T.C.
TRAKYA ÜNİVERSİTESİ

FEN BİLİMLERİ ENSTİTÜSÜ

STEGANOGRAFİK GİZLİ GÖRÜNTÜ PAYLAŞIM ŞEMALARININ İNCELENMESİ VE UYGULAMALARI

SERMİN KAVAK

YÜKSEK LİSANS TEZİ

HESAPLAMALI BİLİMLER ANABİLİM DALI

Tez Danışmanı: Dr. Öğr. Üyesi Derya ARDA

EDİRNE-2019

Sermin KAVAK' ın hazırladığı "Steganografik Gizli Görüntü Paylaşım Şemalarının İncelenmesi Ve Uygulamaları" başlıklı bu tez, tarafımızca okunmuş, kapsam ve niteliği açısından Hesaplamalı Bilimler Anabilim Dalında bir Yüksek lisans tezi olarak kabul edilmiştir.

Jüri Üyeleri — İmza

Doç. Dr. M. Tolga Sakallı .....

Dr. Öğrt. Üyesi Halil Nusret Buluş .....

Dr. Öğrt. Üyesi. Derya Arda .....

Tez Savunma Tarihi: 17/07/2019

Bu tezin Yüksek Lisans tezi olarak gerekli şartları sağladığını onaylarım.

İmza

Dr. Öğrt. Üyesi. Derya ARDA
Tez Danışmanı .....

Trakya Üniversitesi Fen Bilimleri Enstitüsü onayı

Prof. Dr. Murat YURTCAN

Fen Bilimleri Enstitüsü Müdürü

T.Ü.FEN BİLİMLERİ ENSTİTÜSÜ

HESAPLAMALI BİLLİMLER ANABİLİM DALI YÜKSEK LİSANS PROGRAMI

DOĞRULUK BEYANI

Trakya Üniversitesi Fen Bilimleri Enstitüsü, tez yazım kurallarına uygun olarak hazırladığım bu tez çalışmasında, tüm verilerin bilimsel ve akademik kurallar çerçevesinde elde edildiğini, kullanılan verilerde tahrifat yapılmadığını, tezin akademik ve etik kurallara uygun olarak yazıldığını, kullanılan tüm literatür bilgilerinin bilimsel normlara uygun bir şekilde kaynak gösterilerek ilgili tezde yer aldığını ve bu tezin tamamı ya da herhangi bir bölümünün daha önceden Trakya Üniversitesi ya da farklı bir üniversitede tez çalışması olarak sunulmadığını beyan ederim.



17/07/2019

Sermin Kavak

iii

Yüksek Lisans Tezi
Steganografik Gizli Görüntü Paylaşım Şemalarının İncelenmesi Ve Uygulamaları
T.Ü. Fen Bilimleri Enstitüsü
Hesaplamalı Bilimler Anabilim Dalı

ÖZET

Günümüzde, haberleşme sistemlerinde bilgi akışının artması ve bu sebeple güvenlik açıklarının ve siber saldırıların olması bilginin dış ortamlara karşı korunmasını gerektirmiştir. Bu nedenle bilginin gizliliğini ve güvenliğini sağlamak için pek çok yöntemler kullanılmaktadır. Bunlardan bazıları steganografi ve kriptolojidir. Steganografide amaç sır bilgiyi bir ortama saklamaktır. Kriptolojide amaç sır bilginin çeşitli algoritmalarla şifrelenerek anlamsız hale getirilmesidir. Bu yöntemlerin dışında sır bilginin ya da şifrelemede kullanılan gizli anahtarın korunması için Sır Paylaşım Şemaları (SPŞ) vardır. Bu şemalar aynı zamanda (k,n) eşik sır paylaşım şemaları olarak bilinir. SPŞ ile sır bilginin güvenliğini sağlamak için saklamak ya da tek bir kişide bulunması problemi ortadan kalkmıştır. Bir (k,n) eşik sır paylaşım şemasında gizli bilgi n paya dağıtılır ve ancak k pay ile sır bilgi yeniden elde edilebilir.

Bu tezde şifrelemede kullanılan gizli anahtarın ya da gizli bilginin güvenliğini sağlamak için görüntü steganografi ve sır paylaşım şemalarının birlikte kullanılması üzerinedir. Gizli anahtar olarak bir şifreleme algoritmasının anahtarı ya da gizli bir metin seçilen görüntünün RGB renk kanalında sadece mavi kanala gizlenmiştir. Bilgi gizleme aşamasında LSB ve 2LSB yöntemleri kullanılmıştır. Daha sonra bu görüntü Shamir' in polinomsal tabanlı Thien- Lin sır paylaşım şeması ve Çin Kalan teorisi tabanlı Asmuth-Bloom şeması ile anlamsız pay görüntülere bölünmüştür. Yapılan uygulama PSNR, MSE, SSIM, Korelasyon katsayısı ve Histogram analizleri ile

değerlendirilmiştir. Sonuç olarak bu iki güvenlik yöntemleri ile gizli bilginin güvenliğinin arttığı gösterilmiştir.

Bu tezde yapılan çalışmalardan esinlenerek veri güvenliğini arttırmada farklı şifreleme teknikleri, farklı bilgi gizleme yöntemleri, farklı sır paylaşım şemaları ve kodlama teorisi gibi alanların birlikte kullanımının etkili olacağı söylenebilir.

Yıl : 2019
Sayfa Sayısı : 76
Anahtar Kelimeler : Gizli görüntü paylaşımı, Steganografi, Kriptoloji, Sır Paylaşım Şemaları

Master's Thesis

An Investigation of Steganographic Secret Image Sharing Schemes and its applications

Trakya University Institute of Natural Sciences

Computational Science Department

ABSTRACT

Nowadays, increase of the flow of information in communication systems and therefore occurence of security vulnerability and cyber attacks have required the protection of information against external environments. Therefore, many methods have been used to provide protection and security of the information. Some of these are steganography and cryptology. The main purpose of steganography is to conceal an information within a media. The purpose of cryptology is to make the secret information meaningless by encrypting it with various algorithms. Apart from these methods, there are Secret Sharing Schemes (SSS) for the protection of secret information or secret key used in encryption. These schemes are also known as (k,n) threshold secret sharing schemes. With the SSS, the problem of keeping the secret information in order to secure it or having it in a single person is eliminated. In a (k, n) threshold secret sharing scheme, confidential information is distributed to n shares, and only with k share, secret information can be recovered.

In this thesis, image steganography and secret sharing schemes are used together to secure the secret information or seret key used in encryption. The secret key an encryption algorithm or a secret text has been hidden in the RGB color channel of the selected image only to the blue channel. LSB and 2LSB methods were used in the process of hiding information. Later, this image was divided into meaningless share images by Shamir's polynomial based Thien-Lin secret sharing scheme and the Chinese remainder theory-based Asmuth-Bloom scheme. The application was evaluated by

PSNR, MSE, SSIM, correlation coefficient and histogram analysis. As a result, it has been shown that the security of confidential information increases with these two security methods.

Inspired by the studies conducted in this thesis, it can be stated that the use of different encryption techniques, different information hiding methods, different secret sharing schemes and coding theory will be effective in increasing the data security.

.

Year: 2019
Number of Pages: 76
Keywords: Hidden image Sharing, Secret Sharing Schemes, Steganography, Cryptology,

TEŞEKKÜR

Tez danışmanlığımı üstlenen daima beni yüreklendiren, yol gösteren çok sevdiğim değerli hocam Dr. Öğrt. Üyesi Derya ARDA' ya en içten teşekkürlerimi sunuyorum.

Tez çalışmam sırasında yardımlarını esirgemeyen yapıcı görüşleri ile destek veren saygıdeğer hocam Doç. Dr. M. Tolga SAKALLI' ya teşekkür ediyorum.

Ayrıca çalışmamda yaptıkları yardımlarından dolayı Bilgisayar Mühendisi Selin DEMİRBİLEK' e, Okcan AYYILDIZ' a ve Muammer YILMAZ' a teşekkürlerimi sunuyorum.

Son olarak bugünlere gelmemde en büyük paya sahip sevgili aileme, desteğini hep hissettiğim daima yanımda olan Abdurrahman BEŞER' e ve tüm arkadaşlarıma teşekkür ederim.

İÇİNDEKİLER

ÖZET iv
ABSTRACT vi
TEŞEKKÜR viii
ŞEKİLLER DİZİNİ xii
ÇİZELGELER DİZİNİ xiv
KISALTMALAR DİZİNİ xv
BÖLÜM 1 1
GİRİŞ 1
BÖLÜM 2 3
KRİPTOLOJİ 3
2.1. Kriptolojiye Giriş 3
2.2. Asimetrik Şifreleme Algoritması 4
2.3. Simetrik Şifreleme Algoritmaları 5
2.3.1. AES Şifreleme Algoritması 5
BÖLÜM 3 8
STEGANOGRAFİ 8
3.1. Steganografik Yöntemler 9
3.1.1. Metin Steganografi 9
3.1.2. Ses Steganografi 9
3.1.3. Görüntü Steganografi 10
BÖLÜM 4 14
SIR PAYLAŞIM ŞEMALARI 14

4.1. Genel Sır Paylaşımı Tanımı 14
4.2. Shamir' in Polinomsal Tabanlı Sır Paylaşım Şeması 15
4.3. Çin Kalan Teoremi Tabanlı Sır Paylaşım Şemaları 17
4.3.1. Asmuth-Bloom Sır Paylaşım Şeması 17
4.4. Blakley' in Geometrik Tabanlı Sır Paylaşım Şeması 19
4.4.1. Blakley' in Sır Paylaşım Şeması 19
4.5. Gizli Görüntü Sır Paylaşımı 20
4.5.1. Thien ve Lin Sır Paylaşım Şeması 21
BÖLÜM 5 23
ANALİZ YÖNTEMLERİ 23
5.1. Uygulamada Kullanılan Analizler 23
5.2. PSNR (Tepe Sinyal Gürültü Oranı) 23
5.3. SSIM (Yapısal Benzerlik Endeksi Ölçütü) 24
5.4. Korelasyon Katsayısı (Correlation Coefficient) 24
5.5. Histogram Testi 25
BÖLÜM 6 27
UYGULAMANIN GERÇEKLEŞTİRİLMESİ 27
6.1. Kriptografik Anahtarın veya Gizli Verinin Güvenliğinde Steganografi ile Thien-Lin' in Görüntü Sır Paylaşımı Uygulaması ve Analizleri 27
6.1.1. LSB Yöntemi İle Görüntünün Mavi Kanalına Bilgi Gizleme Ve Thien-Lin Görüntü Sır Paylaşımı Uygulaması 27
6.1.2. LSB yöntemi ve Thien-Lin Görüntü Sır Paylaşımı Uygulamasının Analizi 36
6.1.3. 2LSB ile görüntünün mavi kanalına bilgi gizleme ve Thien-Lin GSP Şeması Uygulaması 39

6.1.4. 2LSB yöntemi ve Thien-Lin Görüntü Sır Paylaşımı Uygulamasının Analizi 41

6.2. Kriptografik Anahtarın Veya Gizli Verinin Güvenliğinde Steganografi ile Çin kalan teorisi tabanlı Asmuth-Bloom Şeması ile Görüntü Sır Paylaşımı Uygulaması ve Analizleri 45

6.2.1. 2LSB ile veri gizlenmiş görüntünün Çin kalan teorisi tabanlı Asmuth-Bloom Şeması ile Görüntü Sır Paylaşım Uygulaması 45

6.2.2. 2LSB ile Veri Gizlenmiş Görüntünün Çin Kalan Teorisi Tabanlı Asmuth-Bloom Şeması ile Görüntü Sır Paylaşımının Analizi 49

