GÖRSEL ŞIFRELEME VE GÖRÜNTÜ İŞLEME

Piksellerden Kriptografiye: Neden Standart Metin Şifreleme Görseller İçin Yetersiz?

Eren Balkış

GÖRSEL VERİNİN DOĞASI

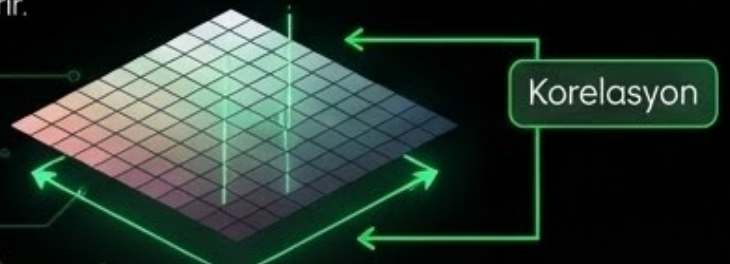
Sadece JPEG/PNG dosyaları değil: tıbbi röntgenler, askeri uydu görüntüleri, parmak izi taramaları... Hepsi kritik öneme sahip görsel verilerdir.

YÜKSEK KORELASYON VE FAZLALIK

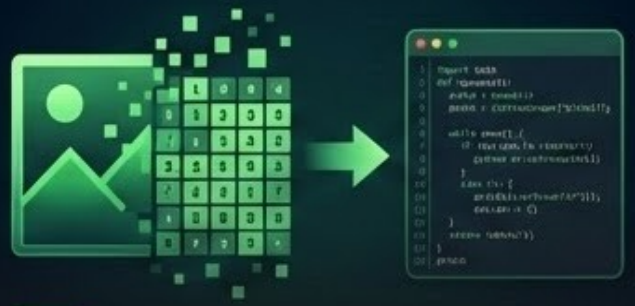
Standart metin verisinin aksine, dijital görsellerde yan yana duran pikseller genellikle birbirine çok benzer renk değerlerine sahiptir. Bu duruma **korelasyon** denir. İşte bu özellik, şifrelemeyi zorlaştırır.

MATRİS YAPISI

Bilgisayar için bir görsel, aslında sayısal bir matristir. (Örn: 1080x1920 boyutunda, her hücresinde 0-255 arası değer olan bir ızgara). Bu yapı, şifrelemede özel yaklaşımlar gerektirir.



TEMEL KAVRAMLAR

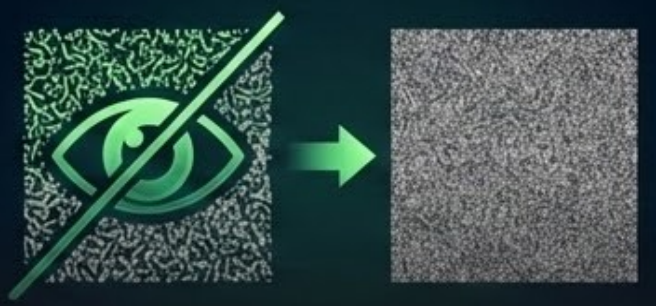


PIKSEL MATRISI

Görselleri NumPy dizisine (matrise) çevirme işlemi, bilgisayarın resmi "görmesini" sağlayan tercüme işlemidir. Bilgisayar "kırmızı elma"yı bilmez, ama (255, 0, 0) sayı grubunu bilir.

AES ŞIFRELEME

Advanced Encryption Standard. Simetrik bir algoritmadır. Görsellerde genellikle 128-bit bloklar halinde çalışır. Aynı anahtar hem şifreler hem çözer



DESEN GIZLEME

İyi bir şifrelerne, görseldeki desenleri yok etmeli ve Histogramı düzleştirerek homojen bir gürültü (noise) oluşturmalıdır.

Playfair, Vigenère ve Hill Şifreleme

Neden Kullanılmaz?

Bu yöntemler harf (alfabe) tabanlıdır. Bir görüntünün pikselleri 0-255 arası sayısal değerlerdir. Bu algoritmaları piksellere uyarlasak bile, **Karıştırma (Confusion)** ve **Yayma (Diffusion)** özellikleri düşüktür.

Zafiyet:

Şifrelenmiş görüntüde orijinal resmin hatları hala belli olabilir. Özellikle Hill şifreleme 'lineer' (doğrusal) bir işlem olduğu için görselin ana hatlarını gizleyemez bu yüzden de modern saldırılara (Known-Plaintext Attack) karşı dayanıksızdır.

