**DİNAMİK S-BOX KULLANILARAK ŞİFRELENMİŞ RESMİN QR KODA DÖNÜŞTÜRÜLMESİ**

**Devran CANİKLİ**

**Eren Alp ŞAKACI**

**Karabük Üniversitesi**

**Bilgisayar Mühendisliği**

**Tez Danışmanı:**

**Dr. Öğr. Üyesi Burhan SELÇUK**

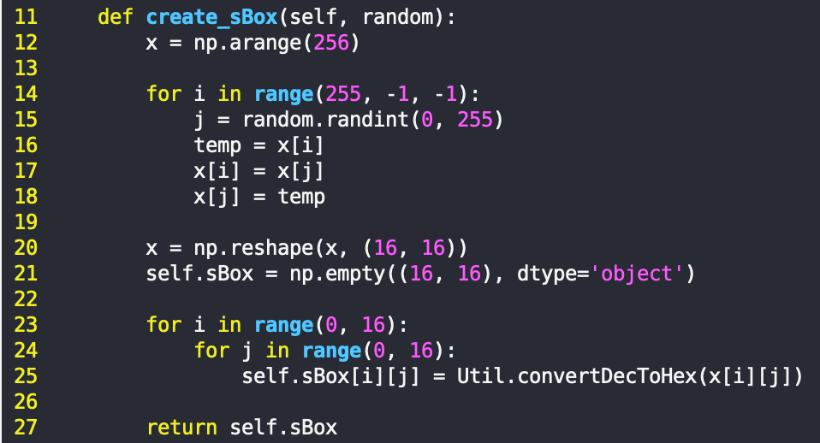
**Özet:** Günümüzde mesajlaşma uygulamalarının yaygınlaşması sebebiyle gün içerisinde yoğun bir şekilde resim alışverişi yapılmaktadır. Bu da çeşitli güvenlik ve gizlilik sorunlarına neden olmaktadır. Bu çalışmada hassas içeriğe sahip resimlerin bir anahtar ile şifrelenip, QR koda dönüştürülerek güvenliğinin ve gizliliğinin artırılması amaçlanmıştır. Şifrelenen resim sadece anahtarı bilen kullanıcı tarafından çözülebilmektedir. Bu sayede resmin paylaşıldığı ortama saldırılması halinde üçüncü şahıslar resmin içeriğini görüntüleyememektedir. Şifreleme algoritmasında dinamik S-box kullanılmıştır.

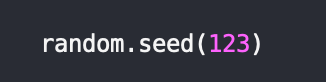
**Giriş**

AES (Advanced Encryption Standard) veya DES (Data Encryption Standard) gibi blok şifreleme algoritmalarının, resim dosyalarının boyutlarının büyük olmasından dolayı resim şifreleme için kullanılması uygun görülmemektedir. Bu çalışmada AES’in temelinde bulunan S-box (substitution-box) yöntemi kullanılmıştır. S-box, simetrik şifreleme algoritmalarında yer değiştirme (substitution) amacıyla kullanılan bir tekniktir. Blok şifrelemede kullanılan S-box’lar genellikle statik bir şekilde üretilmektedir. Bu çalışmada kullanılan S-box güvenliği artırmak amacıyla belirlenen anahtara göre dinamik bir şekilde üretilmiştir.

**1. S-box Üretimi**

Çalışmada kullanılan S-box 0-255 aralığında 256 adet sayı içermektedir. Bu sayıları 16x16 boyutundaki matrise dinamik (rastgele) olarak yerleştirebilmek için öncelikle bir seed (anahtar) değeri belirlenmiştir. Bu anahtar Knuth Shuffle algoritmasında sayıları karıştırmak amacıyla kullanılmıştır.

