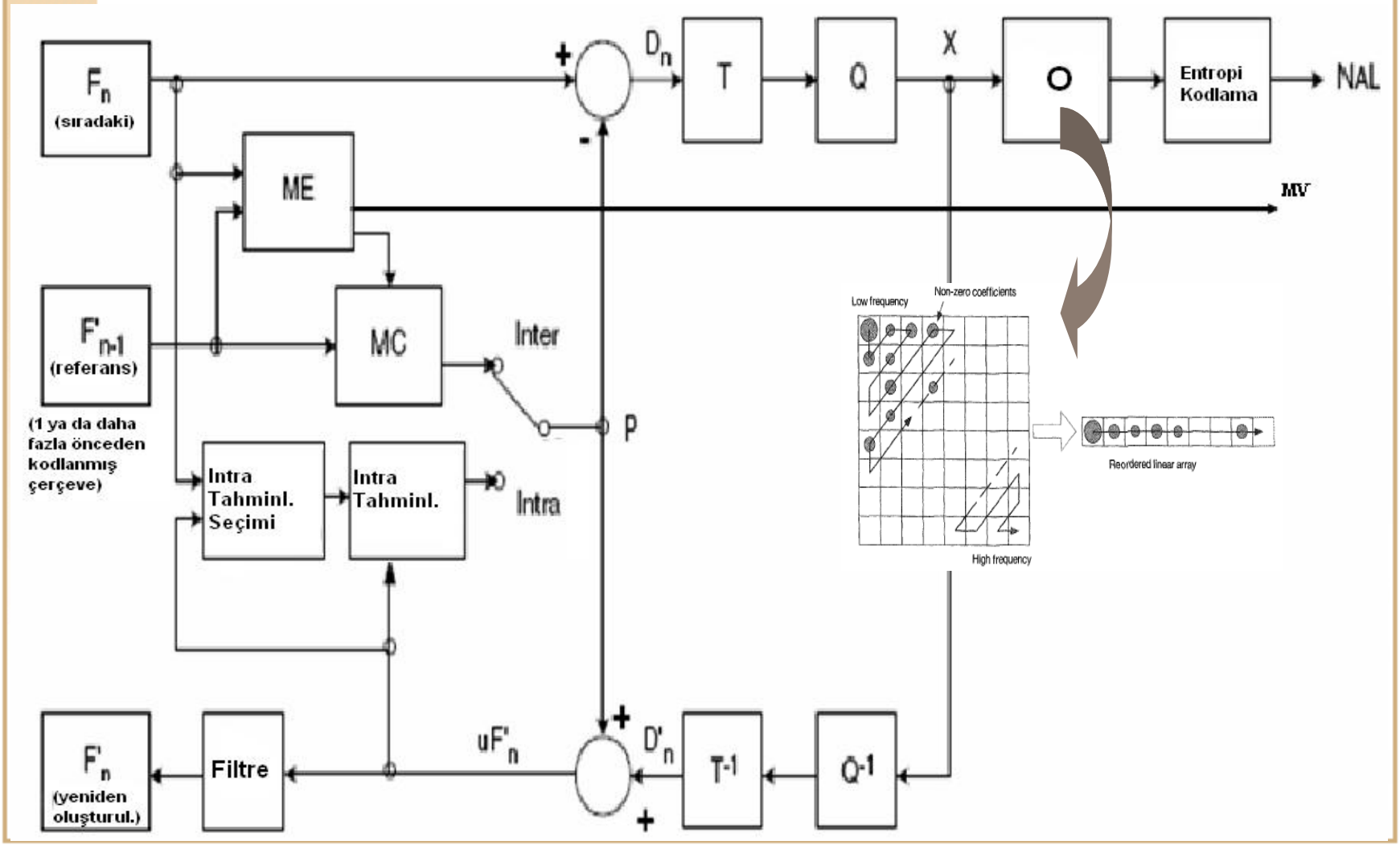
Dönüştürme : *Transformation*

Nicelendirme : *Quantization*

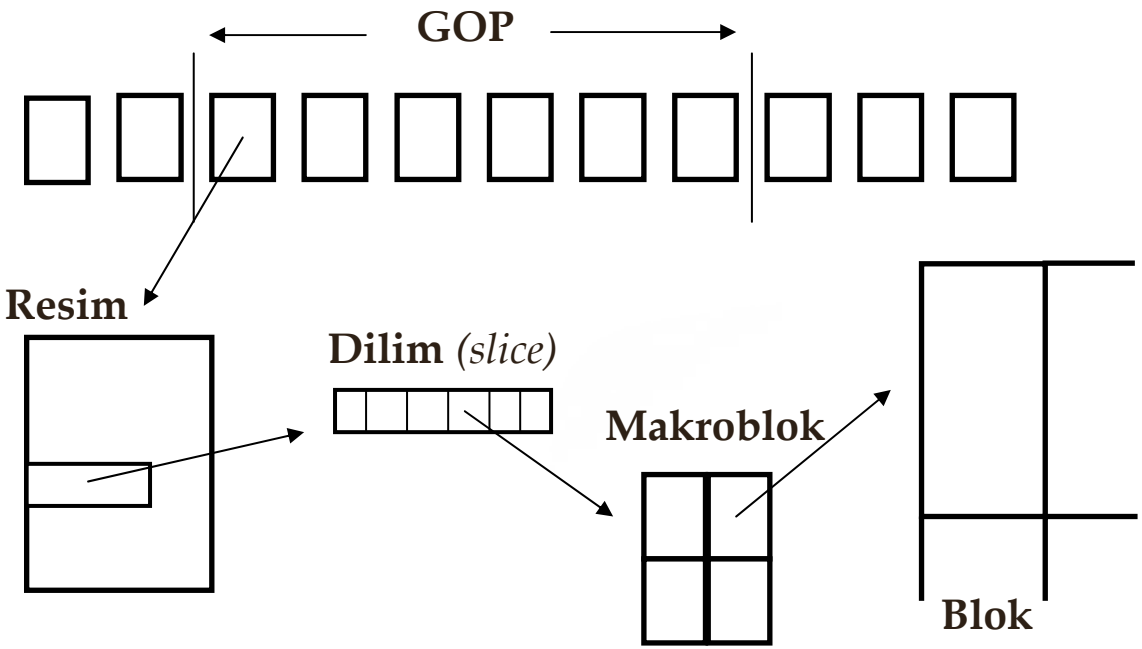
Sıralama : *Ordering*

Entropi Kodlama : *Entropy Coding*

Video Sıkıştırma ve H.264 (devam)



Video Sıkıştırma ve H.264 (devam)



Video Verisinin Güvenlik Gereksinimleri