Hill Şifreleme

Mantık: Görseldeki pikselleri ikili veya üçlü gruplara ayırır ve bir anahtar matrisi ile çarpar. Matris çarpımı esaslıdır. $\begin{bmatrix} 1 & 2 & 3 \\ 4 & 5 & 6 \\ 7 & 8 & 1 \end{bmatrix}$

Görsel Şifrelemedeki Yeri:

Zayıflık: Lineer bir işlem olduğu için görseldeki keskin hatları (kontrastı) tam olarak yok edemez. Silüetler sızabilir.

SAYISAL ÖRNEK (MOD 256)

Gri Tonlama Piksel Çifti: [100, 50]

$$\begin{bmatrix} 3 & 2 \\ 5 & 7 \end{bmatrix} \times \begin{bmatrix} 100 \\ 50 \end{bmatrix} = \begin{bmatrix} 400 \\ 850 \end{bmatrix}$$

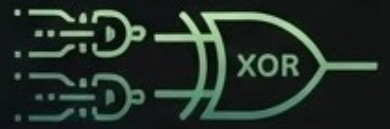
Sonuç (Mod 256):

P1 = 400 % 256 = **144**

P2 = 850 % 256 = **82**

Vernam Şifreleme (XOR)

Mantık: Her piksel, rastgele üretilmiş bir anahtar değeriyle XOR işlemine (Özel VEYA) sokulur.



Görsel Şifrelemedeki Yeri:

Mükemmel Gizlilik: Eğer anahtar resimle aynı boyutta ve rastgele ise, sonuç tamamen gürültü (noise) olur.

Pratik Değil: 10 MB'lık bir resmi şifrelemek için 10 MB'lık anahtar gerekir. Bu anahtarı saklamak ve iletmek zordur.

SAYISAL ÖRNEK (BİTWİSE XOR)

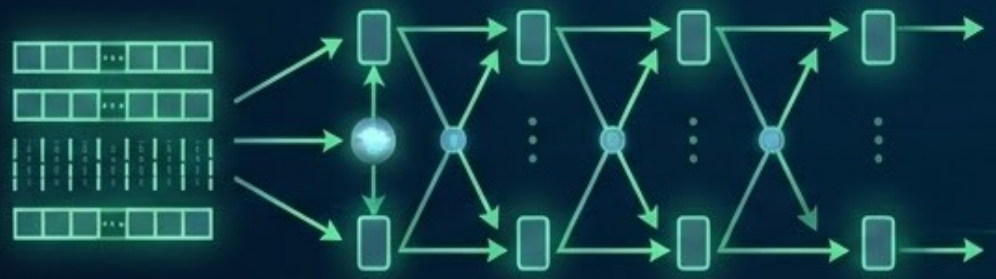
```
Piksel:     11001010 (202)
Anahtar:    10100110 (166)
XOR Sonuç:  01101100 (108)
```

İşlem tersine çevrilebilir:
108 XOR 166 = 202 (Orijinal)

DES (Eski Standart)

Mantık:

Görseli 64-bitlik (8x8 piksel değil, veri biti) bloklara ayırır. Karmaşık ve tersine çevrilebilir "**Feistel Yapısı**" kullanır.



Görsel Şifrelemedeki Yeri:

Klasik yöntemlerden çok daha karmaşıktır (Confusion & Diffusion).

Artık Güvensiz: 56-bit anahtar günümüz bilgisayarlarıyla dakikalar içinde kırılabilir.

Görseller büyük veri olduğu için DES yavaş kalabilir.

YAPISAL BAKIŞ

Blok Boyutu: 64 Bit

Anahtar: 56 Bit (Çok kısa!)

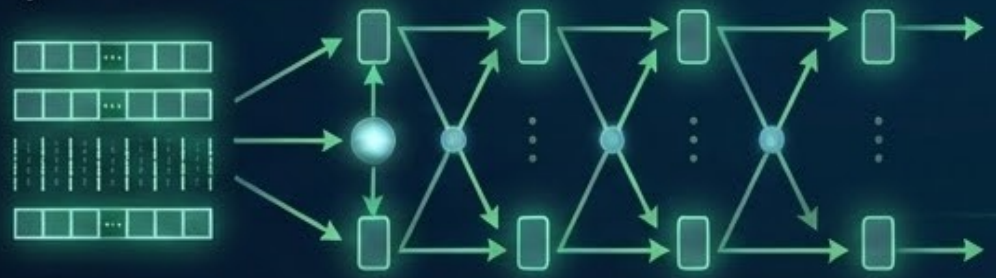
Döngü (Round): 16 Kez

Günümüzde "Brute-Force" ile kırılması çok kolaydır.