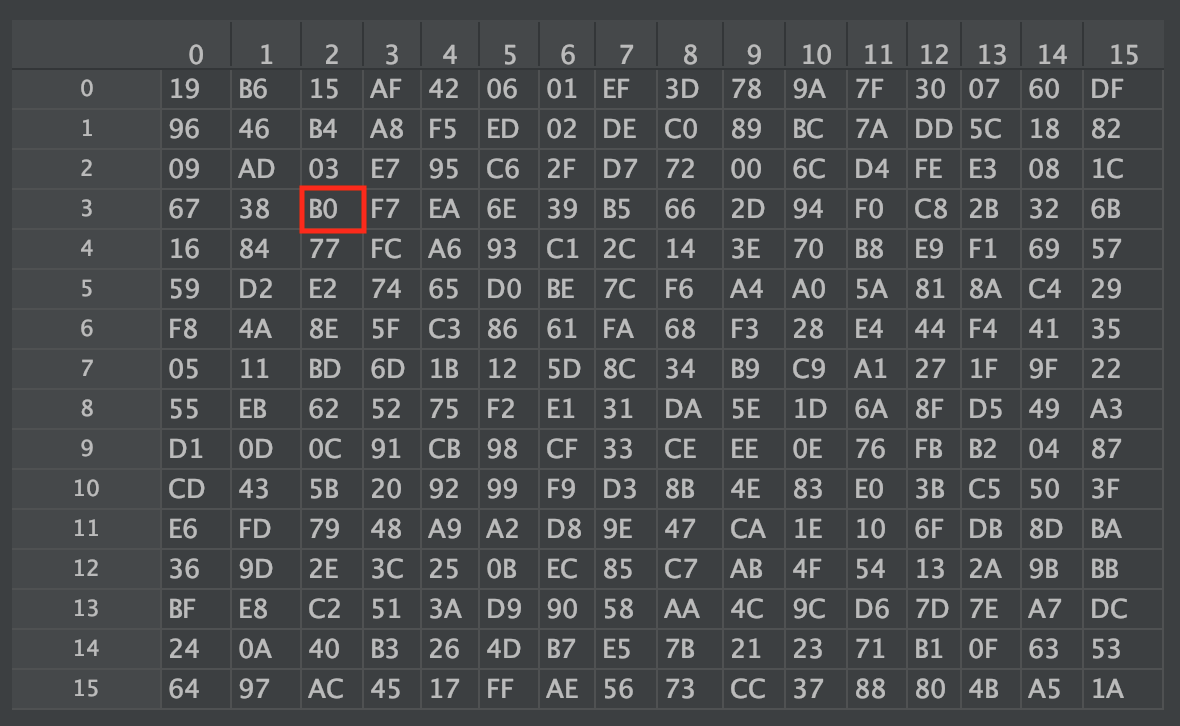




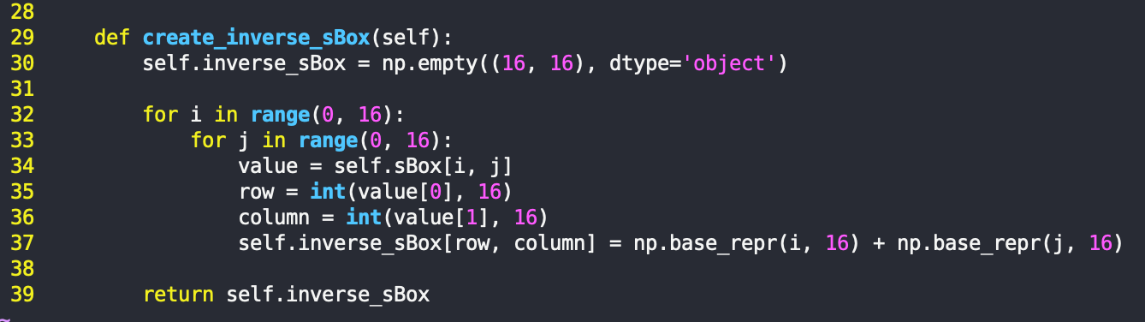
Şekil 1: Seed Değerinin Belirlenmesi

Şekil 2: S-Box’ın Üretilmesi.