Video kodlayıcılarının amacı; olabilecek en yüksek kalitede veriyi olabildiğince küçük boyutlarla temsil edebilmektir.

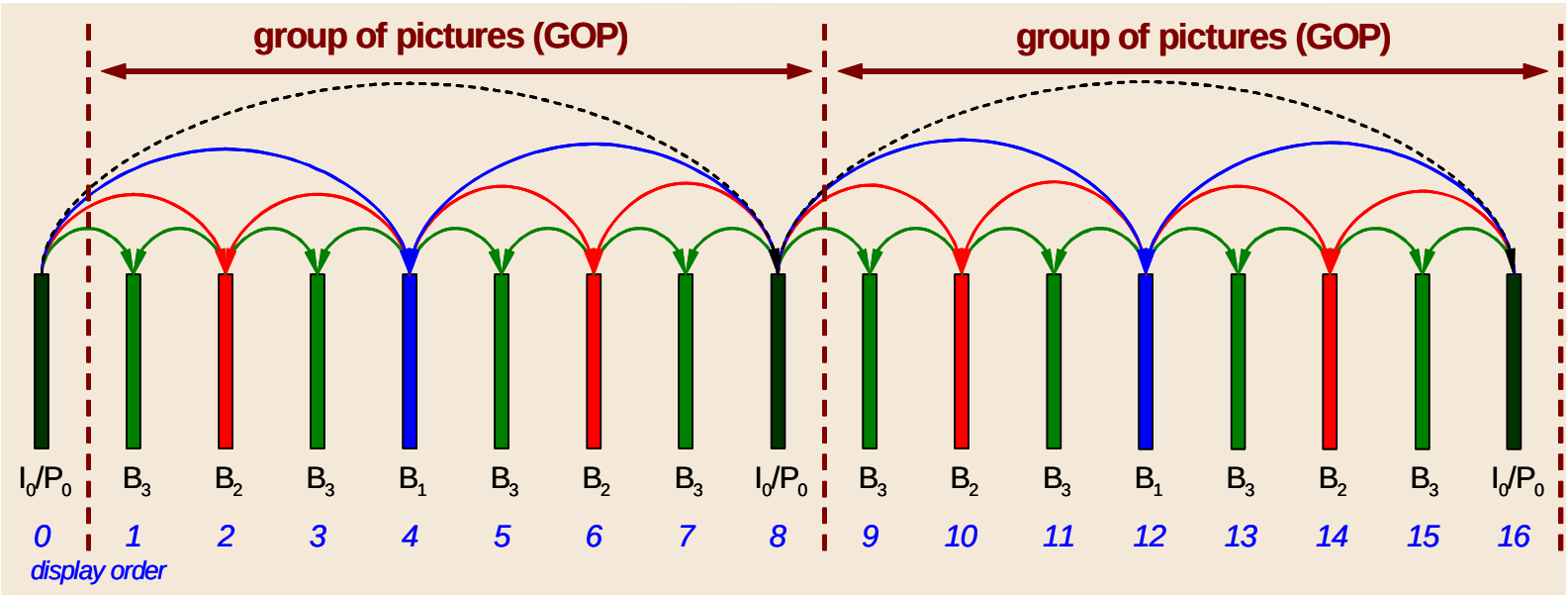
Geliştirilecek şifreleme algoritmalarının da kodlayıcıların bu özelliğini bozmayacak şekilde tasarlanması gerekmektedir.