BÖLÜM 7 53

SONUÇ VE ÖNERİLER 53

KAYNAKLAR 56

ÖZGEÇMİŞ 60

TEZ ÖĞRENCİSİNE AİT TEZ İLE İLGİLİ BİLİMSEL FAALİYETLER 61

ŞEKİLLER DİZİNİ

Şekil 2.1. Asimetrik Şifreleme Algoritması Şeması....4
Şekil 2.2. Simetrik Şifreleme Algoritması Şeması....5
Şekil 2.3. AES Şifreleme Algoritmasının Genel Tasarımı....6
Şekil 2.4. AES şifreleme algoritmasında bir turdaki işlemler....7
Şekil 3.1. Sayısal Steganografi yöntemlerinin sınıflandırılması....9
Şekil 3.2. Görüntüler için bilgi gizleme şeması....10
Şekil 3.3. LSB Yönteminin Uygulanması....11
Şekil 3.4. 2LSB Yönteminin Uygulanması....13
Şekil 4.1. Blakley sır paylaşım şeması....19
Şekil 5.1. 256x256 boyutlu Lena.bmp Histogramı....25
Şekil 5.2. 2LSB ile Mavi kanala gizlenmiş veri olan Lena bmp. Histogramı....26
Şekil 6.1. Gizli Görüntü Paylaşımı, Steganografik Metot ve şifreleme (AES ya da herhangi bir şifreleme algoritması) İşlemleri....28
Şekil 6.2. Bir gizli anahtarın LSB ya da 2LSB ile Lena bmp.gizlenmesi ve (2,4) Thien-Lin Şeması ile pay görüntülere bölünmesi....29
Şekil 6.3. 256 x 256 Lena.bmp görseli....30
Şekil 6.4. Gizli Görüntünün, gizli anahtarın yeniden elde edilme ve şifre çözme işlemleri....33
Şekil 6.5. k=2 pay görüntüden gizli anahtarın ve gizli görüntünün elde edilmesi....34
Şekil 6.6. AES Şifreleme....35
Şekil 6.7. AES Şifre Çözme....35
Şekil 6.8. Lena.bmp, (LSB) Stego-Lena bmp ve histogramları....36
Şekil 6.9. Permüte edilen resim (f), pay1(g), pay2(h), pay3(t), pay4(k) payları, (1-2) payları ile yeniden elde edilen resim (m) histogram analizi....38
Şekil 6.10. 6872 bit veri gömülmüş görüntü için (2,4) Thien-Lin Şeması Uygulaması39

Şekil 6.11. k=2 pay görüntüyle görüntüyü yeniden elde etme ve gömülü gizli bilgiyi çıkarma uygulaması 41
Şekil 6.12. Orijinal ve 2LSB yöntemiyle bilgi gizlenmiş görüntünün permütasyonlu görüntüsü 41
Şekil 6.13. Sırasıyla Pay 1 (80bit) ve (6872 bitlik) metin gömülüye ait histogramlar . 42
Şekil 6.14. Sırasıyla Pay 2 (80bit)ve (6872 bitlik) metin gömülüye ait histogramlar .. 42
Şekil 6.15. Sırasıyla Pay 3 (80bitlik) ve (6872) bitlik metin gömülüye ait histogramlar 42
Şekil 6.16. Sırasıyla Pay 4 (80bitlik) ve (6872) bitlik metin gömülüye ait histogramlar 43
Şekil 6.17. Pay1 ve Pay2 ile elde edilen gizli anahtar gömülü resmin histogramı 43
Şekil 6.18. Pay3 ve Pay4 ile elde edilen gizli metin gömülü(6872bit) resmin histogramı 43
Şekil 6.19. 2LSB ile Mavi kanala gizli anahtar(80bit) gömülü resmin histogramı..... 44
Şekil 6.20. 2LSB ile Mavi kanala 6872bit gömülü resme ait histogram..... 44
Şekil 6.21. 80 bit gizli veri gömülü stego-görüntüsüne seçilen asallarla Çin kalan Teorisi tabanlı Asmuth- Bloom GSP şeması ile n=4 Pay görüntüye bölünmesi..... 46
Şekil 6.22. Çin Kalan Teoremini kullanarak (1-2-3) Pay görüntüleri ile permütasyonlu görüntünün elde edilmesi 47
Şekil 6.23. Stegolu görüntü ve gizli verinin elde edilmesi 47
Şekil 6.24. 6872 bit gizli veri gömülü stego-görüntüsüne seçilen asallarla Çin kalan Teorisi tabanlı Asmuth- Bloom GSP şeması ile n=4 Pay görüntüye bölünmesi..... 48
Şekil 6.25. Çin Kalan Teoremini kullanarak (1-3-4) Pay görüntüleri ile permütasyonlu görüntünün elde edilmesi 48
Şekil 6.26. Stegolu görüntü ve gizli verinin elde edilmesi 49
Şekil 6.27. Asmuth-Bloom GSP şemasıyla elde edilen pay görüntülerin histogramları 51
Şekil 6.28. 80 bit veri gömülü olan (1-3-4) Pay görüntüleri ile elde edilen görüntünün histogramı 51
Şekil 6.29. 6872 bit veri gömülü olan (1-3-4) Pay görüntüleri ile elde edilen görüntünün histogramı 52

ÇİZELGELER DİZİNİ

Çizelge 2.1. Bazı Şifreleme Algoritmaları.....4
Çizelge 6.1. Orijinal, LSB-mavi kanala gömülü, permütasyonlu Lena bmp. Görselinin Piksel Renk Değerleri 30
Çizelge 6.2. Pay görüntülerin [0,0]. renk piksel değerleri.....32
Çizelge 6.3. Orijinal, 2LSB-mavi kanala 80 bit(gizli anahtar) gömme, ve permütasyonlu Lena bmp. Görselinin 1x3'lük Piksel Renk Değerleri.....40
Çizelge 6.4. 1x3 boyutlu pay görüntülerin renk piksel değerleri.....40
Çizelge 6.5. 2LSB yöntemi ile 80bit ve 6872bit gömülü Görüntüler ve Thien-Lin Şeması ile elde edilen görüntülerin PSNR, MSE, SSIM, Korelasyon testi sonuçları ..45
Çizelge 6.6. 2LSB yöntemi ile 80bit ve 6872bit gömülü Görüntüler ve Asmuth-Bloom GSP şeması ile elde edilen görüntülerin PSNR, MSE, SSIM, Korelasyon testi sonuçları 50

KISALTMALAR DİZİNİ

AES	Advanced Encryption Standard(İleri Şifreleme Standardı)
GSP	Görsel Sır Paylaşım
MSE	Mean Squared Error (Hata Kare Ortalama)
LSB	Least Significant Bit (En Önemsiz Bit)
2LSB	2 Least Significant Bit (En Önemsiz 2 Bit)
PSNR	Peak Signal To Noise Ratio (Tepe Sinyal Gürültü Oranı)
SPŞ	Sır Paylaşım Şemaları
SSIM	Structural Similarity Indeks (Yapısal Benzerlik Endeksi Ölçütü)
CC	Correaliton Coefficient (Korelasyon Katsayısı)

BÖLÜM 1

GİRİŞ

İnternet kullanımının yaygınlaşması ve bulut teknolojisinin kullanımının artmasıyla birlikte, sayısal ortamda verilerin güvenli bir şekilde saklanması, korunması, iletilmesi gibi bilgi güvenliği gereksinimleri gittikçe artmaktadır. Bilgi güvenliğini sağlayabilmek için çeşitli yöntemler ve protokoller kullanılmaktadır. Yaygın olarak kullanılan güvenlik yöntemlerinin başında kriptoloji ve steganografi gelmektedir.

Kriptolojide amaç gizli veriyi bir anahtar yardımıyla anlaşılmaz forma getirmektir. Kriptolojik algoritmalarda kullanılan anahtar gizli ya da açık olabilir. Anahtar seçimine göre simetrik (gizli anahtarlı) ve asimetrik (açık anahtarlı) şifreleme olarak bilinir (Stinson, 2002). Kriptografide kullanılan şifreleme anahtarının gizli kalması çok önemlidir. Bunun gibi anahtar yönetim sorunlarına çözüm olarak literatürde pek çok protokoller önerilmiştir. Bunlardan birisi Shamir (Shamir, 1979) ve Blakley (Blakley, 1979) tarafından önerilen sır paylaşım şemalarıdır. Bu şemalar aynı zamanda (k,n) eşik sır paylaşım şemaları olarak bilinmektedir. Bir (k,n) şemasında temel olarak gizli bilgi tek parça olarak bir yerde olması yerine n paylara ayrılır k adet payın bir araya gelmesi ile yeniden elde edilir. Bu sayede gizli anahtarın ya da gizli bilginin güvenliği sağlanmış olur.

Steganografi şifrelemeden farklı olarak verinin içeriğini karmaşık hale getirmek değil içeriği bir ortama saklamaktır. Steganografinin kelime anlamı gizlenmiş yazı demektir (Petitcolas, Anderson, & Kuhn, 1999). İletmek istediğimiz gizli bilgiyi saklamak ve üçüncü kişilerin eline geçmemesi için bir örtü nesnesi olarak sayısal resim, metin, ses ya da video dosyası kullanılabilir (Wang & Wang, 2004).

Bu tezde Bölüm 2’ de kriptolojinin temelleri üzerinde genel bilgiler verilmiştir. Uygulamada kullanılmış olan AES şifreleme algoritmasının genel yapısı ve işleyişi anlatılmıştır.

Bölüm 3’ de Steganografi bilimi anlatılmıştır. Uygulamada kullanılan LSB ve 2LSB bilgi gizleme teknikleri açıklanmıştır.

Bölüm 4’ de Sır Paylaşım Şemaları anlatılmıştır. Özellikle Shamir’ in polinom tabanlı Sır Paylaşımı, Asmuth-Bloom tarafından önerilen Çin Kalan Teorisi tabanlı Sır Paylaşım Şeması, Blakley’ in geometrik tabanlı Sır Paylaşım Şeması ve görüntü sır paylaşımı için Thien-Lin’ in Shamir’ in polinomsal tabanlı şeması açıklanmıştır.

Bölüm 5’ de gerçekleştirilen uygulamanın değerlendirilmesinde kullanılan PSNR, MSE, SSIM, Korelasyon analizi ve Histogram testi yöntemleri açıklanmıştır.

Bölüm 6’ de şifrelemede kullanılan herhangi bir gizli anahtarın ya da sır bilginin güvenliği için LSB ve 2LSB bilgi gizleme yöntemi ile birlikte Thien-Lin yöntemine göre sır görüntü paylaşım şeması ve Asmuth-Bloom’ un Çin Kalan Teorisi tabanlı sır görüntü paylaşım şemasının uygulaması yapılmıştır. Ayrıca seçilen bir gizli anahtar ile 128 bitlik bir AES şifreleme algoritmasıyla bir uygulama gerçekleştirilmiştir.

Yapılan uygulamalar PSNR, MSE, SSIM, Korelasyon analizi ve Histogram testleri ile değerlendirilmiştir.

BÖLÜM 2

KRİPTOLOJİ

2.1. Kriptolojiye Giriş

Kriptoloji kriptografi ve kriptoanaliz olarak temel iki alanı birleştiren şifreleme bilimidir. Kriptografi, bilgi güvenliğini sağlamak için geliştirilmiş çeşitli matematiksel yöntemlerdir. Bu yöntemlerde gizlilik, güvenilirlik, veri bütünlüğü, erişilebilirlik, kimlik doğrulama ve reddedilemezlik esasları üzerinde çalışılır. Ayrıca bir bilginin istenmeyen taraflarca anlaşılamayacak bir hale dönüştürülmesi ile bilgiyi, göndereni ve alıcıyı korumak için geliştirilmiştir. Kriptanaliz ise şifreli metinlerden farklı teknikler kullanarak açık metinleri elde etme işlemidir.

Bir kripto sistem açık metin, şifreleme algoritması, anahtar ve şifreli metinden oluşmaktadır (Stinson, 2002).