AES (Gelişmiş Şifreleme)

MANTIK

Feistel ağı yerine “Substitution-Permutation” ağı kullanır. Pikselleri baytlar halinde matrise yerleştirir ve karıştırır. AES bir Blok Şifreleme türüdür. Görüntüyü 128 bitlik bloklara böler.



ÖNEMLİ: ECB modu desen sızdırır ve zayıftır. Görsel şifrelemede AES mutlaka CBC, GCM veya CTR modlarında kullanılmalıdır.

GÖRSEL ŞİFRELEMEDEKİ YERİ (ALTIN STANDART)

S-Box (SubBytes): Pikselleri tablodan rastgele değerlerle değiştirir (Confusion).

ShiftRows & MixColumns: Pikselleri satır/sütun bazında karıştırır (Diffusion).

Hız: Donanım destekli olduğu için yüksek çözünürlüklü görselleri hızlı şifreler.

AES ADIMLARI (PİKSEL MATRİSİNDE)

`Durum Matrisi (State Matrix - 4x4 Byte)`

↓

1. SubBytes: Piksel → S-Tablosu → Yeni Piksel

↓

2. ShifttRows: Satırları sola kaydır

↓

3. MixColumns: Sütunları matematiksel karıştır

↓

4. AddRoundKey: Anahtar ile XOR'la

***CBC Modu kullanıldığında görsel tamamen gürültüye dönüşür.**

GÜNLÜK HAYATTA ve AKIŞ ŞİFRELEME

GÜNLÜK KULLANIM (DAILY USE)

1. Mesajlaşma (WhatsApp/Signal)

Fotoğraflar AES ile şifrelenir, anahtar değişimi için asimetrik yöntemler kullanılır.

2. Web Güvenliği (HTTPS)

Tarayıcıdan resim indirirken AES-GCM veya ChaCha20-Poly1305 kullanılır.

3. Dijital Hak Yönetimi (DRM)

Netflix/Spotify görüntü verisini AES-128 ile şifreler, donanım tabanlı çözümleme yapılır.

AKIŞ ŞİFRELEME (STREAM CIPHERS)

Kullanım Alanı: Netflix, YouTube, Zoom gibi video akışlarında, veri bit-bit veya bayt-bayt şifrelenir.

Neden Kullanılır?: Blok şifrelemeye göre daha hızlıdır ve verinin tamamının gelmesini beklemez, gerçek zamanlıdır.

ALGORITMALARIN KARŞILAŞTIRILMASI

DES (Eski)

Anahtar Boyutu: 56-bit

Görsel İşleme Hızı: Yavaş

Güvenlik Seviyesi: Düşük (Kırılabilir)

Güvenlik Seviyesi: **Düşük (Kırılabilir)**

AES (Standart)

Anahtar Boyutu: 128/256-bit

Görsel İşleme Hızı: **Hızlı (Donanım destekli)**

Güvenlik Seviyesi: **Çok Yüksek**

RSA (Asimetrik)

Anahtar Boyutu: 2048-bit+

Görsel İşleme Hızı: Çok Yavaş

Güvenlik Seviyesi: **Yüksek (Ancak görseller için hantal)**

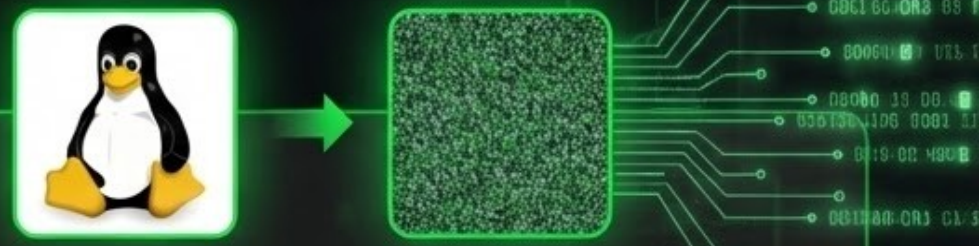
Not: Görsel şifrelemede hız kritik olduğu için AES gibi simetrik algoritmalar tercih edilir.

AES Her Zaman Güvenli midir?

KRITIK NOKTA: İŞLEM MODLARI

ECB MODU
DESEN SIZDIRAN (PATTERN LEAKAGE)

Electronic Codebook. Deterministik bir yapıdadır; yani aynı renk değerine sahip pikseller (veri blokları) her zaman aynı şifreli çıktıya dönüşür. Bu durum, görseldeki veri fazlalığını (redundancy) gizleyemez ve sllüetlerin çıplak gözle seçilmesine neden olur.