Video Verisinin Güvenlik Gereksinimleri (devam)

1. *Verinin istatistiki yapısının ve sıkıştırma oranının korunması,*
2. *Veriye olabildiğince az eklenti (overhead) eklenmesi,*
3. *Hızlı ve düşük karmaşıklıkta, gerçek zamanlı kısıtlarına uygun olarak çalışması,*

Video Verisinin Güvenlik Gereksinimleri (devam)

4. Referans çerçevelere erişimde sıkıntı yaratmaması,



Video Verisinin Güvenlik Gereksinimleri (devam)

5. *Kodlayıcı içinde gömülü olan kod çözücü yapısının unutulmaması,*

6. *Senkronizasyon noktaları kullanması, küçük bit hatalarını düzeltebilmesi, hata yayılmasını (error propogation) engellemesi ve hata düzeltme (error recovery) mekanizmasını bozmaması,*

Video Verisinin Güvenlik Gereksinimleri (devam)

7. *İletimde ara nodlarda şifre çözümü gerektirmemesi,*
8. *Video kalitesini düşürmemesi,*
9. *Şifreleme birimlerinin küçük ve birbirinden bağımsız olması,*
10. *Çeşitli güvenlik seviyelerinde video içeriğini ve hareketlerini gizlemesi.*

Geliştirilmiş Güvenlik Algoritmaları

Anılan ihtiyaçlar doğrultusunda geliştirilebilecek yöntemlerin kendilerine göre artı ve eksi yönleri bulunmaktadır.

Asıl hedef, video verisinin kendine has özelliklerinden faydalanmak yoluyla şifreleme algoritmasının etkinliğini arttırarak masrafını düşürmek olacaktır.

Geliştirilmiş Güvenlik Algoritmaları (devam)

Yapılmış çalışmalar sınıflandırılmak istenirse;

1. ***Video verisini düz metin verisiymiş gibi ele alan algoritmalar,***
2. ***Video verisinin yapısal özelliklerini kullanan seçimli*** (*selective*) ***algoritmalar,***

olmak üzere iki ana gruptan bahsedilebilir.

Geliştirilmiş Güvenlik Algoritmaları – Grup 1

1. ***Basit Şifreleme***(*Naive Algorithm*)
2. ***Bölünmüş Bit Akışları Üzerinde Rasgele Rotasyon*** (*Random Rotation in Partitioned Bit Streams*)

Geliştirilmiş Güvenlik Algoritmaları – Grup 2

1. Sadece *I tipi çerçeve şifrelemesi,*

2. *SEC-MPEG:*

   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.

Geliştirilmiş Güvenlik Algoritmaları – Grup 2 (devam)

3. ***Zig Zag Sıralama*** *(Zig Zag Permutation Algorithm)*

4. *Video Encryption Algorithm* ***(VEA)***

$$\begin{array}{c} a_1\ a_3 \ldots a_{2n-1} \\ \oplus\ a_2\ a_4 \ldots a_{2n} \\ \hline c1\ c2 \ldots cn \end{array}$$

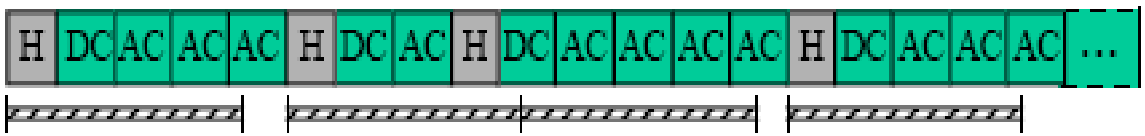
$$S = a_1\, a_2\, a_3\, a_4 \ldots a_{2n-1}\, a_{2n}$$

$$C = c_1\, c_2 \ldots c_n E(\, a_2\, a_4 \ldots a_{2n}\,)$$

5. ***Sade karıştırma yöntemi*** *(Pure Permutation)*

Geliştirilmiş Güvenlik Algoritmaları – Grup 2 (devam)

6. ***Ölçeklenebilir seçimli şifreleme*** (*Scalable Partial Encryption*)



n= 3 için seçimli şifreleme

Geliştirilmiş Güvenlik Algoritmaları – Grup 2 (devam)