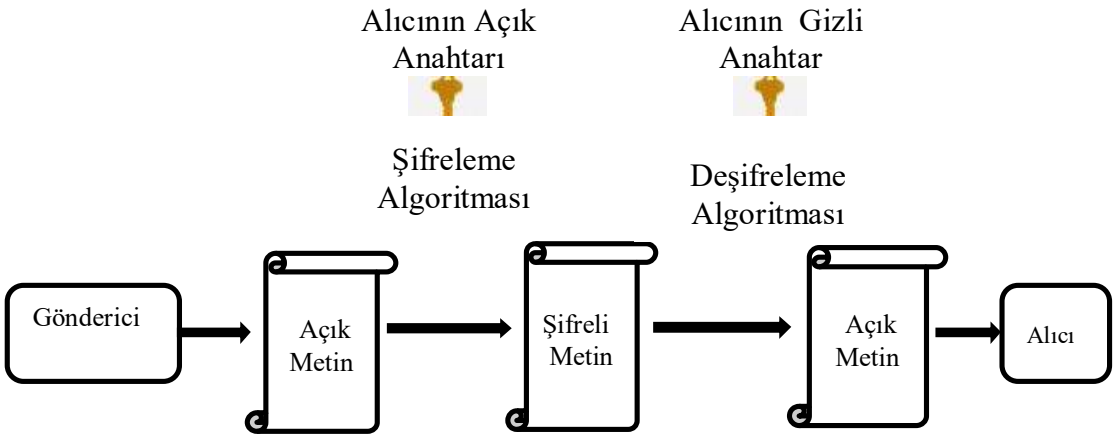
Şifreleme algoritmaları asimetrik (açık anahtarlı) ve simetrik (gizli anahtarlı) algoritmalar olarak iki kategoride incelenmektedir. Bazı şifreleme algoritmaları Çizelge 2.1' de verilmiştir.

Çizelge 2.1. Bazı Şifreleme Algoritmaları

Simetrik Şifreleme Algoritmaları		Asimetrik Şifreleme Algoritmaları
Blok Şifreler	Akan Şifreler	RSA ElGamal ECC
DES-IDEA Square -AES Camellia- ARIA Khazad	RC4 Trivium HC-256	

2.2. Asimetrik Şifreleme Algoritması

Asimetrik şifreleme algoritmalarında şifrelemede açık bir anahtar kullanılırken şifre çözmede gizli anahtar kullanır. Asimetrik şifreleme algoritmalarından bazıları RSA (Rivest, Shamir, & Adleman, 1978), ECC (Koblitz , 1987) ve Elgamal (Elgamal, 1985) dır. Bu algoritmanın çalışma mantığı Şekil 2.1' de verilmiştir.

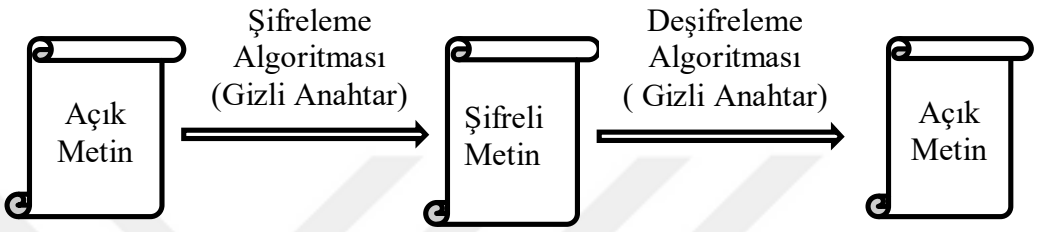


Şekil 2.1. Asimetrik Şifreleme Algoritması Şeması

Kriptografi sadece veriyi gizlemek, iletmek ve saldırıları engellemek gibi konulara çözüm aramaz. Elektronik imza, elektronik seçim vb. gibi farklı alanlarda da kullanılır. Şifrelemede kullanılan anahtarın korunması için pek çok yöntemler ortaya atılmıştır. Bunlardan birisi de sır paylaşım şemalarıdır.

2.3. Simetrik Şifreleme Algoritmaları

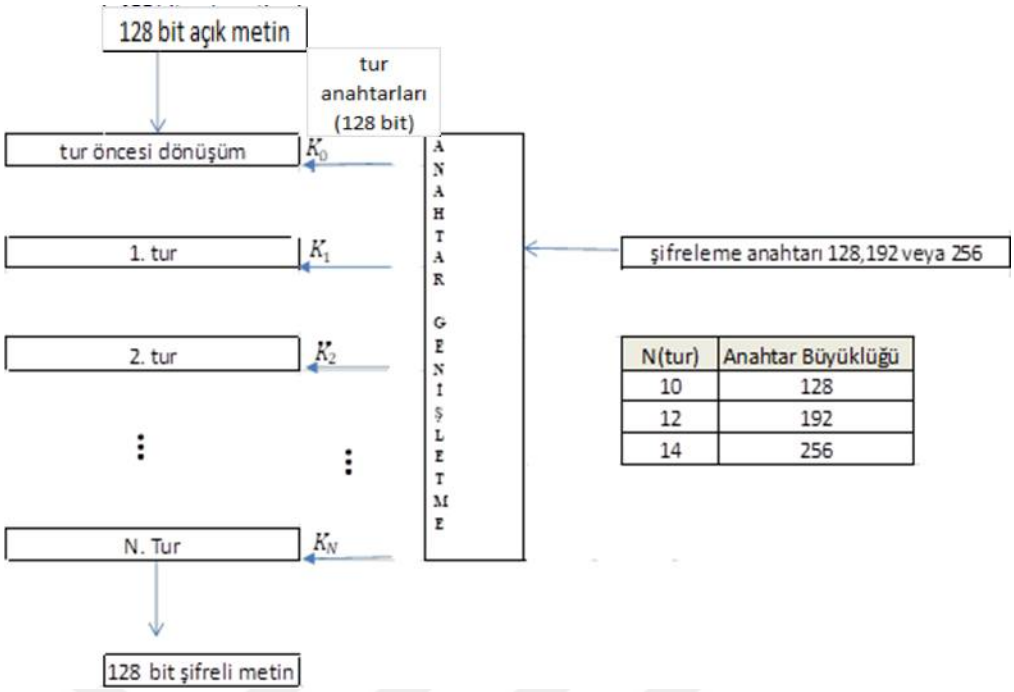
Simetrik şifreleme algoritmalarında şifreleme ve şifre çözme işlemlerinde aynı gizli anahtar kullanılır. Şifreleme işleminde açık metin gizli anahtar ile şifrelenirken şifre çözme işleminde de aynı gizli anahtarla şifreli metin çözülür (Stinson, 2002). Simetrik şifreleme algoritmalarının çalışma biçimi Şekil 2.2' de gösterilmiştir.



Şekil 2.2. Simetrik Şifreleme Algoritması Şeması

2.3.1. AES Şifreleme Algoritması

Joan Daemen ve Vincent Rijmen (Daemen & Rijmen, 2002) tarafından geliştirilmiş FIBS-197 (FIBS PUB-197, 2001) onaylı AES (Rijndael) şifreleme algoritması 128 bit veri bloklarını 128, 192, 256 bit anahtar seçenekleri ile şifreleme yapan bir algoritmadır. AES Algoritması farklı uzunlukta anahtarlara göre farklı sayıda döngüsel işlemler yapar. 128 bit anahtar için 10 döngüde şifreleme yaparken 192 ve 256 bit anahtarlar için sırasıyla 12 ve 14 döngüde şifreleme yapmaktadır. AES Algoritmasındaki anahtar uzunluğu ile tur ilişkisi ve genel tasarımı aşağıdaki Şekil 2.3' de gösterilmiştir.



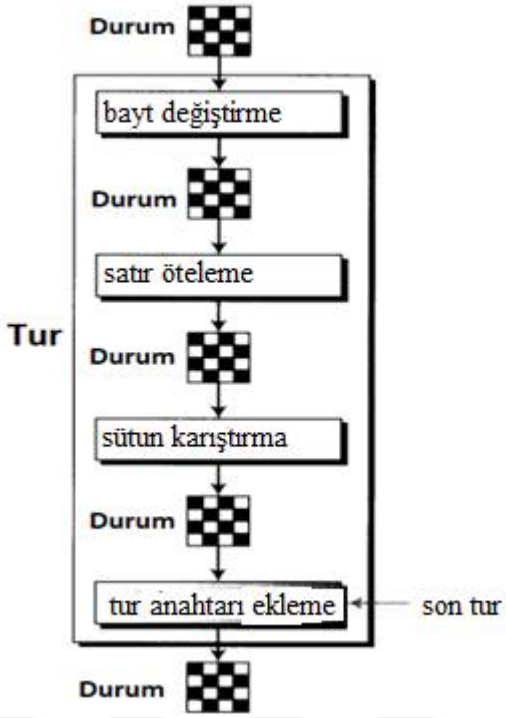
N(tur)	Anahtar Büyüklüğü
10	128
12	192
14	256

Şekil 2.3. AES Şifreleme Algoritmasının Genel Tasarımı

AES algoritmasında her döngü dört katmandan oluşur. İlk olarak 128 bit uzunluğunda olan veri 4×4 lük byte matrisine dönüştürülür. Bu matrise durum matrisi denilir ve her bir satırı kelime olarak adlandırılır. Daha sonra her döngüde sırasıyla:

- Byte Değiştirme (Subbytes)
- Satır Kaydırma (ShiftRows)
- Sütun Karıştırma (MixColumns)
- Döngü Anahtarı Ekleme (AddRoundKey)

adımları izlenir. Anahtar planlama evresinden gelen o döngü için belirlenen anahtar ile XOR' lama işlemleri gerçeklenerek şifrelenmiş veri elde edilir ve tekrar byte değiştirme adımına dönülür. Ve döngü sayısı anahtar uzunluğuna göre değişir. Son döngüde sütun karıştırma işlemi yapılmaz. Döngü anahtarı ile toplama işlemi yapılır ve şifreli bloklar elde edilir. Şifrelenmiş veriyi çözerken de bu işlemlerin tersi uygulanır (Forouzan , 2008). AES şifreleme algoritması ile ilgili detaylı bilgiye (Forouzan , 2008) kaynağından ulaşılabilir.



Şekil 2.4. AES şifreleme algoritmasında bir turdaki işlemler

BÖLÜM 3

STEGANOGRAFİ

Steganografi iletmek istediğimiz bilginin üçüncü kişilerin eline geçmemesi için bir ortama gizlenmesidir. Latince'de 'steganos' 'gizli' ve 'graphein' 'yazı' kelimelerinin bir araya gelmesi ile oluşmuş olup gizlenmiş yazı anlamına gelmektedir (Petitcolas, Anderson, & Kuhn, 1999).

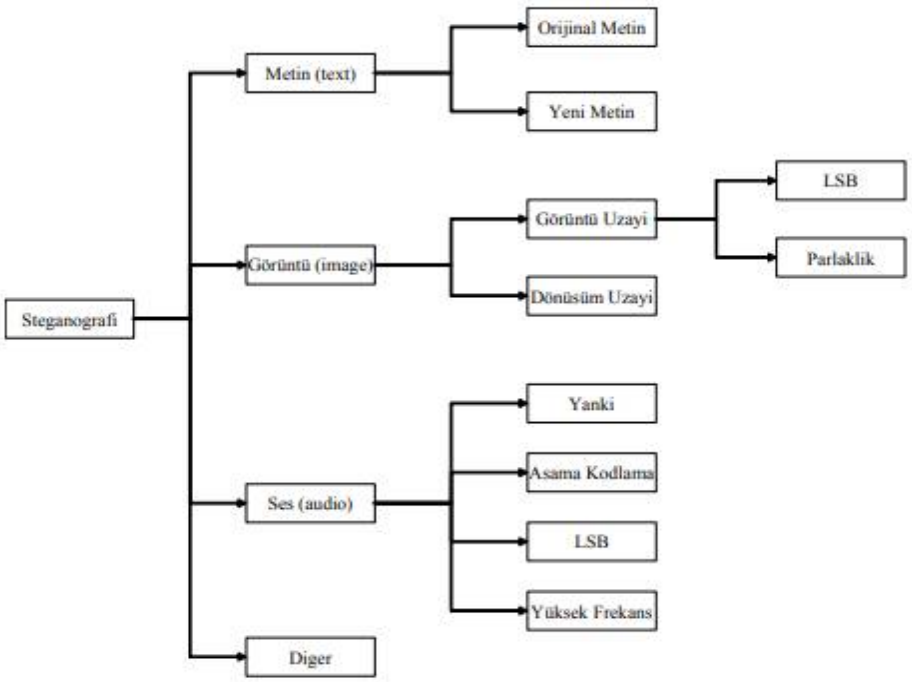
Stegonografide gizlemek istenen veriyi sayısal resim, metin, ses ya da video dosyasına saklamak mümkündür. Gizlenen veri metin, ses, video ya da dijital resim olabilir. Stegonografide bilgi gizlenecek ortama örtü verisi (cover-data) gizli veriyi bulunduran haline stego nesnesi adı verilir (Memon & Wong, 1998) (Wang & Wang, 2004).