Şekil 2’de bulunan **‘create\_sBox’** metodu 16x16 boyutunda 0-255 aralığında rastgele sıralanmış 256 adet sayılardan oluşan matris döndürmektedir. 12. Satırda 0-255 aralığında sıralı bir dizi oluşturulmaktadır. 14. satırda başlayan for döngüsü Knuth Shuffle algoritması ile dizi içerisinde bulunan sayıları karıştırmaktadır. Elde edilen tek boyutlu dizi 20. satırda 16x16 boyutunda matrise dönüştürülmektedir. 23. satırdaki for döngüsü, oluşturulan x matrisindeki değerleri on altı tabanındaki sayılara dönüştürerek S-Box matrisine atamaktadır.

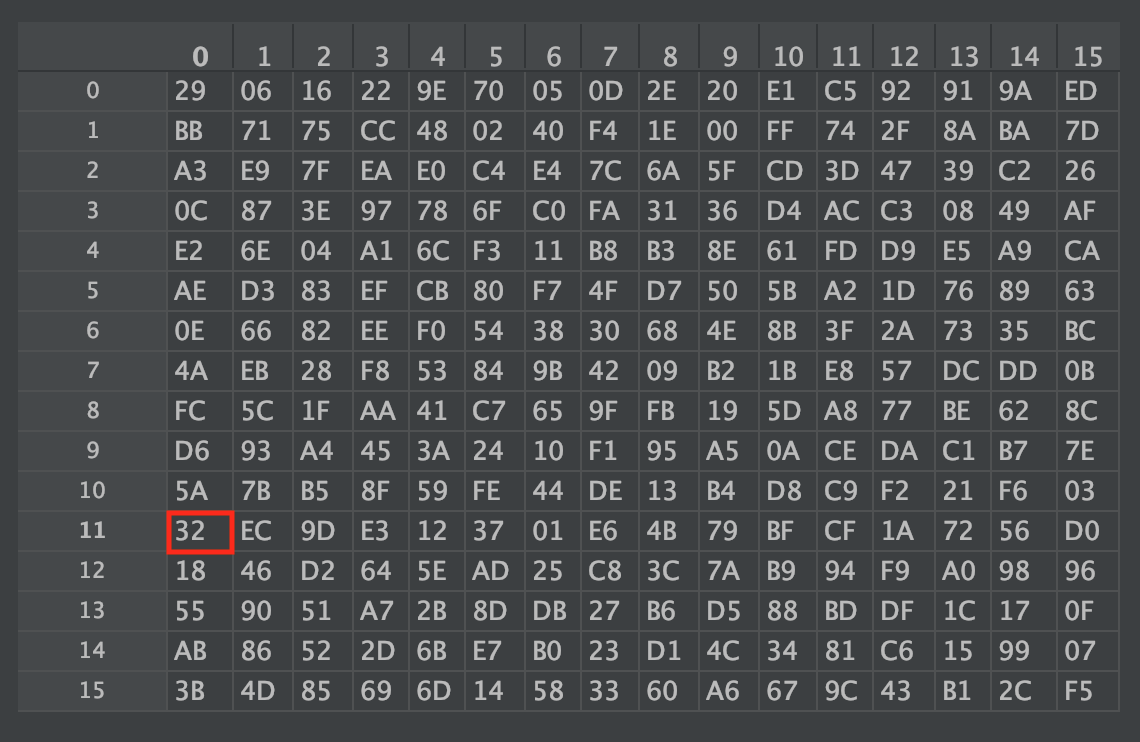


Şekil 3: ‘123’ Seed Değerine Göre Üretilen S-Box.

Deşifreleme aşamasında kullanılan ters (inverse) S-box’ın üretildiği metot aşağıdaki gibidir.

Şekil 4: Ters S-Box üretilmesi.

Ters S-Box, S-Box değerlerine bağlı üretilen bir matristir. Örneğin, S-Box matrisinde 3. Satır 2. Sütundaki değer B0’dır. Ters S-Box’ta B. Satır (11. Satır) 0. Sütundaki değer 32 olacaktır.



