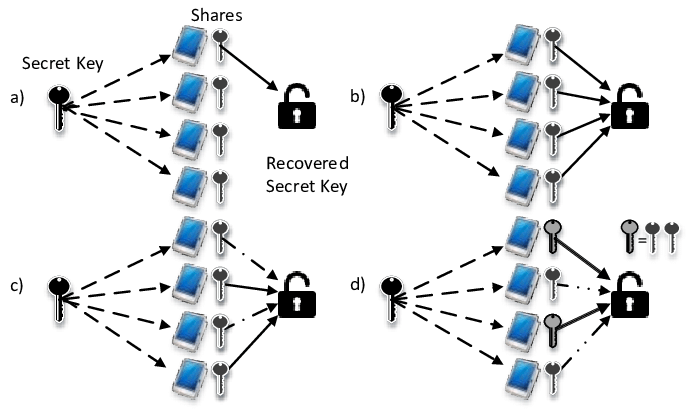
**Secret Image Sharing Nedir?**

Genellikle kullanıcıların belirli bir resmi diğer kullanıcılarla paylaşırken resmin içeriğini gizli tutmak için kullanılan bir yöntemdir. Bu tür bir paylaşım genellikle kriptografi veya diğer güvenlik teknolojileri kullanılarak gerçekleştirilir.

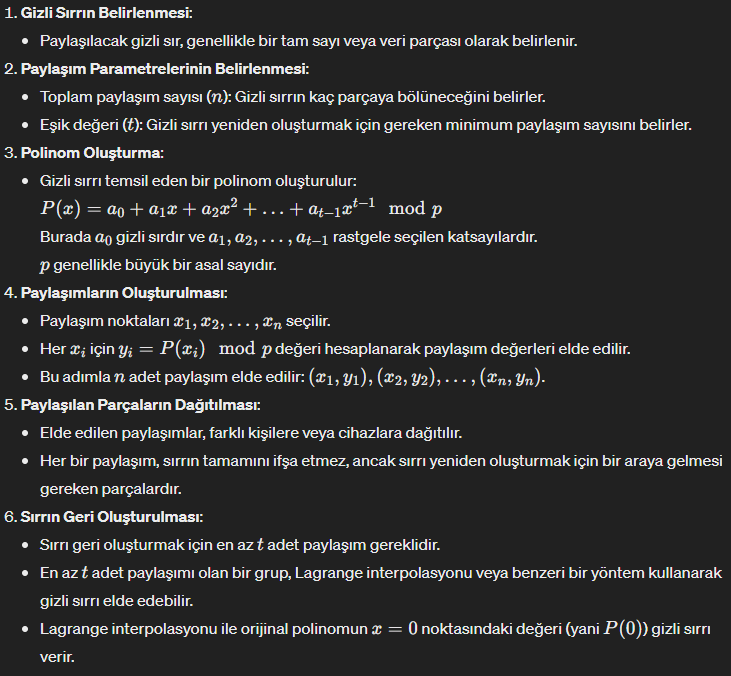
Birçok farklı yöntem bulunabilir, ancak en yaygın olanı resmi şifreleyerek veya gizleyerek paylaşmaktır. Alıcılar, belirli bir anahtar veya parola kullanarak resmi çözebilir ve görüntüleyebilirler. Bu, hassas veya özel içeriğe sahip resimleri paylaşırken gizliliği sağlamak için kullanılabilir.

Bu tür teknikler, çevrimiçi mesajlaşma uygulamalarında veya dosya paylaşım platformlarında gizli bilgilerin paylaşılmasında sıklıkla kullanılır. Ancak, güvenlik açısından, kullanıcıların güvenilir ve güvenli yöntemler kullanmasını sağlamak önemlidir, çünkü bazı yöntemler hala potansiyel olarak riskli olabilir.