Steganografi şifrelemeden farklı olarak verinin içeriğini karmaşık hale getirmek değil içeriği bir ortama saklamaktır.

Steganografide bir tekniğin diğerleri ile üç temel şekilde kıyaslanması gerekmektedir. Bunlar güvenlik, kapasite ve anlaşılmazlıktır. Güvenlik, gizli mesajın varlığının tespit edilememesi; kapasite, daha büyük boyutlu mesajların gizlenebilmesi ve anlaşılmazlık ise daha az bitte değişiklik yapılarak mesajın gizlenmesidir. Kullanılan yöntemin başarılı olması demek örtü nesnesindeki gizli bilginin olup olmadığının anlaşılamamasıdır. Ancak istatiksel yöntemler ile bu fark ortaya çıkabilmektedir. Burada en çok kullanılan yöntemler MSE (Ortalama Karesel Hata) ,PSNR (Tepe sinyal Gürültü Oranı), SSIM, Korelasyon katsayısı ve Histogram analizleridir.

3.1. Steganografik Yöntemler

Steganografik yöntemler gizlenecek olan veri ve örtü nesnesine göre resim, ses ve metin olmak üzere üç grupta incelenmektedir. Yaygın olarak kullanılan steganografik yöntemler Şekil 3.1' de gösterilmiştir.



Şekil 3.1. Sayısal Steganografi yöntemlerinin sınıflandırılması

3.1.1. Metin Steganografi

Örtü nesnesinin metin olduğu steganografi yöntemidir. Metin steganografide saklanabilecek veri miktarı azdır. Metin steganografi şu şekilde sınıflandırılabilir (Popa, 1998) ;

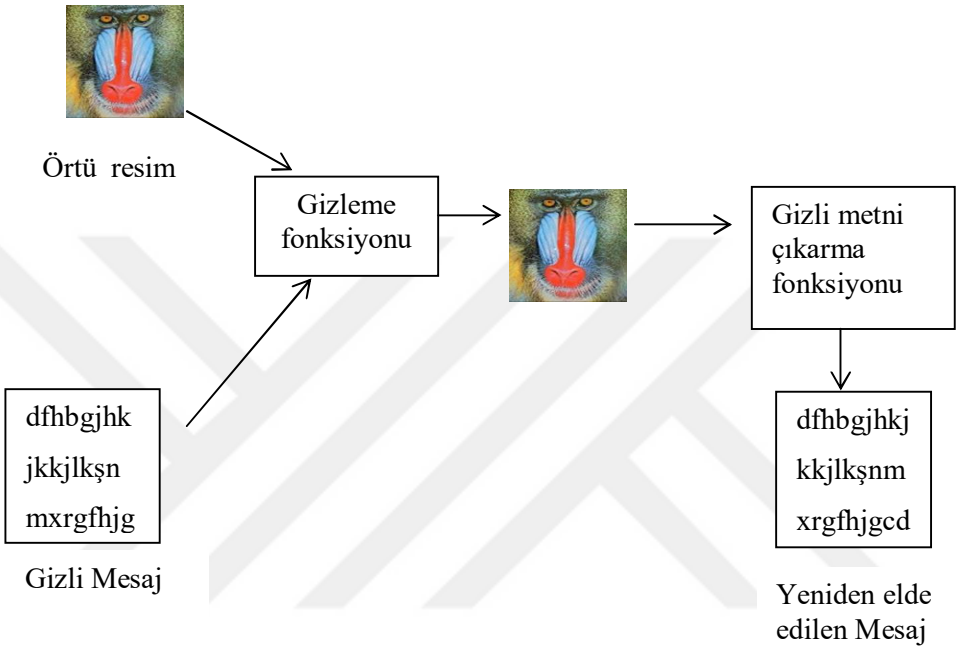
- Açık alan yöntemleri
- Yazımsal yöntemler
- Anlamsal yöntemler

3.1.2. Ses Steganografi

Ses steganografi en önemsiz bite gömme, eşlik kodlama, faz kodlama, yaygın spektrum ve yankı saklamadan meydana gelen bir yöntemdir (Baker , Lin , Shahi , & Jayaram, 2011).

3.1.3. Görüntü Steganografi

Steganografide en çok kullanılan yöntem görüntü içine bilgi gizlemedir. Görüntü dosyaları için bilgi gizleme şeması Şekil 3.2' de detaylı olarak gösterilmiştir. Gizleme fonksiyonu, verinin saklanacağı taşıyıcı ortam ve gizlenecek veri olmak üzere iki parametreye sahiptir (Westfeld & Pfitzmann, 2000). Görüntü dosyalarının içerisine bir metin gizlenebileceği gibi başka bir resim de gizlenebilir.



Şekil 3.2. Görüntüler için bilgi gizleme şeması

Görüntü steganografide verinin resim içerisine saklanmasında çeşitli yöntemler kullanılır. Şekil 3.2' de verilen gizleme fonksiyonunda

- En önemsiz bite ekleme
- Maskeleme ve filtreleme
- Algoritmalar ve dönüşümler (Sellars, 1999) kullanılabilir.

3.1.3.1. En Önemsiz Bite Ekleme Yöntemi (LSB)

En önemsiz bite ekleme yöntemi yaygın olarak kullanılan ve uygulaması basit bir yöntemdir (Johnson & Katzenbeisser, 2000). Gömülecek ikili metin örtü verisinde yani bilgi gizlemek istediğimiz görüntüdeki her bir pikselin en önemsiz bitine belirli bir algoritmaya göre değil sıralı olarak gömülür. Daha sonra gömülen

veriyi ortaya çıkarma sırasında metnin kaç karakterden oluştuğu bilinmeyeceği için sonuna işaret karakteri eklenir.

LSB Algoritmasının adımları şu şekildedir:

1.Adım: Örtü resmi(cover image) ve saklanacak metni al.

2.Adım: Saklanacak metni ikili olarak dönüştür.

3.Adım: Metnin bitleri bitene kadar 4 ve 5 adımlarını uygula.

4.Adım: Örtü resmin piksellerini ikilik sistemde yaz.

5.Adım: Veri gömülecek resmin piksellerindeki en önemsiz biti ile saklanacak verinin sıradaki biti ile değiştir.

6.Adım: Stego bilgiyi yaz. İşlemi sonlandır.

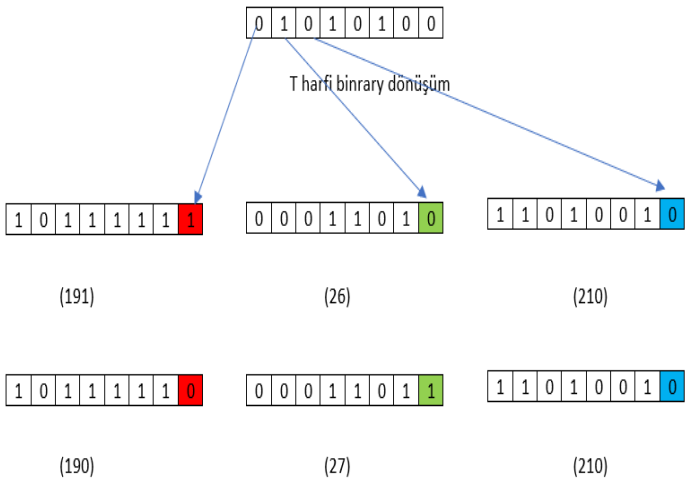
Bu yöntemde resmin boyutuna bağlı olarak belirli miktarda veri gizlenebilmektedir. 256×256 piksel boyutunda bir resme her pikselin kırmızı, yeşil ve mavi renk değerleri için 3×256×256 uzunlukta bir bit dizisi gizlenebilir. Bu bit dizisi tüm renk kanalına gizlendiği gibi seçilen bir renk kanalına da gizlenebilir (Öztürk, Şahin Mesut, & Mesut, 2011).

Örnek 3.1. LSB yöntemin uygulanması:

Gizlenecek mesaj: TRAKYA ÜNİVERSİTESİ

İkili Dönüşüm: 01010100 01010010 01000001 01001011 01011001 01000001 00100000 00010000 01001110 00010001 01010110 01000101 01010010 01010011 00010001 01010100 01000101 01010011 00010001

Renkli resim içerisindeki ilk RGB piksel değerleri Şekil 3.3' de verildiği gibi olsun:



Şekil 3.3. LSB Yönteminin Uygulanması

Bu teknikten başka her baytın sadece son bitinde değiştirme yapmak yerine son 2 veya daha fazla bitinde değişim yapılabilir. Bu yöntemde örtülü-nesnedeki (cover-object) gizli bilginin kapasitesini arttırmakla birlikte örtülü nesnedeki bozulma da daha fazla olmaktadır.

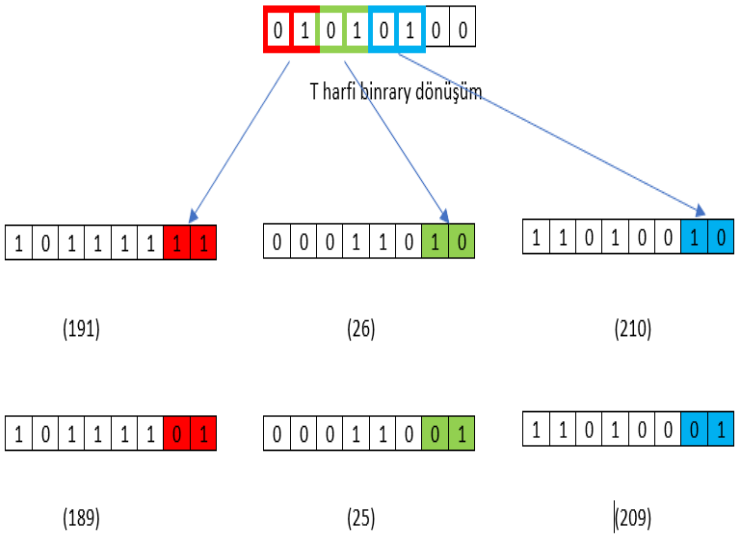
3.1.3.2. En Önemsiz 2 Bite Ekleme Yöntemi (2LSB)

2 LSB yöntemi, LSB yöntemine göre 2 kat veri gizleme kapasitesine sahiptir. Ancak LSB' ye göre biraz daha fazla bozulma gerçekleşir. Öncelikli olarak resmin piksel değerleri tek tek alınır ve gizlenecek olan veri 2 bitlik bloklar halinde RGB değerlerinin son 2 bitine gömülür. Bu döngü gelen bit dizisin sonuna kadar devam eder. Bu algoritmanın uygulanışı Şekil 3.4' de detaylı olarak gösterilmiştir.

2 LSB yöntemi maskeleme ve filtreleme gibi pek çok algoritma ile pek çok yönteme göre oluşabilecek tespitlere karşı daha dayanıklıdır (Sivaram, Devi, & Steffi, 2012).

2LSB Algoritması adımları:

1.Adım: Örtü resmi(cover image) ve saklanacak metni al.
2.Adım: Saklanacak metni ikili olarak dönüştür.
3.Adım: Metninin bitleri bitene kadar 4 ve 5 adımlarını uygula.
4.Adım: Örtü resmin piksellerini ikilik sistemde yaz.
5.Adım: Veri gömülecek resmin piksellerindeki en önemsiz
2 biti ile saklanacak verinin sıradaki 2 biti ile değiştir.
6.Adım: Stego bilgiyi yaz. İşlemi sonlandır.



Şekil 3.4. 2LSB Yönteminin Uygulanması

BÖLÜM 4

SIR PAYLAŞIM ŞEMALARI

Teknolojinin gelişmesi ile birlikte sayısal bilginin hızlı, hatasız ve güvenli bir şekilde iletilmesi oldukça önemlidir. Özellikle askeri, siyasi, bankacılık ve ticari alanlarda güvenli iletim daha da gereklidir. Bunun gibi pek çok alanda bilgi güvenliğini sağlamak için birçok metotlar kullanılmaktadır. Bu güvenlik metotlarının başında şifreleme, veri gizleme ve sır paylaşım şemaları gelmektedir.

