# **Yazılım Güvenliği**

## **Stenografi Kavramı ve Uygulaması**

### **Hazırlayan:**

Ali ARSLAN

### **Stenografi Kavramı**

**Tanım:** Stenografi, bir bilginin doğrudan içeriğini değil, varlığını gizlemeye yönelik bir tekniktir. Veri, bir taşıyıcı (örn. resim, ses, video) içerisine entegre edilerek gizlenir ve böylece iletişim doğal görünümünü korur. Kriptografiden farklı olarak, burada gizli iletişimin varlığı bile mümkün olduğunca saklanmaya çalışılır.

**Tarihçe:** Stenografi uygulamaları antik çağlara dayanmaktadır. Örneğin, Antik Yunan'da gizli yazılar, balmumu kaplı tabletlerin altına kazınarak iletiliyordu. Orta Çağ boyunca görünmez mürekkepler ve kodlu yazışmalar kullanıldı. 20. yüzyılda mikrofilm teknolojileri geliştirildi. Günümüzde ise, stenografi kavramı dijital dosyalar (resim, ses, video) üzerinde uygulanarak çok daha sofistike bir hal almıştır.

**Dijital Dünyadaki Önemi:**

* Dijital ortamda veri güvenliği sağlama
* Fikri mülkiyet koruması (örn. dijital watermarking)
* Kimlik doğrulama ve belge bütünlüğü kontrolü
* Bilgi sızdırmayı önlemeye veya gerçekleştirmeye yönelik siber güvenlik uygulamaları

**Stenografi ve Kriptografi Arasındaki Farklar**

|  | **Stenografi** | **Kriptografi** |
| --- | --- | --- |
| **Amaç** | Bilginin varlığını gizlemek | Bilginin içeriğini okunamaz hale getirmek |
| **Görünürlük** | Gizlenmiş veri normal veri gibi görünür | Şifreli veri dikkat çeker |
| **Güvenlik Temeli** | Gizliliğin fark edilmemesi | Matematiksel hesaplamaların kırılması zorluğu |
| **Risk Durumu** | Bulunursa içerik doğrudan açığa çıkar | Bulunsa bile çözülmesi zaman alır |

Kısaca, stenografi bir iletişimin "**var olup olmadığını**" gizlerken, kriptografi iletişimin "**anlamını**" gizler.

**Görsel Tabanlı Stenografinin Temel Prensipleri**

Görsel tabanlı (image-based) stenografide, gizli veri bir görsel dosyasının içine entegre edilir. Bu süreç belirli teknik prensiplere dayanır:

* **Taşıyıcı (Cover) Dosya Seçimi:**  
  Genellikle kayıpsız formatlar (BMP, PNG) tercih edilir. JPEG gibi kayıplı sıkıştırmalar veri kaybı oluşturabileceği için risklidir.
* **LSB (Least Significant Bit) Tekniği:**  
  Piksel değerlerinin en düşük öneme sahip bitleri değiştirilerek veri yerleştirilir. Örneğin, bir RGB pikselde yalnızca son biti değiştirerek görselde insan gözüyle algılanamayacak değişimler yapılır.
* **Dağıtılmış Veri Gömme:**  
  Verinin doğrudan ardışık piksellere değil, belirli bir algoritmaya (örn. rastgele seçim) göre dağıtılması, stenografik tespiti daha da zorlaştırır.
* **Ön Şifreleme:**  
  Gizlenen verinin ayrıca kriptografik olarak şifrelenmesi, bir saldırı durumunda verinin açığa çıkmasını daha da güçleştirir.

Bu prensipler, yazılım projelerinde hem gizli iletişim uygulamalarında hem de dijital telif koruma sistemlerinde temel yapı taşıdır.