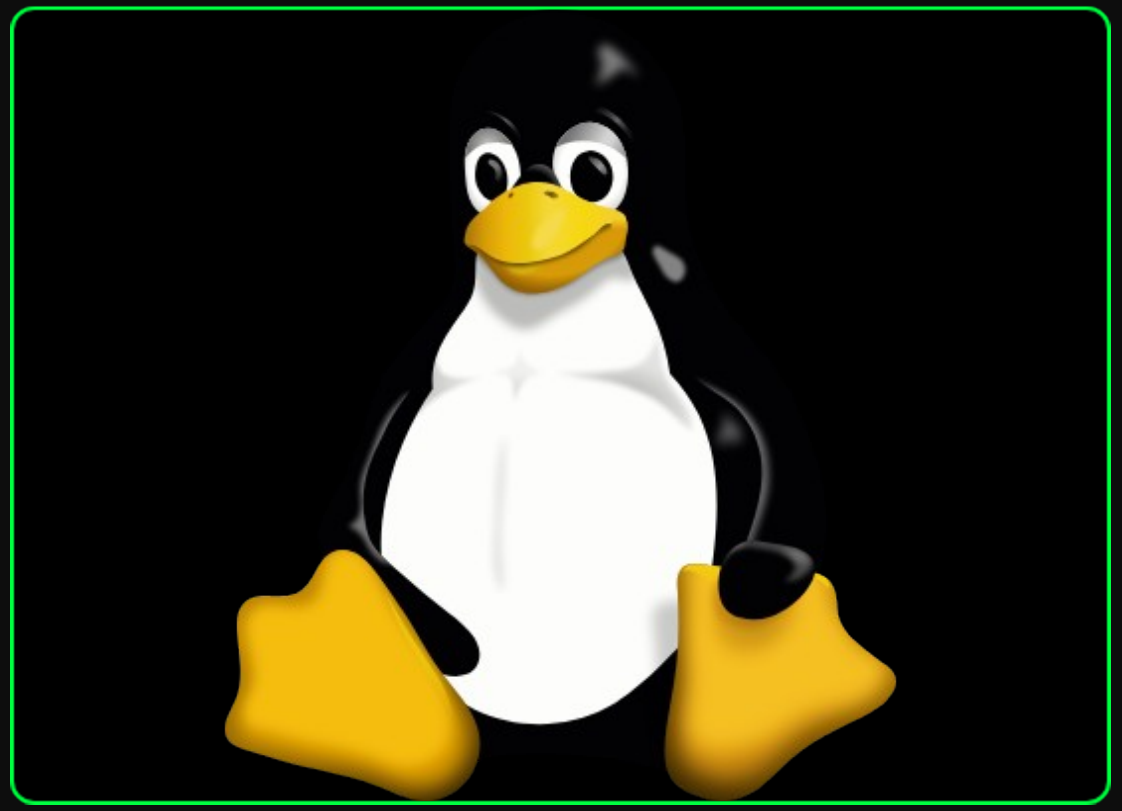
CBC MODU
YÜKSEK ENTROPİ (HIGH ENTROPY)

Cipher Block Chaining. Zincirleme etkisi kullanır. Her blok şifrelenmeden önce bir önceki şifreli blok ile XOR işlemine girer. Bu sayede, görselde aynı renk blokları olsa bile şifreli çıktı tamamen farklı olur (Diffusion/Yayılım ilkesi). Tam bir gürültü görüntüsü oluşur.