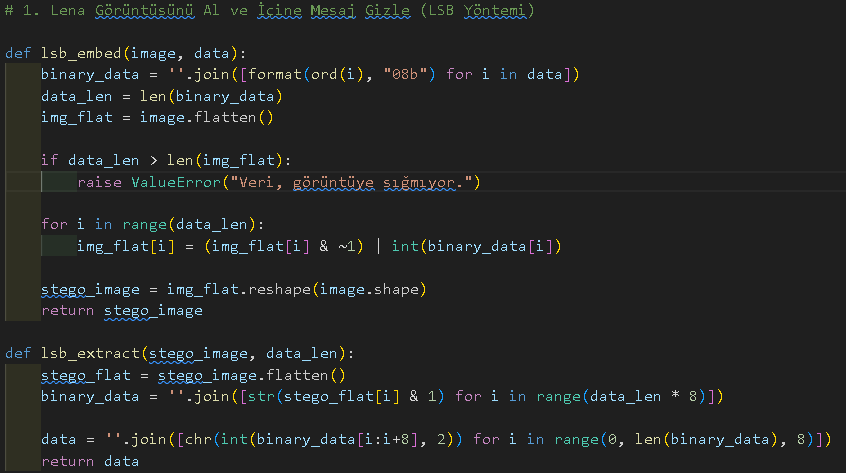
**Shamir'in Sırrı Paylaşımı (Shamir's Secret Sharing)**

Bilgiyi (genellikle bir sırrı) belirli bir grup insan arasında paylaşmanın matematiksel bir yöntemidir. Bu yöntem, sırrın paylaşılan parçalarını (paylaşımları) oluşturur ve bu parçaların belirli bir eşik değeriyle birleştirilerek sırrın yeniden oluşturulmasını sağlar. İşte Shamir'in Sırrı Paylaşımı'nın ana hatları:



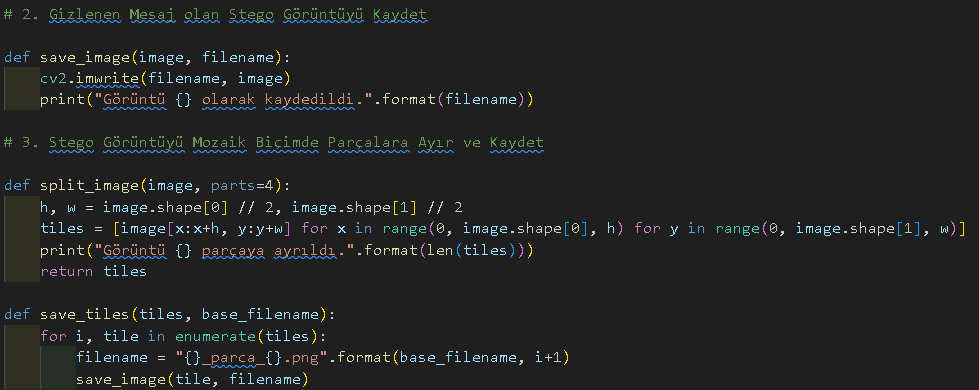
Shamir'in Sırrı Paylaşımı, bilginin güvenli bir şekilde parçalara bölünerek dağıtılmasını ve gerektiğinde orijinal bilgiyi yeniden oluşturmak için parçaların bir araya getirilmesini sağlar. Bu yöntem, kritik bilgilerin korunması ve güvenli paylaşımı için kullanılır.