Sır paylaşım şemasındaki amaç sır bilginin tek bir yerde ya da tek bir kişide muhafaza etmek yerine sorumluluğu birçok yetkili ile paylaşarak güvenliğini sağlamaktır. Dolayısıyla bu şema birçok alanda kullanıldığı gibi şifrelemede anahtar yönetiminde de kullanılan önemli bir yapıdır (Pang & Wang, 2005). Şifrelemede kullanılan anahtarın ya da gizli bilginin saklanmasında güvenlik açıklarının olması veya yöntemin kullanışsız olması nedenleri gibi problemlere çözüm olarak ilk defa 1979' da Shamir ve Blakley tarafından sır paylaşım şemaları önerilmiştir (Blakley, 1979; Shamir, 1979).

Bu şemalarda gizli bilginin tek bir kişide olması değil birçok kişiye dağıtılması esas alınır. (k,n) eşik şeması da denilen bu yöntemde gizlilik n kişi ya da n pay arasında dağıtılır ve herhangi k kişinin ya da payın bir araya gelmesi ile gizli bilgi yeniden elde edilir. k' dan az kişinin bir araya gelmesi ile gizlilik elde edilemez (Blakley, 1979; Shamir, 1979).

4.1. Genel Sır Paylaşımı Tanımı

Tanım 4.1. Bir sır paylaşım şemasında D dağıtıcı ve $P_1,...,P_n$ yetkili kişiler olmak üzere aşağıdaki temel yapı ile gerçekleştirilir.

- **Dağıtım Şeması:** D dağıtıcı S sır bilgiyi $1 \le i \le n$ olmak üzere her P_i yetkililerine s_i pay bilgisi dağıtılır.
- **Yeniden elde etme:** S sır bilgisi, s_i yetkililerinin paylarını birleştirilmesi ile yeniden elde edilir. Burada $i \in A$ ve $A \subseteq \{P_1,...,P_n\}$ olmak üzere her yetkilendirilmiş katılımcıların kümesi ile sır bilgi elde edilir.

Sır paylaşım şemalarının güvenlik gereksinimleri şu şekildedir:

- Her yetkili katılımcılar paylarını birleştirerek S sır bilgisini elde edebilirler.
- Her yetkilendirilmemiş katılımcılar paylarını birleştirdiğinde *S* sırrı hakkında hiçbir bilgiyi elde edemezler.

Bu güvenlik gereksinimlerini doğrulayan Sır Paylaşım Şeması mükemmel olarak adlandırılır (Schoenmaker, 2011).

4.2. Shamir' in Polinomsal Tabanlı Sır Paylaşım Şeması

Shamir tarafından 1979' da önerilen ilk sır paylaşım şeması Shamir' in eşik şeması veya lagrenge interpolasyon şeması olarak bilinmektedir.

Bir (k, n) sır paylaşımında p bir asal sayı ve Z_p sonlu bir cisim, k eşik değer ve $a_0 \in Z_p$ sır bilgisi (0, p-1) aralığında olmak üzere $a_1,...,a_{k-1} \in Z_p$ rastgele elemanları seçilip $k-1$ dereceli polinomu kurulur. Ve aşağıdaki polinom ile n kişi arasında dağıtılır.

$$f(x) = (a_{k-1}x^{k-1} + \cdots + a_1x + a_0) \in Z_p[x] \qquad (4.1)$$

- **Dağıtım Kısmı:**

Gizli bilgi farklı x değerleri ile aşağıdaki denklem kullanılarak dağıtma işlemi yapılır.

$$h(x) \equiv (a_{k-1}x^{k-1} + \cdots + a_1x + a_0) mod\ p \qquad (4.2)$$

$y_i = h(x_i) \bmod p$ eşitsizliğine göre gizli bilgi içeren paylar (x_i, y_i) şeklinde n adet yetkili kullanıcılara dağıtılır.

- **Sır Bilginin Yeniden Elde Edilmesi:**

a_0 sırrını ve $k-1$ dereceli $h(x)$ polinomunu bulmak için k adet yetkilinin payları yeterlidir. $h(x)$ ve a_0 lagrange polinomundan yeniden elde edilir. İlk olarak $l_k(x)$ polinomu şu şekilde tanımlanır (Denning, 1982) (Trappe & Washington, 2006) (Zhu, Bao, Deng, & Kankanhalli, 2005).

$$I_t(x) = \prod_{\substack{i=1 \\ i \neq t}}^{k} \frac{x - x_i}{x_t - x_i} mod(p) \qquad (4.3)$$

Lagrange interpolasyon polinomu:

$$p(x) = \sum_{t=1}^{k} y_t l_t(x) \qquad (4.4)$$

Örnek 4.1.

Shamir' in (k,n)=(3,6) eşik şemasını kuralım. Burada 6 yetkili kişi var ve bunlardan herhangi 3 tanesi kendi pay bilgileri ile gizliliği belirleyebilir. Ancak 2 kişi ve daha az kişi gizli bilgiyi elde edemez.

Farz edelim ki a_0=5 sayısı gizliliğimiz olsun. Bu gizli bir kelime veya anahtar olabilir. p=17 asal bir sayı ve $a_1, a_2 \in Z_{17}$ katsayıları ile rastgele aşağıdaki polinom seçilsin.

$$h(x) = (5 + 7x + 9x^2) mod\ 17$$

Bu polinomu kullanarak 6 yetkiliye (x,h(x)) anahtar parçası dağıtılsın. (1,4);(2,4);(3,5);(4,7);(5,10);(6;15). Bu ayrık noktalardan herhangi 3 tanesi ile ilgili polinom ve sır bilgisi elde edilir: $(x_0, y_0) = (1,4)$; $(x_1, y_1) = (2,4)$; $(x_2, y_2) = (3,5)$. Bu 3 nokta ile ilgili fonksiyon ve a_0 sır bilgisi lagrange interpolasyonu ile şu şekilde bulunur.

$$h(x) = \left[4\frac{(x-2)(x-3)}{(1-2)(1-3)} + 4\frac{(x-1)(x-3)}{(2-1)(2-3)} + 5\frac{(x-1)(x-2)}{(3-1)(3-2)}\right] m\ od17$$

$$= [(2x-4)(x-3) - 4(x-1)(x-3) + 45(x-1)(x-2)] mod17$$

$$= [2x^2 - 6x - 4x + 12 - 4x^2 + 16x - 12 + 45x^2 - 135x + 90] mod17$$

$$= [43x^2 - 129x + 90] mod 17$$

$$= 9x^2 + 7x + 5$$

Bu polinom görüldüğü gibi orijinal h(x) polinomudur. Ayrıca sabit terim olan 5 sır bilgisidir (Arda, Buluş, Akgün, & Yerlikaya, 2008).

4.3. Çin Kalan Teoremi Tabanlı Sır Paylaşım Şemaları

Çin Kalan Teoremi tabanlı sır paylaşım şemaları Mignotte (Mignotte, 1983) ve Asmuth-Bloom (Asmuth & Bloom, 1983) tarafından önerilmiştir. Bu şemalarda çin kalan teoremi boyunca özel bir sırada pozitif tam sayı dizileri kullanılır.

Tanım 4.1. $a, b, m \in Z$; m> 0 tam sayıları verilsin. Eğer m\ (a-b) ise *a, b* ye *m* modülüne göre kongrüenttir denir ve $a \equiv b$(mod m) şeklinde gösterilir.

Teorem 4.1. (Çin Kalan Teoremi) m_1 m_1, m_2, …, m_r pozitif tam sayılar ve her $i \neq j$ için (m_i, m_j)= 1 olsun. $a_1, a_2, \dots, a_r$ tam sayıları verildiğinde

$$\boldsymbol{x} \equiv a_i (mod\ m_i), (i = 1, 2, \dots, r) \qquad (4.5)$$

kongrüanslarının ortak çözümleri vardır ve herhangi iki ortak çözüm mod$(m_1, m_2, \dots, m_r)$ birbirine kongrüdür (Erdoğan & Yılmaz, 2008).

4.3.1. Asmuth-Bloom Sır Paylaşım Şeması

Asmuth-Bloom sır paylaşım şemasında sır bilgiyi dağıtma ve yeniden elde etme işlemleri aşağıdaki gibi yapılmaktadır (Asmuth & Bloom, 1983).

- **Dağıtım Kısmı**: n kullanıcılı bir gurup arasında S sırrını paylaştırmak için dağıtıcı şu işlemleri yapar:

n pay sayısı ve k eşik değer olmak üzere $2 \leq k \leq n$ olmalı ve $S + m_0\alpha < m_1.m_2 \dots m_n$ koşulunu sağlayacak özel sıralı aralarında asal pozitif tam sayılar seçilmek zorundadır. Gizli veri S , Zm_0 kümesinin bir elemanı olarak seçilir. Bu koşullar için aşağıdaki ifade kullanılmaktadır.

$$\prod_{i=1}^{k} m_i > m_0 \prod_{i=1}^{k-1} m_{n-i+1} \qquad (4.6)$$

$M = \prod_{i=1}^{k} m_i$ olmak üzere $y = S + \alpha m_0$ değeri hesaplanır. Buradaki α, $0 \leq y < M$ koşulunu sağlayan rastgele üretilmiş pozitif bir tamsayıdır. y_i payları $1 \leq i \leq n$ olmak üzere aşağıdaki denklemden elde edilir.

$$y_i = y mod m_i \qquad (4.7)$$

- **Yeniden Elde Etme:** *k* adet pay ile sırrı yeniden elde etmek için Çin kalan teoremi kullanılarak *y* aşağıdaki denklem sistemi ile bulunur.

$$y \equiv y_i mod m_i$$

$m_1 . m_2 \ldots m_k$ ' ler aralarında asal olduğu için y değeri k adet denklik ifadesi için tek bir çözümdür. Bu denklik ifadesi Çin Kalan Teoremi ile hesaplanır. S sırrı ise $S \equiv y \, mod m_0$ ile bulunur.

Asmuth-Bloom sır paylaşım şemasında k' dan daha az pay birleşerek gizlilik hakkında hiçbir bilgi elde edemezler. Bundan dolayı bu şema mükemmele yakın bir şemadır. Ancak α' nın rastgeleliği ve özel sıralı pozitif asalların uygun seçilmesi sistemin güvenliğini arttırmaktadır (Kaya, Selçuk, & Tezcan, 2006) (Arda & Buluş, 2009).

Örnek 4.2. Asmuth-Bloom şemasının (k,n)=(3,4) sır paylaşımı için özel sıralı aralarında asal pozitif tam sayıları m_0, m_1, m_2, m_3, m_4 şeklinde sırasıyla 11,19,23,31,37 olsun. $11.37 < 19.23.31$ koşulu sağlanır. Bu durumda gizli veri $S < m_0$ şeklinde $8 < 11$ seçilebilir.

$8 + 11\alpha < 19.23.31$ koşuluna uygun $\alpha = 100$ seçilebilir.

$$1108 \, mod \, 19 \equiv 6$$
$$1108 \, mod \, 23 \equiv 4$$
$$1108 \, mod \, 31 \equiv 23$$
$$1108 \, mod \, 37 \equiv 35$$

k=3 adet pay değerleri ile aşağıdaki denklik sisteminin çin kalan teoremi ile çözümünden

$$y \, mod 19 \equiv 6$$
$$y \, mod 23 \equiv 4$$
$$y \, mod 31 \equiv 23$$

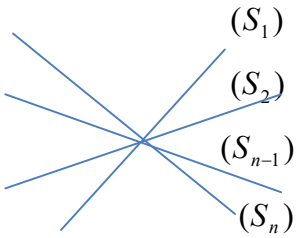
y=1108 olarak bulunur. $1108\, mod 11 \equiv 8$ olarak gizli veri elde edilir (Ulutaş, Ulutaş, & Nabiyev, 2011)

4.4. Blakley' in Geometrik Tabanlı Sır Paylaşım Şeması

Blakley' in sır paylaşma yöntemi gizli verinin n kişi arasında paylaştırılması için geometrik yöntemlerden faydalanmaktadır (Blakley, 1979). Katılımcıları birer düzlem ya da doğru ile temsil edersek bu hiper denklemlerin kesişimi noktayı verecektir. Saklanmak istenen veri kesişim noktasına gizlenecektir. Dağıtılan n tane denklem için herhangi k katılımcı bir araya geldiğinde gizli nokta bulunmuş olacaktır.