Şekil 5: ‘123’ Seed Değerine Göre Üretilen Ters S-Box.

**2. Resmin Şifrelenmesi**

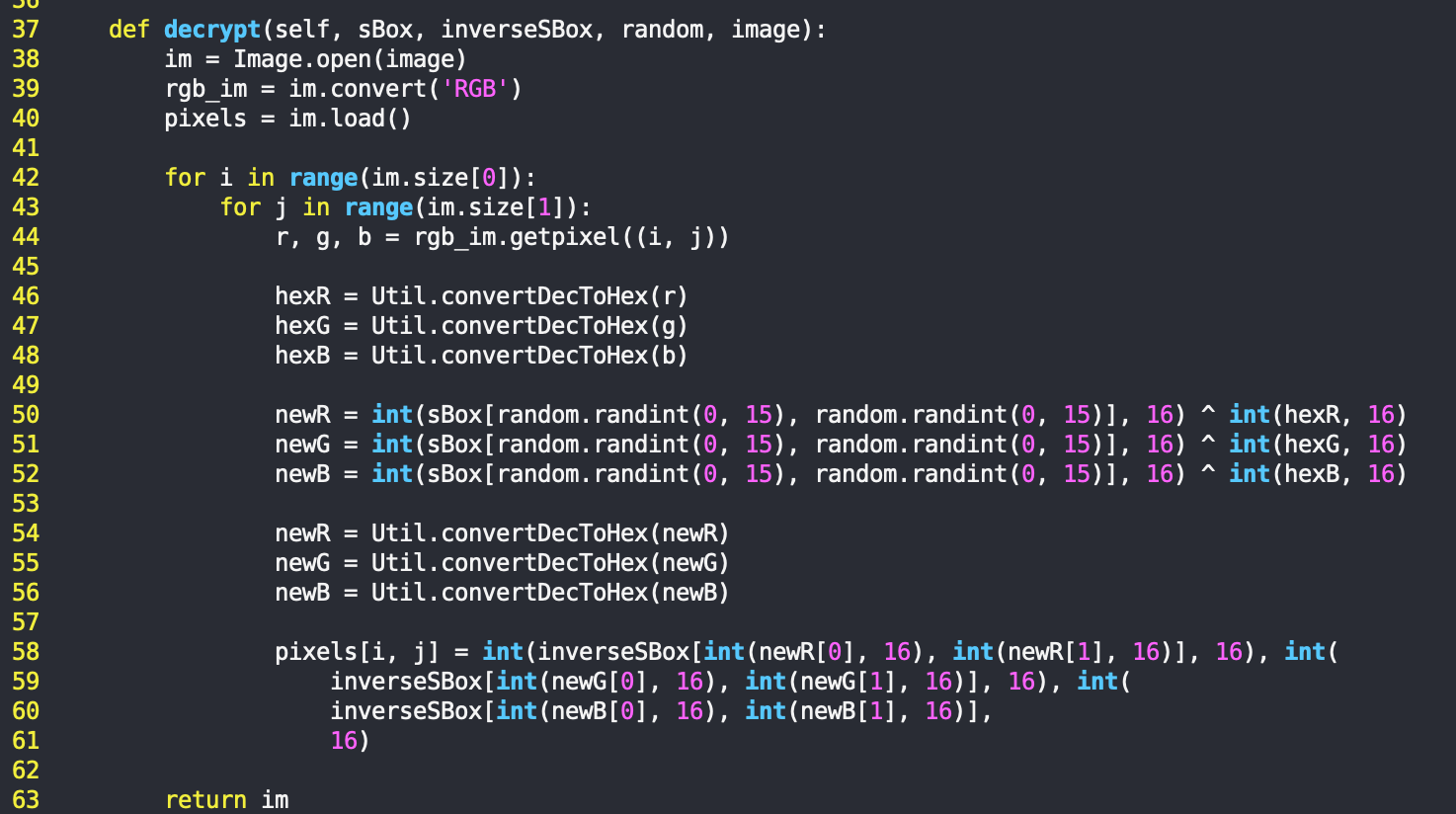
Şifreleme metodu aşağıdaki gibidir:



Şekil 6: Şifreleme Metodu

Şekil 6’daki şifreleme metodu parametre olarak üretilen S-box’ı, random nesnesini ve şifrelenmesi istenen resmi almaktadır. 8. Satırda okuna resim 9. Satırda ‘RGB’ formatına dönüştürülmektedir. Bu değerler ‘pixels’ matrisine atanmaktadır. For döngülerinin içinde her bir pikselin R (Red), G (Green), B (Blue) değerleri 16 tabanında sayıya dönüştürülmektedir. Örneğin, R değerini E8 olarak kabul edelim. S-box ta kullanılmak üzere E değeri satır, 8 değeri sütun olarak atanır. 29, 30, 31. Satırlarda xor işlemi gerçekleşmektedir. S-box’ın rastgele satır ve sütunundaki değer ile S-box’ın E. Satır, 8. Sütunundaki değer xor işlemine tabi tutulur. İşlem sonucunda oluşan sayı yeni R değeri olarak belirlenir. Bu işlem bütün piksellerin RGB değerleri için tekrarlanır. Metot sonunda şifrelenmiş resim döndürülür.

**3. Resmin Deşifrelenmesi**

Deşifreleme metodu aşağıdaki gibidir:

Şekil 7: Deşifreleme Metodu

Şekil 7’deki deşifreleme metodunda, şifreleme metodundaki gibi resmin RGB değerleri okunur. 50, 51 ve 52. satırlarda S-box’ın rastgele satır ve sütun değerleri ile şifrelenmiş resmin RGB değerleri xor işlemine tabi tutulur. İşlem sonucunda elde edilen RGB değerleri orijinal resmin RGB değerleri ile aynıdır. Bu değerler ‘pixels’ matrisine atanır. Metodun sonunda deşifrelenmiş resim döndürülür.

İşlemler sonucunda elde edilen şifrelenmiş ve deşifrelenmiş resimler aşağıdaki gibidir:



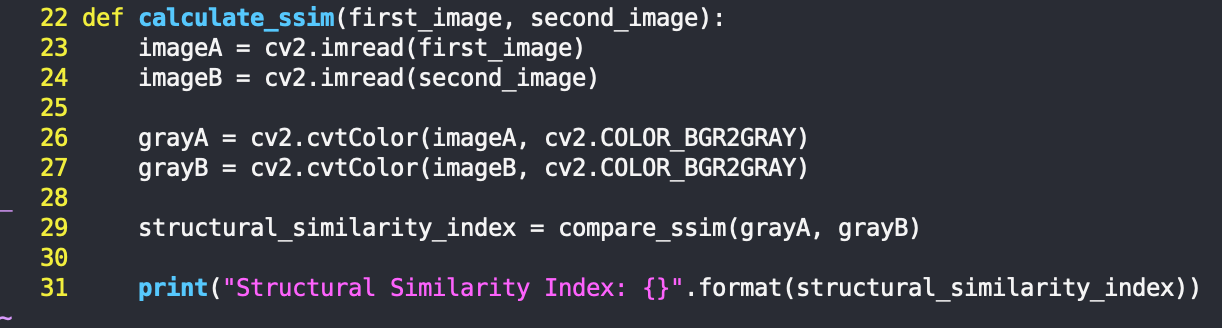
Şekil 10: Deşifrelenmiş Resim

Şekil 9: Şifrelenmiş Resim

Şekil 8: Orijinal Resim

**4. Yapısal Benzerlik İndeksi**

Orijinal resim ile deşifrelenmiş resmin yapısal benzerlik indeksi hesaplanarak indeks değerinin 1.0 olduğu gözlendi. Bu değer, orijinal resim ile deşifrelenmiş resmin birebir aynı olduğunu göstermektedir.



Şekil 11: Yapısal Benzerlik İndeksinin Hesaplanması.



Şekil 12: Yapısal Benzerlik İndeksi.