Shamir’s Secret Sharing - Demo

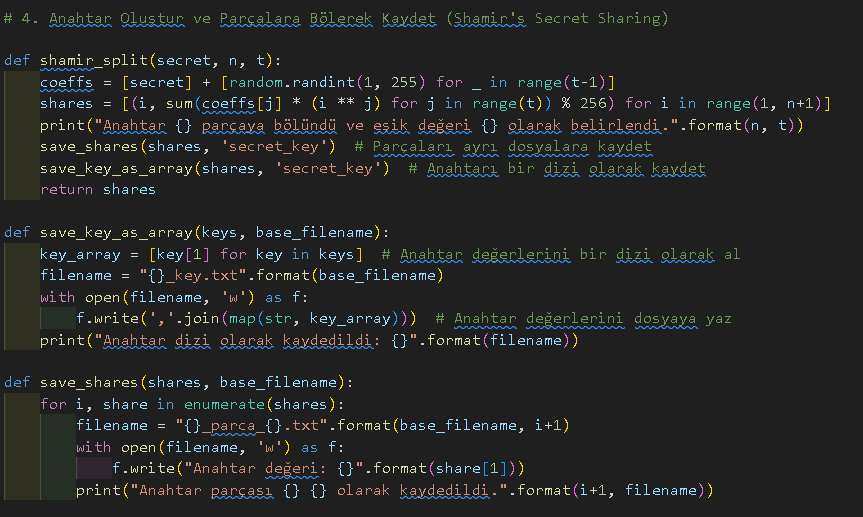


Veri gizlemek ve gizlenen veriyi geri çıkarmak için kullanılır.**lsb\_embed** fonksiyonu, verilen metni binary forma çevirir ve görüntünün piksellerinin en az anlamlı bitlerine yerleştirir. Görüntüyü düz bir diziye dönüştürüp, her pikselin en az anlamlı bitini veri bitiyle değiştirerek gizlenmiş veri içeren yeni bir görüntü oluşturur ve döndürür.

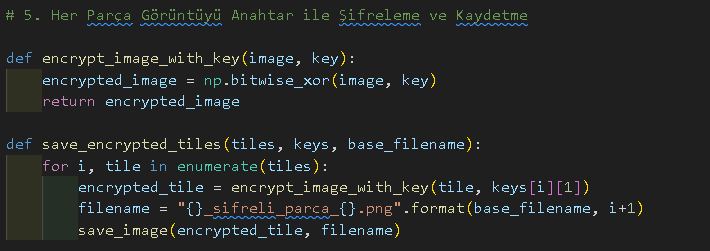
**lsb\_extract** fonksiyonu ise, gizlenmiş veri içeren görüntüyü düz bir diziye dönüştürerek, piksellerin en az anlamlı bitlerinden veriyi geri çıkarır. Bu bitleri 8 bitlik gruplar halinde birleştirerek orijinal metni elde eder ve döndürür. Bu yöntem, veriyi görüntü kalitesinde fark edilir bir değişiklik yaratmadan saklar.



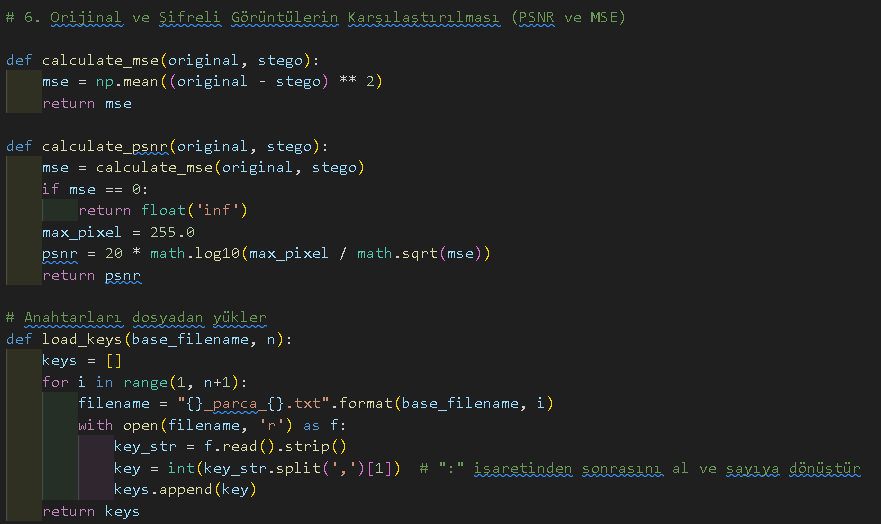
Gizlenen mesajı içeren stego görüntüyü kaydetmek ve daha sonra bu görüntüyü mozaik biçimde parçalara ayırmak için kullanılır. **save\_image** fonksiyonu, verilen görüntüyü belirtilen dosya adına kaydeder. **split\_image** fonksiyonu, görüntüyü eşit parçalara böler; varsayılan olarak 4 parçaya ayırır. **save\_tiles** fonksiyonu ise, bu parçaları ayrı dosyalar olarak kaydeder. Parçaların her biri, temel dosya adını ve parça numarasını içeren bir isimle dosya olarak kaydedilir.