4.4.1. Blakley' in Sır Paylaşım Şeması

Blakley' in metodunda (k, n) eşik şeması için n katılımcının her birine GF(q) sonlu alan üzerinde k boyutlu uzayda bir hiper düzlem denklemi verilir. Hiper düzlemler $a_1x_1 + a_2x_2 + ... + a_kx_k = b$ şeklinde tanımlanmaktadır. $S = (x_1, x_2, x_3, ..., x_k)$ pay değerlerini tanımlamada kullanılır. Her bir hiper düzlem belli bir noktadan geçmektedir. Hiper düzlemlerin kesişme noktaları sır olarak tanımlanmaktadır. k katılımcının paylarını bir araya getirmesi ile sırrı yeniden elde etmek için denklem sisteminin çözülmesi gerekmektedir.



Şekil 4.1. Blakley sır paylaşım şeması

Örnek 4.3

Blakley' in yöntemine göre gizli veri üç boyutlu uzayda bir noktanın koordinatları ile (2,4,9) olarak verilsin. (3,4) şeması için GF(11)' de

$$2x_1 + 4x_2 + 9x_3 = b$$

olarak alalım. Her bir katılımcıya gönderilecek olan 4 farklı değerler kümesi (x_1, x_2, x_3, b) pay değerlerini oluşturur. Bu denkleme göre hesaplanan pay değerleri $S_1 = (1,1,1,4),\ S_2 = (1,3,2,10),\ S_3 = (4,2,1,3),\ S_4 = (3,2,6,2)$ dır.

Bu pay değerlerinden herhangi üçü bir araya gelerek düzlemlerinin kesişme noktası olan (2,4,9) yeniden elde edilir. S_1, S_2, S_3 katılımcıların pay değerleri ile denklem sistemini çözerek gizli veriyi elde edelim.

$$x_1 + x_2 + x_3 = 4$$
$$x_1 + 3x_2 + 2x_3 = 10$$
$$4x_1 + 2x_2 + x_3 = 3$$

Denklem sistemi mod11 e göre çözülerek $(x_1, x_2, x_3) = (2,4,9)$ kesişim noktası olan gizli veri elde edildi.

4.5. Gizli Görüntü Sır Paylaşımı

İnternetin ve teknolojinin gelişmesiyle birlikte dijital ortamda elektronik bilgiler, videolar, resimler, metinler ve sesler gibi çeşitli bilgiler paylaşılmaktadır. Paylaşılan bu veriler gizlilik gerektiren askeri veya tıbbi bir görüntü olabilmektedir. Bundan dolayı gizli görüntünün güvenliğini sağlamak için literatürde gizli görüntü sır paylaşım şeması gibi yöntemler önerilmiştir.

İlk olarak Görsel Sır Paylaşım Şeması (GSP) 1994' de Naor ve Shamir tarafından önerilmiştir (Naor & Shamir, 1995). Bu şemada paylaşılan sır gizli bir görüntüdür. Shamir' in *(k,n)* GSP şemasında olduğu gibi, gizli görüntüye görsel şifreleme teknikleri uygulanarak *n* adet anlamsız pay oluşturulur ve sırrı paylaşacak katılımcılara dağıtılır. Gizli görüntünün yeniden elde edilebilmesi için en az *k* adet katılımcının elindeki payları üst üste koyması gerekmektedir. Eğer katılımcı sayısı *k'* dan az ise gizli görüntü hakkında hiçbir bilgiye ulaşılamaz. Bu teknikte payların boyutunun gizli görüntünün iki katı olması sebebiyle, yeniden elde edilme aşamasında gizli görüntüyle orijinal görüntü kıyaslandığında kontrast kaybı oluşmaktadır (Cimato, De Prisco, & De Santis, 2007).

(k,n) GSP şemalarının başarımı için dört parametre kullanılmaktadır.

1- Güvenlik: k' dan az pay bir araya gelerek sır hakkında hiçbir bilgi elde edememelidir.
2- Doğruluk: En az k adet payın bir araya gelerek elde edilen sır bilgisinin orjinaliyle benzerliğidir.
3- Hesaplama Karmaşıklığı: Payları elde etmede kullanılan işlem sayısıdır.
4- Büyüme oranı: Gizli görüntüdeki bir pikselin paylarda kaç piksel ile ifade edildiğine bağlı olarak değişen orandır (Ulutaş, Ulutaş, & Nabiyev, 2011).

2002' de Thien ve Lin, Shamir'in 1979' da önermiş olduğu (k,n) eşik şemalarını kullanan Gizli Görüntü Paylaşım yöntemini önermişlerdir (Thien & Lin, 2002). Bu yöntemde *lxl* boyutunda görüntü Shamir' in polinomsal yöntemiyle *n* adet pay görüntülere bölünmekte ve bunlardan *k* tanesi bir araya gelerek gizli görüntüyü elde edebilmektedir. Üretilen pay görüntüleri gizli görüntünün *l/k'* sı kadardır.

Gizli Görüntü paylaşım şemalarında gri seviyeli görüntüler için piksel değerleri [0-255] aralığındadır (Cimato, De Prisco, & De Santis, 2007). Paylaşma şemasında kullanılan polinomun modül değeri bu aralıkta seçilen en büyük asal olan 251' dir. Asal sayı seçilmesindeki önem orijinal görüntüyü elde etmede tek bir çözüme ulaşılmasıdır. Ancak burada elde edilen piksel değerleri [0-250] arasındadır. Dolayısıyla [251-255] aralığındaki değerler yoktur ve 250' ye ötelenmişlerdir. Bu da görüntüde parlaklık kaybına sebep olmaktadır.

Renkli görüntüler için de renk aralığı RGB paletinde bulunun Red-Green-Blue renkleri için ayrı ayrı [0-255]' dir (Şahin Mesut & Arda, 2009).

4.5.1. Thien ve Lin Sır Paylaşım Şeması

Thien ve Lin, Shamir tarafından 1979' da geliştirilen sır paylaşım şemasını kullanarak (k,n) eşik-tabanlı bir görüntü paylaşımı önermiştir. lxl boyutlu gizli resimden n tane pay görüntü elde etmek için $(k-1)$ dereceli bir polinom kullanılmaktır. $0 \le i \le \left(\frac{l}{k}\right)$ ve $1 \le j \le l$ olmak üzere polinom şu şekilde tanımlanmaktadır. Polinomun modül değeri [0,255] aralığında seçilen en büyük asal olan p=251' dir.

$$S_x(i,j) = I(ik+1,j) + I(ik+2,j)x + \cdots + I(ik+k,j)x^{k-1}(mod\ p) \qquad (4.8)$$

Oluşturulan pay görüntülerin boyutu, gizli resmin $\frac{l}{k}$' sı büyüklüğündedir. Elde edilen n adet pay görüntüden en az k adet bir araya gelerek Lagrange İnterpolasyon yöntemi ile orijinal görüntü yeniden elde edilir.

Thien ve Lin ayrıca görüntünün paylara bölme işleminden önce permüte edilmesi yolu ile güvenliğinin daha da artırmasını önermektedir. Permütasyon işlemi herhangi bir anahtar değeri ile ya da çeşitli algoritmalarla yapılabilmektedir. Bu şekilde güvenlik ve saldırılara karşı dayanıklılık arttırılmış olmaktadır (Thien & Lin, 2002).

BÖLÜM 5

ANALİZ YÖNTEMLERİ

5.1. Uygulamada Kullanılan Analizler

Bir steganografik yöntemin başarısı, steganaliz yöntemlerine karşı güçlülüğüdür. Steganalizin en önemli amacı bir örtü nesnesinde bir verinin gizli olup olmadığını tespit etmektir. Eğer stego nesnede gizli veri olduğu tespit edilirse o zaman gizli verinin ne olduğunu elde etmek için çalışılır. Gizlenecek verinin tespit edilmemesi veya zor tespit edilmesi için stego nesne üzerinde yapılacak değişikliklerin az olması gereklidir. Bu nedenle, örtü resmin kullanıldığı steganografik yönteminin başarısı için hata kare ortalama (MSE) ve PSNR değerlerine bakılmaktadır. MSE hesaplamasında, örtü resim ve stego resim arasındaki fark değerlerinin karelerini tüm piksel sayılarına bölünmesidir. Eğer iki resim aynı ise MSE değeri 0' dır**.** SSIM analizi iki resim arasındaki benzerliği ölçmek için ortalama parlaklık ve renk değişimi bilgilerini kullanır ve (0-1) arasında değer alır. Histogram analizi görüntü üzerindeki piksellerin değerlerinin parlaklık seviyelerinin sayıca dağılımını grafiksel gösteren fonksiyondur. Resimler arasındaki ilişki için ise ayrıca korelasyon katsayısı hesaplanabilir.

5.2. PSNR (Tepe Sinyal Gürültü Oranı)

PSNR(Peak Sıgnal To Noise Ratio) stego nesnenin kalitesini ölçmede kullanılan yöntemlerden birisidir (Chen, Cheng, & Tsai, 2011). Bu test iki dizi arasındaki farkı ölçmek için ortalama karesel hatayı kullanır. M×N boyutlarında x kaynak resmi ve y veri gömülmüş resim olarak alınırsa ortalama karesel hata (MSE) (5.1) formülü ile hesaplanır.

$$MSE = \left(\frac{1}{M \times N}\right) \sum_{i=1}^{M} \sum_{j=1}^{N} \left(x_{ij} - y_{ij}\right)^2 \quad (5.1)$$

PSNR ve MSE değerleri ters orantılıdır. MSE nin düşük olması ve PSNR nin büyük olması iki resmin benzerliğinin fazla olduğu anlamına gelir. Düşük PSNR değeri ise görüntüler arasında oldukça büyük fark olduğu anlamına gelir. Bir görüntünün PSNR değerini hesaplayan formül (5.2)' de gösterilmektedir (Tanchenko, 2014).

$$PSNR = 10 \times log_{10} \left[\frac{255^2}{MSE}\right] \quad (dB) \quad (5.2)$$

5.3. SSIM (Yapısal Benzerlik Endeksi Ölçütü)

Bu test iki resim arasındaki benzerliği ölçmek için ortalama parlaklık ve renk değişimi bilgilerini kullanır. Bu yaklaşım 2004 yılında Wang ve arkadaşları tarafından ortaya konulmuştur (Wang, Bovik, Sheikh, & Simoncelli, 2004).

μ_x μ_y ,σ_x σ_y veσ_{xy} değişkenleri, x ve y görüntüleri için sırasıyla yerel ortalamalar, standart sapmalar ve kovaryans değerleri olarak hesaplanmaktadır. c_1, c_2, c_3 değerleri çok küçük değerler olarak alınıp $c_3 = \frac{c_2}{2}$ seçilirse denklem aşağıdaki gibi ifade edilir.

$$SSIM(x, y) \frac{(2\mu_x\mu_y + c_1)(2\sigma_x\sigma_y + c_2)}{(\mu_x^2 + \mu_y^2 + c_1)(\sigma_x^2 + \sigma_y^2 + c_2)} \quad (5.3)$$

SSIM değeri (0-1) arasında değer alır. Karşılaştırılacak iki resmin SSIM değeri 0 ise iki resmin benzemediği anlamına gelmektedir. 1 e yakın olması benzerliğin yüksek olduğunu gösterir.