7. *Algorithm 1*

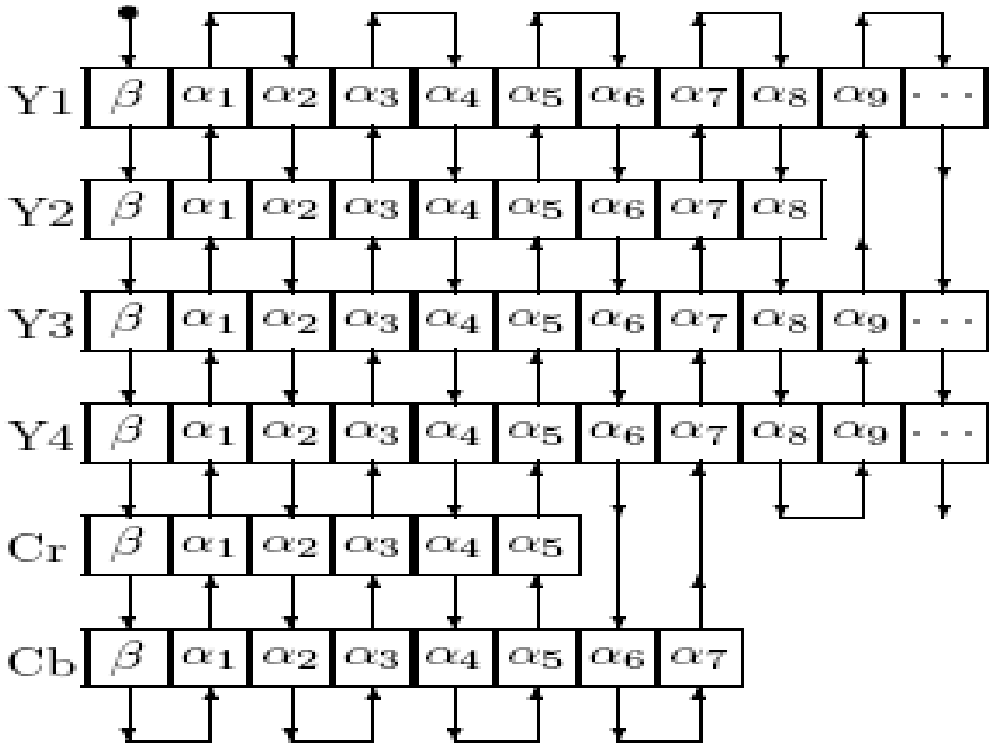
8. ***VEA –*** *Video Encryption Algorithm*

$$E_k(S) = (b_1 \oplus s_1)\cdots(b_m \oplus s_m)\cdots(b_1 \oplus s_{m+1})\cdots(b_m \oplus s_{2m})$$

9. ***MVEA –*** *Modified VEA*

Geliştirilmiş Güvenlik Algoritmaları – Grup 2 (devam)

10. RVEA – Robust VEA



Y: *parlaklık* (*luminance*)

Cr, Cb: *krominans*

Geliştirilmiş Güvenlik Algoritmaları – Grup 2 (devam)

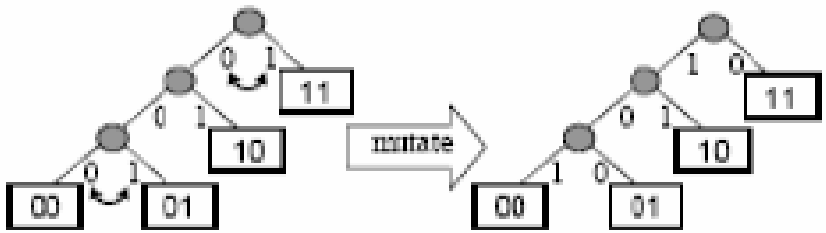
11. PVEA – Perceptual VEA

1. **Intra DC katsayıları –** Genel görüntü bilgisi taşır.
2. **AC ve Inter DC katsayıların işaret bitleri ve ESCAPE DCT katsayıları –** Blok bazında detayları temsil eder.
3. **Hareket vektörlerinin değerleri ve işaret bitleri –** Hareket bilgilerini içeren görsel kaliteyi temsil eder.

Geliştirilmiş Güvenlik Algoritmaları – Grup 2 (devam)

12. Çoklu Huffman Tabloları (Multiple Huffman Tables - MHT)

Huffman Ağacı Mutasyon (*Huffman Tree Mutation*) yöntemi ile ağaç üretimi zahmetsizce yapılabilir.



Sonuç

Bu çalışmamızda, popüler bir çoklu ortam öğesi olan video verisinin yapısal özelliklerine değinilerek veriye özel şifreleme algoritmasının yerine getirmesi gereken koşullar incelenmiştir.

Katılımınız için Teşekkür Ederiz..

Gül BOZTOK ALGIN

E. Turhan TUNALI