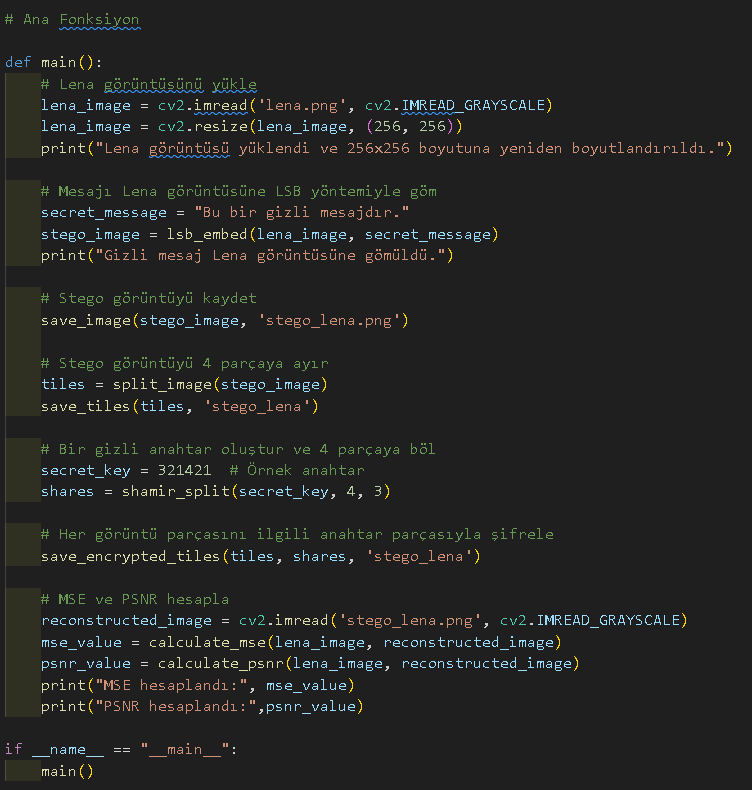
Shamir'in Sır Paylaşımı algoritmasını kullanarak bir anahtarı parçalara böler ve kaydeder. **shamir\_split** fonksiyonu, verilen gizli anahtarı ve eşik değerini kullanarak bir polinom oluşturur, ardından bu polinomdan n adet anahtar parçası üretir ve her parçayı dosyalara kaydeder. **save\_key\_as\_array** fonksiyonu, anahtar parçalarını bir dizi olarak kaydeder ve bu diziyi bir metin dosyasına yazar. **save\_shares** fonksiyonu ise her bir anahtar parçasını ayrı metin dosyalarına kaydeder. Böylece, gizli anahtar n parçasına bölünmüş olur ve bu parçalar belirli bir eşik değeri ile bir araya getirildiğinde orijinal anahtar geri elde edilebilir.



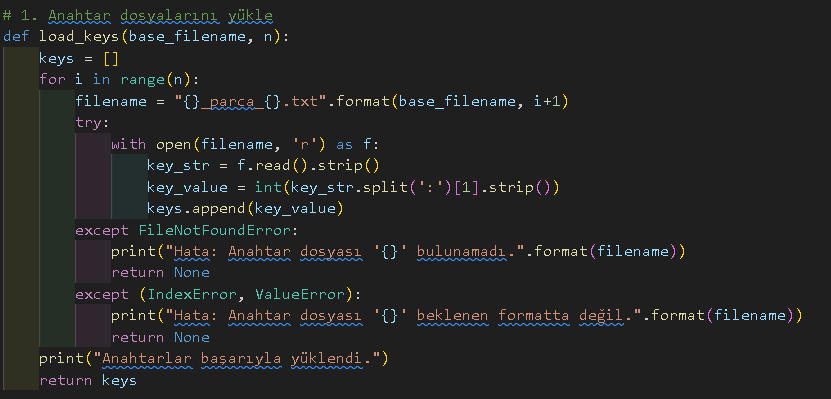
Görüntü parçalarını anahtar ile şifreleyip kaydetmek için kullanılır. **encrypt\_image\_with\_key** fonksiyonu, görüntüyü verilen anahtarla XOR işlemi yaparak şifreler. **save\_encrypted\_tiles** fonksiyonu, her bir görüntü parçasını ilgili anahtar parçası ile şifreler ve şifrelenmiş parçaları dosyalara kaydeder. Şifrelenmiş parçalar, temel dosya adını ve parça numarasını içeren adlarla kaydedilir.