5.4. Korelasyon Katsayısı (Correlation Coefficient)

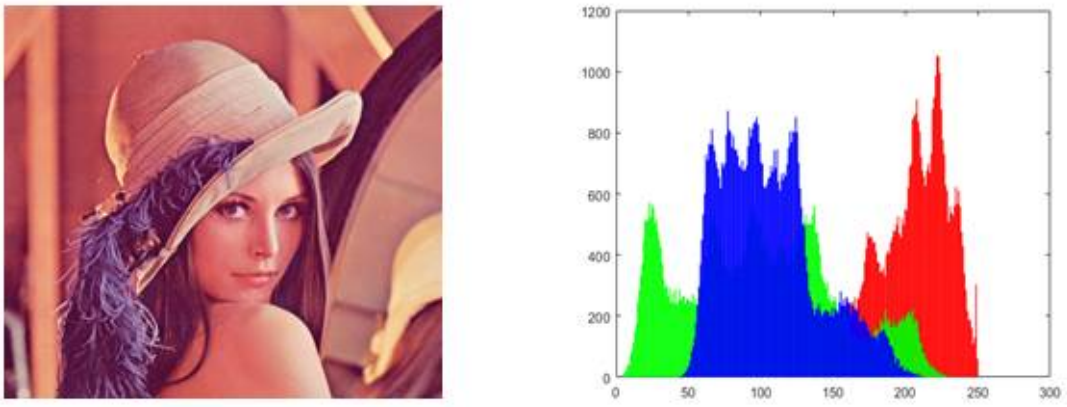
Korelasyon iki değişken arasında ilişki olup olmadığını hesaplamada kullanılan istatiksel metotlardan birisidir. x ve y resimleri arasındaki ilişki için korelasyon katsayısı aşağıdaki formül ile hesaplanır:

$$r = \frac{\sum(x_i - \overline{x})(y_i - \overline{y})}{\sqrt{(\sum(x_i - \overline{x})^2 \sum(y_i - \overline{y})^2}} \qquad (5.4)$$

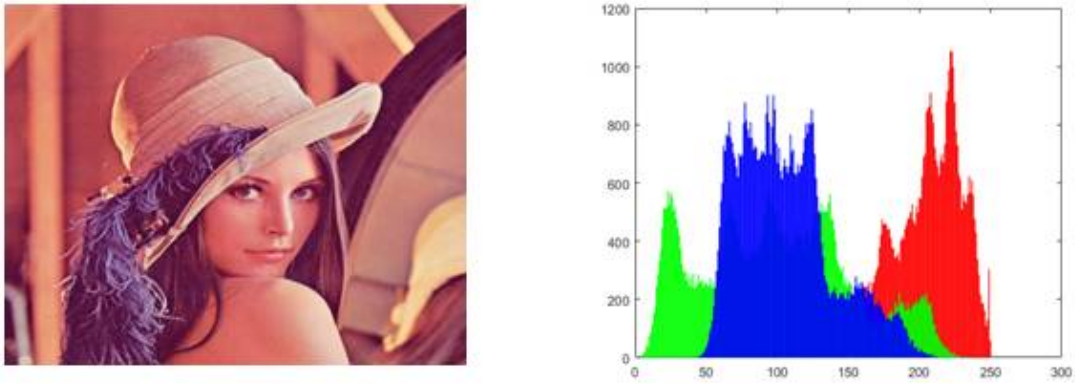
Korelasyon katsayısı +1 -1 arasında değerler alır. $r = -1$ ise aralarındaki ilişkinin mükemmel negatif, $r = +1$ ise aralarında mükemmel pozitif bir ilişki vardır. r=1 ise mükemmel ilişki, $0{,}5 \leq |r| < 1$ aralığında ise kuvvetli ilişki, $0 < |r| < 0{,}5$ ise zayıf ilişki vardır. r= 0 ise ilişki yoktur (Taşdemir, 2010).

5.5. Histogram Testi

Histogram bir veri dizisindeki her bir elemanın sıklığını gösteren ölçüttür. Görüntü işlemede olduğu gibi sayısal resim güvenliği içinde kullanılan bir yöntemdir. Sayısal resmin histogramını elde etmek için başlangıç olarak her bir elemanı sıfır olan resmin bit sayısı kadar bir dizi tanımlanır. Sayısal resmin her pikseli taranır dizinin piksel değerine karşılık düşen elemanın değeri bir arttırılır. Histogramda herhangi bir renk değerine sahip kaç pikselin bulunduğu yer aldığı için bu piksel değerlerindeki bir değişiklik histogram farkıyla rahatlıkla anlaşılabilir (Demirci, 2016).



Şekil 5.1. 256x256 boyutlu Lena.bmp Histogramı



Şekil 5.2. 2LSB ile Mavi kanala gizlenmiş veri olan Lena bmp. Histogramı

BÖLÜM 6

UYGULAMANIN GERÇEKLEŞTİRİLMESİ

6.1. Kriptografik Anahtarın veya Gizli Verinin Güvenliğinde Steganografi ile Thien-Lin' in Görüntü Sır Paylaşımı Uygulaması ve Analizleri

6.1.1. LSB Yöntemi İle Görüntünün Mavi Kanalına Bilgi Gizleme Ve Thien-Lin Görüntü Sır Paylaşımı Uygulaması

Geliştirilen uygulamada renkli görüntüye LSB yöntemiyle şifreleme anahtarı gizlenerek Thien ve Lin tarafından önerilen (k,n)= (2,4) eşik şemasıyla gizli görüntü paylaşımı gerçekleştirilmiştir. Uygulama Visual Studio 2015 ile C#(Sharp) programlama dilinde ve analizleri Matlab 2017b' de yapılmıştır. Elde edilen görüntüler MSE, PSNR, SSIM, Histogram analizleri ve Korelasyon Sabitleri açısından değerlendirilmiştir. Öncelikle renkli görüntünün gizliliğini arttırmak için resmin piksel (kırmızı, yeşil, mavi) değerleri bir anahtar ile permüte edilmiştir. Permütasyon için seçilen anahtar değeri ile gizli görüntünün piksel değerleri toplanmış ya da çarpılmıştır. Çarpma permütasyonu ile gizli görüntü daha karmaşık hale gelmiştir. Daha sonra permütasyon uygulanan görüntünün güvenliğini sağlamak için Shamir' in polinomsal tabanlı Thein-Lin görüntü sır paylaşım şeması ile n adet karmaşık pay görüntülere bölünmüştür. Daha sonra bu görüntülerden k tanesi ile permütasyonlu görüntü yeniden elde edilmiştir. Sonra permütasyonlu görüntüye ters permütasyon uygulayarak stego görüntüye ulaşılmıştır. En son stego kod çözme ile gizli veri görüntüden çıkarılmıştır.

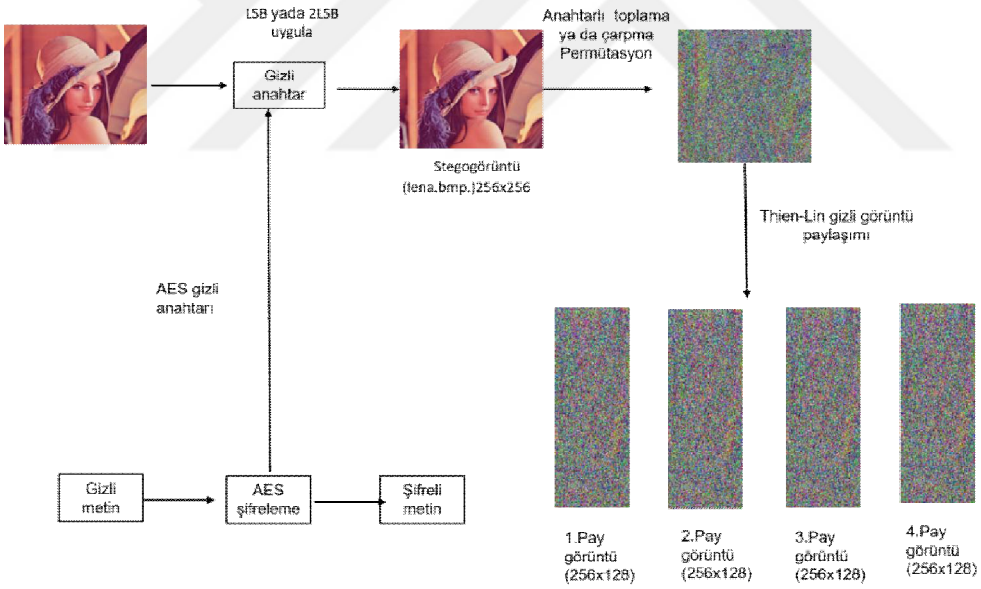
Gerçekleştirilen uygulamada 256x256 büyüklüğünde RGB renk kanalında bitmap türünde Lena resmi seçilmiştir. Bir şifreleme gizli anahtar değeri olarak (1234567890) alınarak LSB yöntemi ile resmin mavi kanalına gömülmüştür. Daha sonra Şekil 6.2' de gösterildiği gibi (100,200,300) anahtar değerine göre çarpma

işlemi ile resim permüte edilmiştir. Daha sonra (2,4) Thien-Lin görüntü sır paylaşım şeması ile 4 adet pay görüntülere bölünmüştür. Elde edilen pay görüntülerinin her birinin boyutu 128x256' dır. Dolayısıyla en az 2 pay görüntü ile gizli görüntü yeniden elde edilmiştir. Yeniden elde edilen permütasyonlu görüntüye ters permütasyon yapılarak gizli anahtar gömülü görüntüye ulaşılmıştır. Daha sonra gizli anahtar, uygulanan steganografik yönteme göre görüntü içinden çıkarılmıştır.

Yine benzer şekilde rastgele girilen başka bir gizli anahtarın gizlenmesi için LSB yöntemi ve Thien-Lin SPŞ uygulaması yapılmıştır. Yukarıda detaylandırıldığı gibi yeniden elde edilen bu gizli anahtar ile 128 bitlik bir AES şifreleme ve şifre çözme uygulaması gerçekleştirilmiştir (Arda, Demirbilek, & Kavak, 2017).

6.1.1.1. Veriyi gizleme ve Pay görüntüleri Dağıtım Kısmı

Bu bölümde stegolu görüntünün Thien-Lin GSP şemasına göre paylara bölünmesi Şekil 6.1' de ve adımları algoritma1 ile verilmiştir.



Şekil 6.1. Gizli Görüntü Paylaşımı, Steganografik Metot ve şifreleme (AES ya da herhangi bir şifreleme algoritması) İşlemleri

Şekil 6.1 için algoritma 1 aşağıdaki gibidir.

Algoritma1. Thien-Lin Stego Gizli Görüntü Dağıtım Şeması

Girdi: I gizli görüntü ve gizli anahtar ya da gizli bilgi

Çıktı: n adet pay görüntü I_1, I_2, .., I_n

Adım1: Gizli anahtarı (gizli bilgiyi) ikiliye dönüştür.

Adım2: I görüntünün (RGB) tüm piksellerini ikiliye çevir.

Adım3: LSB yada 2LSB ile mavi renk kanalına gizli anahtarı göm.

Adım4: Bir anahtar değeri ile stego-görüntüye çarpma veya toplama permütasyonu yap.

Adım5: $S_x(i,j) = I(ik+1,j) + I(ik+2,j)x + ... + I(ik+k,j)x^{k-1} \pmod{p}$ (p=251)

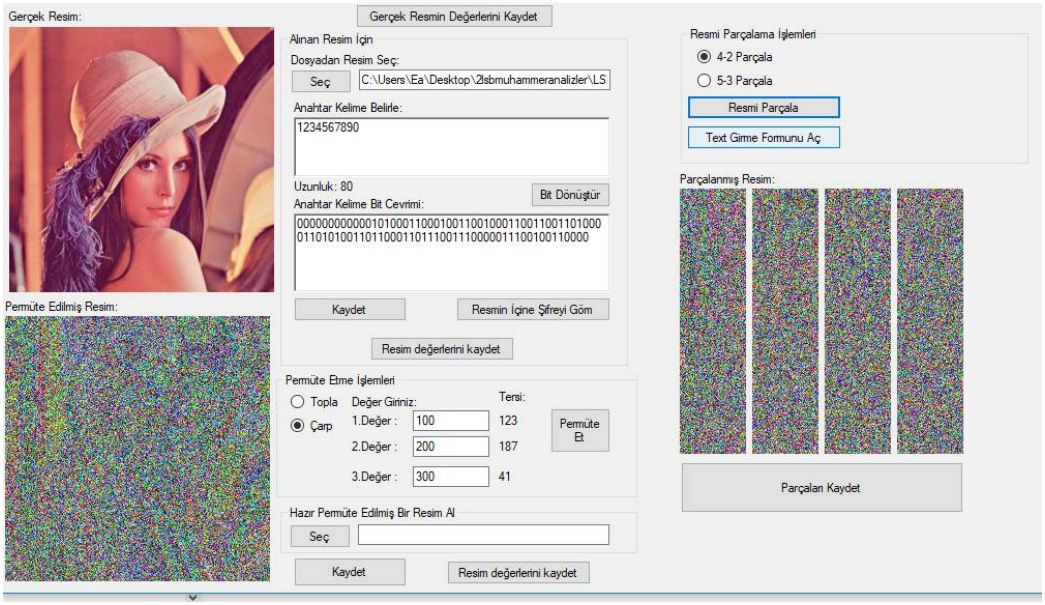
(k-1) dereceli polinomu $S_x(i,j)$ için permütasyonlu resmi kullan.