PYTHON ILE SÜREÇ AKIŞI

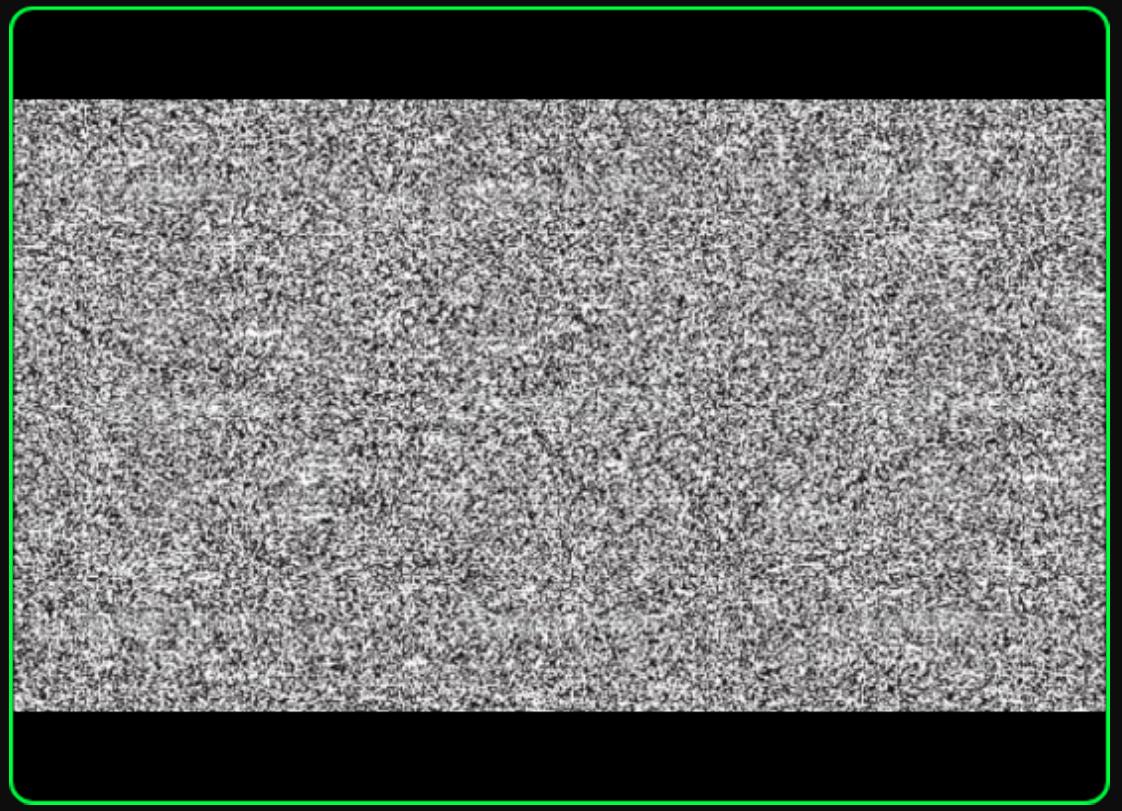
- **Görüntü Okuma:** PIL kütüphanesi ile resim yüklenir.
- **Matris Dönüşümü:** NumPy kullanılarak resim, sayısal bir matrise (Array) çevrilir.
- **Düzleştirme (Flatten):** AES bloklar halinde çalıştığı için 2D/3D matris, tek boyutlu bayt dizisine indirgenir.
- **Şifreleme:** Başlangıç Vektörü (IV)" ile rastgelelık eklenir ve AES algoritması ile veri şifrelenir.
- **Yeniden Şekillendirme:** Şifreli bayt dizisi, tekrar orijinal resim boyutlarına (Reshape) getirilir..

UYGULAMA: PYTHON ILE AES



ORIJINAL GÖRSEL

Giriş Verisi
(Plaintext)
NumPy Matrisi



ŞIFRELENMIŞ GÖRSEL

Çıkış Verisi
(Ciphertext)
AES-CBC Modu

TEŞEKKÜRLER

Sorularınız?

Eren Balkış
0414230036

Kaynaklar

https://www.youtube.com/playlist?list=PLBlnK6fEyqRgJU3EsOYDTW7m6SUmW6kII

Source: Neso Academy - Cryptography & Network Security

https://upload.wikimedia.org/wikipedia/commons/3/35/Tux.svg

Source: en.wikipedia.org

https://i.ytimg.com/vi/Co-g_JeTiF8/maxresdefault.jpg?sqp=-oaymwEmCIAKENAF8quKqQMa8AEB-AH-CYAC0AWKAgwIABABGGUgZShlMA8=&rs=AOn4CLAyOUucR4gZ7TX_gdsRv_Kds9CP_w

Source: www.youtube.com

- Shannon, C. E. (1949). "Communication Theory of Secrecy Systems". *Bell System Technical Journal*.
  - *Neden Önemli:* Kriptografinin babası sayılan Shannon'un, "Confusion" (Karıştırma) ve "Diffusion" (Yayma) kavramlarını ortaya attığı makaledir. Görsel şifrelemede piksellerin neden iyice karıştırılması gerektiğinin teorik temelidir.

National Institute of Standards and Technology (NIST). (2001). *SP 800-38A: Recommendation for Block Cipher Modes of Operation*.

- *Neden Önemli:* "Penguen sorunu" olarak bilinen, blok şifreleme modlarının görsel verideki desenleri gizleyip gizleyemediğini teknik olarak açıklayan standarttır.

Stallings, W. (2017). *Cryptography and Network Security: Principles and Practice* (7th Edition). Pearson.

- *Neden Önemli:* AES, DES, Blok Şifreleme modları (ECB, CBC) ve Akış şifrelemenin çalışma prensipleri için en yaygın kullanılan ders kitabıdır.