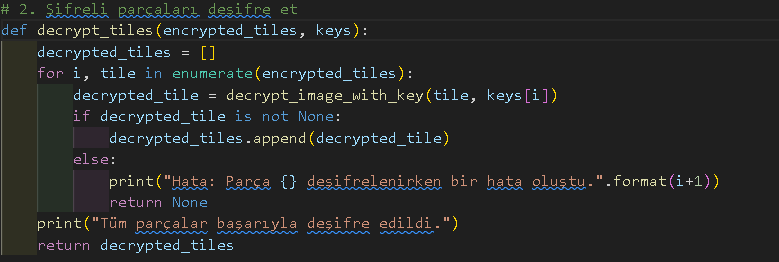
Bu kısımda ise PSNR ve MSE hesaplaması yapıyoruz.Main kısım ise ;



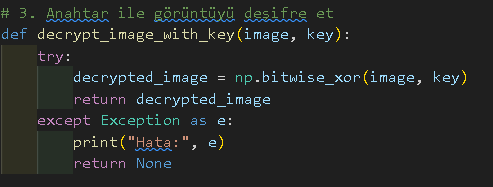
Deşifreleme kısmı ise şu şekilde :

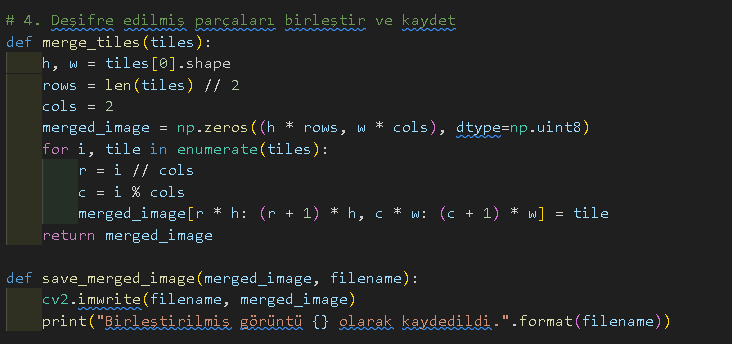


Belirtilen dosyalardan anahtarları yükler. **load\_keys** fonksiyonu, her bir anahtar parçasını dosya adını ve parça numarasını içeren adlarla okur. Dosyadan okunan her anahtar parçasını bir listeye ekler. Dosya bulunamazsa veya beklenen formatta değilse, hata mesajı verir ve **None** döner. Başarılı olduğunda, tüm anahtarlar bir **liste olarak** geri döner.

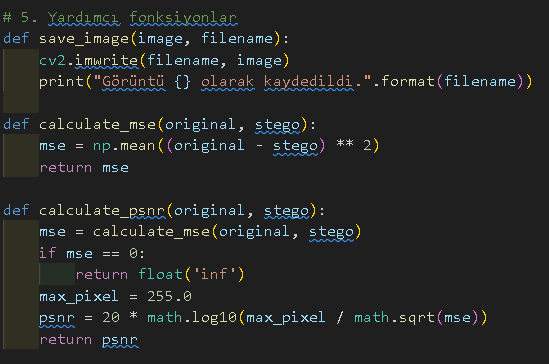


Şifreli görüntü parçalarını anahtarlarla deşifre eder. **decrypt\_tiles** fonksiyonu, her bir şifreli parçayı ilgili anahtarla deşifre ederek bir listeye ekler. Deşifreleme sırasında bir hata oluşursa, hata mesajı verir ve None döner. Başarılı olduğunda, tüm deşifre edilmiş parçaları bir liste olarak geri döner.