**Etik Kullanımı ve Riskler**

**Etik Kullanım Alanları:**

* Sansür uygulamalarının olduğu bölgelerde güvenli iletişim sağlamak
* Telif hakkı koruması için eser sahipliğini göstermek
* Bireysel verilerin siber saldırılardan korunması

**Riskler:**

* Malware ve ransomware saldırılarında veri gizlemek amacıyla kullanılması
* Şirket içi veri sızıntılarında kritik bilgilerin dışarı çıkarılması
* Adli bilişim süreçlerinde delil karartma amaçlı kullanımı

Bu yüzden, yazılım geliştiricilerinin stenografi tekniklerini kullanırken hem **etik ilkelere** hem de **yasal düzenlemelere** dikkat etmesi gerekir.

### **Uygulama**

**Özet**

Bu Python programı, **steganografi** yöntemiyle bir resmi kullanarak içine gizli bir mesaj gömmeyi (**encode**) ve gömülü mesajı tekrar çıkarmayı (**decode**) sağlar. Program, mesajı resmin piksellerinin en düşük anlamlı bitine (LSB) yerleştirir. Mesajın sonuna özel bir bit dizisi (delimiter) eklenerek, mesajın nerede bittiği anlaşılır. Kullanıcı, isterse bir mesajı resme gizleyebilir, isterse daha önce gizlenmiş bir mesajı çözebilir.

**Kod Açıklamaları**

**1. text\_to\_binary(text)**

* Verilen bir metni (string) **ikili (binary)** formata çevirir.
* Her karakter, ASCII karşılığı olan 8 bitlik ikili sayıya dönüştürülür.

**2. binary\_to\_text(binary\_str)**

* Verilen ikili veriyi tekrar **metne (string)** çevirir.
* 8 bitlik parçalara ayırır ve her parçayı ASCII karakterine dönüştürür.

**3. encode\_image(image\_path, secret\_text, output\_path)**

* Bir resim dosyasını açar ve içine gizli mesajı yerleştirir.
* Gizli mesaj ikili koda çevrilir, sonuna **'1111111111111110'** adlı ayırıcı (delimiter) eklenir.
* Mesajın her biti, resim piksellerinin RGB değerlerinin en düşük bitine yazılır.
* Eğer mesaj çok büyükse ve resme sığmıyorsa hata verir.
* İşlem bitince yeni bir resim oluşturur ve kaydeder.

**4. decode\_image(image\_path)**

* Gizli mesaj içeren resmi açar.
* Tüm piksellerin RGB değerlerinin en düşük bitlerini okuyarak bir ikili dizi oluşturur.
* **Delimiter** bulunana kadar veriyi toplar.
* Bulunan ikili veriyi tekrar metne çevirir ve ekrana yazdırır.

**5. main()**

* Kullanıcıya bir menü sunar:
  + 1 seçilirse mesaj gizleme işlemi başlar.
  + 2 seçilirse mesaj çıkarma işlemi yapılır.
* Yanlış girişlerde hata mesajı verir.
* Kullanıcıdan dosya yolları ve mesaj bilgilerini alır.

**Kullanılan Yöntem: LSB (Least Significant Bit)**

* Her pikselin renk değerinin (R, G, B) en düşük biti (1 bit) değiştirilerek mesaj saklanır.
* İnsan gözü bu küçük değişiklikleri fark edemez, böylece mesaj gizlenmiş olur.
* **Delimiter** sayesinde gizli mesajın bittiği yer belirlenir.

**dış mekan, bulut, manzara, gökyüzü içeren bir resim

Yapay zeka tarafından oluşturulan içerik yanlış olabilir.dış mekan, bulut, manzara, gökyüzü içeren bir resim

Yapay zeka tarafından oluşturulan içerik yanlış olabilir.Input Image:** **Output Image:**

**Uygulama Ekran Görüntüleri**

**metin, ekran görüntüsü, yazılım, ekran, görüntüleme içeren bir resim

Yapay zeka tarafından oluşturulan içerik yanlış olabilir.metin, ekran görüntüsü, yazılım, işletim sistemi içeren bir resim

Yapay zeka tarafından oluşturulan içerik yanlış olabilir.metin, ekran görüntüsü, yazılım, multimedya yazılımı içeren bir resim

Yapay zeka tarafından oluşturulan içerik yanlış olabilir.**