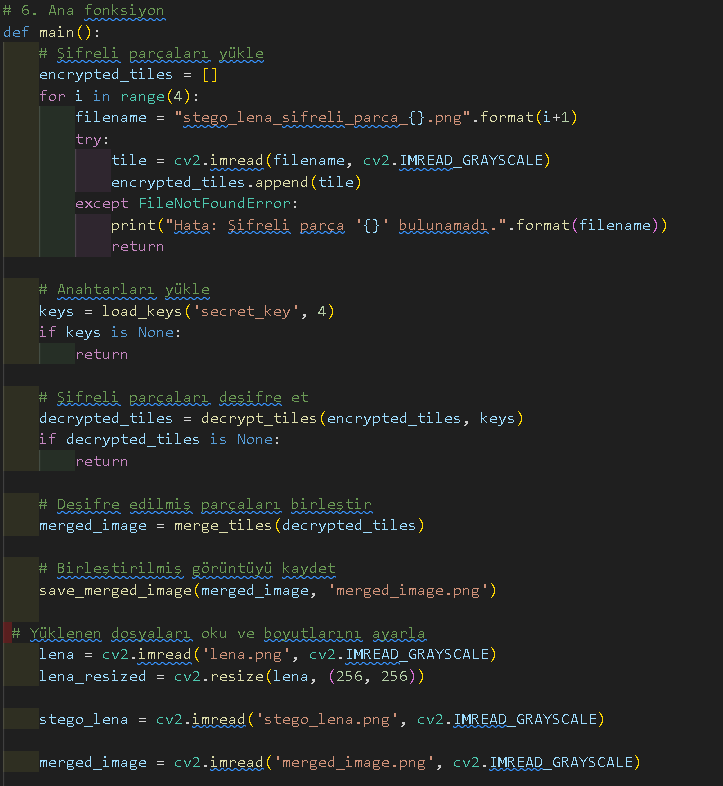


Deşifre edilmiş görüntü parçalarını birleştirir ve kaydeder. **merge\_tiles** fonksiyonu, parçaları belirli bir düzenle birleştirerek orijinal görüntüyü yeniden oluşturur. Her bir parçayı uygun konuma yerleştirerek tam boyutlu bir görüntü elde eder. **save\_merged\_image** fonksiyonu ise, bu birleştirilmiş görüntüyü belirtilen dosya adına kaydeder ve işlemin başarılı olduğunu belirten bir mesaj verir.

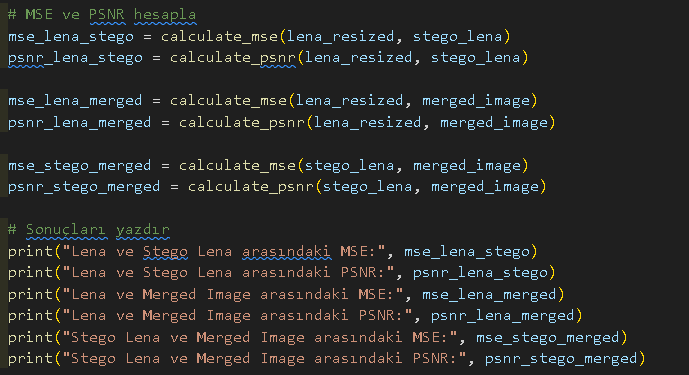


**calculate\_mse** fonksiyonu, orijinal ve stego görüntüleri arasındaki Ortalama Kare Hatasını (MSE) hesaplar. **calculate\_psnr** fonksiyonu ise, bu MSE değerini kullanarak iki görüntü arasındaki Pik Sinyal-Gürültü Oranını (PSNR) hesaplar.

MSE sıfır olduğunda, PSNR sonsuz olarak döner. Bu fonksiyonlar, görüntülerin karşılaştırılması ve kalitelerinin değerlendirilmesi için kullanılır.



Şifreli görüntü parçalarını yükler, bu parçaları belirtilen anahtarlarla deşifre eder, ardından deşifre edilmiş parçaları birleştirip kaydeder. İlk olarak, şifreli parçalar yüklenir ve eksik dosyalar için hata kontrolü yapılır. Deşifreleme işlemi gerçekleştirilir son olarak, birleştirilmiş görüntü kaydedilir.



Son olarak resimler arasındaki PSNR ve MSE değerleri hesaplanır ve ekrana yazdırılır.

Orijinal görüntü Stego görüntü

Stego görüntüsünün parçalanmış hali Anahtarla şifrelenmiş stego görüntüsü



  Birleştirilmiş görüntü

Deşifreleme sonucu her bir parça

görüntünün çıktısı