Her pay görüntünün piksel değerlerini i = 1,2,…, n olmak üzere S(i) hesapla ve

$I_1, I_2, \ldots, I_n$ pay görüntü olarak oluştur.

Adım6: $I_1, I_2, \ldots, I_n$ pay görüntüleri katılımcılara dağıt.

Yürütülen uygulamanın ekran görüntüsü aşağıdaki Şekil 6.2' de gösterilmiştir.



Şekil 6.2. Bir gizli anahtarın LSB ya da 2LSB ile Lena bmp. gizlenmesi ve (2,4) Thien-Lin Şeması ile pay görüntülere bölünmesi

Şekil 6.2' de yürütülen adımlar ve her aşamada elde edilen değerler hesaplanmıştır. Öncelikle 256 x 256 boyutunda Lena bmp. RGB renk kanalında bir deneme görüntüsü Şekil 6.3' deki gibi alınmıştır. Tüm aşamalardaki piksel değerleri yapılan yazılım sonucunda elde edilmiştir. Ancak Çizelge 6.1' de sadece 3x1 boyutunda orijinal Lena bmp., LSB ile sadece mavi kanala bilgi gömülü resim ve

çarpma permütasyonlu renk değerleri verilmiştir. Seçilen görüntüye gizli anahtarın gömülmesi ve permütasyon işleminden sonra (2,4) Thien-Lin sır paylaşım şeması ile 4 pay görüntüye bölünmüştür. Ayrıca görüntünün yeniden elde edilmesi için en az 2 pay görüntü kullanılmıştır. Pay görüntülerin piksel değerlerinin elde edilmesi aşağıdaki detaylı olarak gösterilmiştir. Elde edilen değerleri çizelge 6.2' de özetlenmiştir.



Şekil 6.3. 256 x 256 Lena.bmp görseli

Çizelge 6.1. Orijinal, LSB-mavi kanala gömülü, permütasyonlu Lena bmp. Görselinin Piksel Renk Değerleri

Orijinal Lena bmp. Piksel Renk değerleri	R=225 G=138 B=128 [0,0] piksel	R=224 G=137 B=127 [1,0] piksel	R=227 G=139 B=125 [2,0] piksel
LSB-Mavi kanala gömme	R=225 G=138 B=128 [0,0] piksel	R=225 G=138 B=126 [1,0] piksel	R=227 G=139 B=124 [2,0] piksel
Permütasyonlu Lena bmp Piksel Renk değerleri	R=161 G=241 B=248 [0,0] piksel	R=161 G=241 B=150 [1,0] piksel	R=110 G=190 B=52 [2,0] piksel
Pay 3 ve Pay 4 ile yeniden elde edilen resmin piksel değerleri	R=225 G=138 B=128 [0,0] piksel	R=225 G=138 B=126 [1,0] piksel	R=227 G=139 B=124 [2,0] piksel

Çizelge 6.1' deki permütasyon işlemi için çarpma işlemi uygulanmış ve her renk kanalı için bu işlem mod 251' e göre yapılmıştır.

Görüntünün Paylara Bölünmesi:

$(2,4)$ eşik şemasına göre $k = 2$ ve $n = 4$ ' tür. Verilen sınır şartlarına göre $0 \leq i \leq 2$ ve $1 \leq j \leq 4$ ' tür. Aşağıdaki gibi k-1. dereceden polinom fonksiyonu kullanılarak pay görüntüler elde edilir.

$$S_x(i,j) = I(ik+1,j) + I(ik+2,j)x \ (mod\ 251) \qquad (4.9)$$

Paylaşım için oluşturulacak parçaların hangi pikselinin değeri hesaplanmak isteniyorsa i ve j değerleri ona göre konularak işlemler yapılmaktadır. Tüm işlemler permüte edilmiş görüntünün renk değerleri üzerinden yapılmaktadır.

Bu denklemde de x yerine 1, 2, 3 ve 4 konularak oluşturulacak 4 parçanın [0,0] pikselinin değeri hesaplanmış olur.

x=1 yani 1.pay görüntü için [0,0] piksel değerleri

kırmızı = (0.piksel.R + (1.piksel.R * x)) % sabitmod;

(161 + 161 * 1)mod251= 71

yeşil = (0.piksel.G + (1.piksel.G * x)) % sabitmod;

(241 + 241 *1)mod251= 231

mavi = (0.piksel.B + (1.piksel.B * x)) % sabitmod;

(248 + 150 * 1)mod251=147

1. Pay görüntünün [0,0] piksel değeri [71, 231, 147] olarak bulunur.

x=2 için 2.pay görüntünün [0,0] piksel değerleri

kırmızı = (0.piksel.R + (1.piksel.R * x)) % sabitmod;

(161 + 161 * 2)mod251= 232

yeşil = (0.piksel.G + (1.piksel.G * x)) % sabitmod;

(241 + 241 *2)mod251= 221

mavi = (0.piksel.B + (1.piksel.B * x)) % sabitmod;

(248 + 150 * 2)mod251=46

2. Pay görüntünün [0,0] piksel değeri [32, 221, 46] olarak elde edilir

x=3 için 3.pay görüntünün [0,0] piksel değerleri

kırmızı = (0.piksel.R + (1.piksel.R * x)) % sabitmod;

(161 + 161 * 3)mod251= 142

yeşil = (0.piksel.G + (1.piksel.G * x)) % sabitmod;

(241 + 241 *3)mod251= 211

mavi = (0.piksel.B + (1.piksel.B * x)) % sabitmod;

(248 150 * 3)mod251=196

3. Pay görüntünün [0,0] piksel değeri [142,211, 196] şeklinde elde edilir.

x=4 için 4.pay görüntünün [0,0] piksel değerleri

kırmızı = (0.piksel.R + (1.piksel.R * x)) % sabitmod;

(161 + 161 * 4)mod251= 52

yeşil = (0.piksel.G + (1.piksel.G * x)) % sabitmod;

(241 + 241 *4)mod251= 201

mavi = (0.piksel.B + (1.piksel.B * x)) % sabitmod;

(248 + 150 * 4)mod251=95

4. Pay görüntünün [0,0] piksel değeri [52, 201, 95] olarak elde edilir.

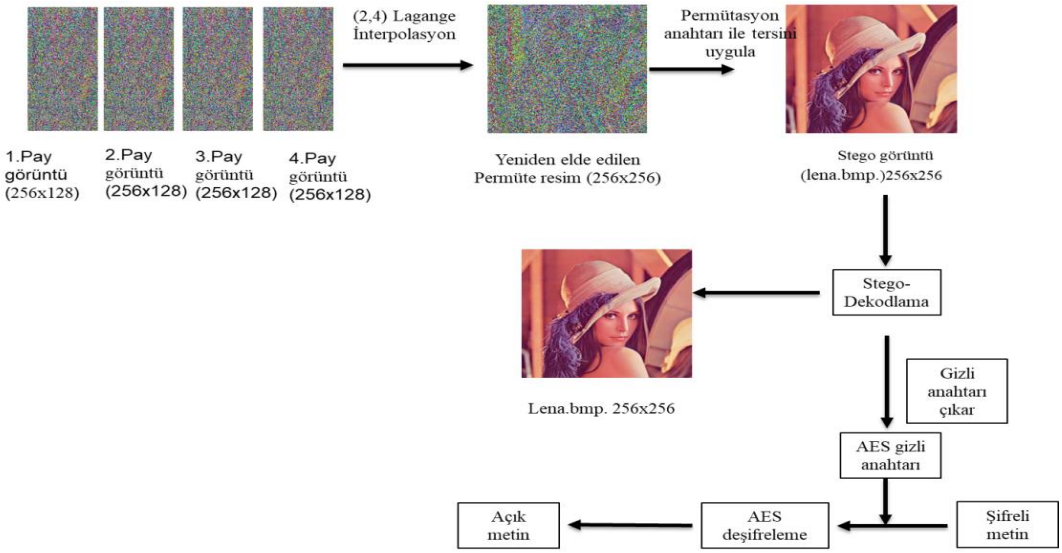
Elde edilen Pay görüntülerin [0,0] renk piksel değerleri Çizelge 6.2' de verilmiştir.

Çizelge 6.2. Pay görüntülerin [0,0]. renk piksel değerleri

1.Pay Görüntünün [0,0] Piksel Değerleri	R:71 G:231 B:147
2.Pay Görüntünün [0,0] Piksel Değerleri	R:32 G:221 B:46
3.Pay Görüntünün [0,0] Piksel Değerleri	R:142 G:211 B:196
4.Pay Görüntünün [0,0] Piksel Değerleri	R:52 G:201 B:95

6.1.1.2. Görüntünün Yeniden Elde Edilmesi Kısmı

Dağıtım kısmından sonra (k,n) Thien-Lin Şemasına göre rastgele k adet pay görüntü ile görüntünün kayıpsız yeniden elde edildiği ve bu görüntüden stego bilgisinin elde etme adımları algoritma 2' de verilmiştir ve ayrıca Şekil 6.4 ile gösterilmiştir.



Şekil 6.4. Gizli Görüntünün, gizli anahtarın yeniden elde edilmesi ve şifre çözme işlemleri

Algoritma 2: Gizli görüntünün ve gizli anahtarın(gizli bilginin) yeniden elde edilmesi

Girdi: Herhangi k adet pay görüntü: I_1, I_2,…, I_n

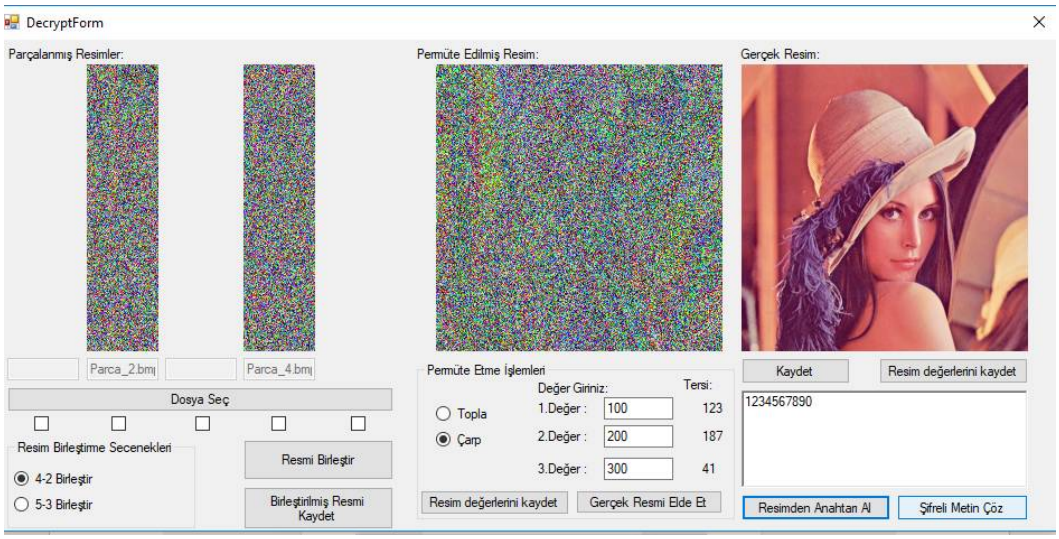
Çıktı: Gizli görüntü ve gizli anahtar(gizli bilgi)

Adım1**.** Permütasyonlu stego-gizli görüntüyü elde etmek için Lagrange interpolasyon ve I_1,…,I_k pay görüntülerini kullan.

Adım 2**.** Ters permütasyonla stego-görüntüyü elde et.

Adım 3. Stego sistem dekodlamasıyla gizli anahtarı (gizli bilgiyi) ve gizli görüntüyü elde et.

Algoritma 2' de verilen adımlar gerçeklendiğinde uygulamanın ekran görüntüsü Şekil 6.5' de verilmiştir.



Şekil 6.5. k=2 pay görüntüden gizli anahtarın ve gizli görüntünün elde edilmesi

Yukarıda algoritma 2' de verilen adımları [0,0] pikselini elde etmek için örnekleyelim. 3. ve 4. pay görüntüler ile önce permüte edilen görüntüyü ve sonra ters permütasyon işlemi ile stego görüntüyü elde edelim. 3. pay görüntünün [0,0]. piksel değerleri [142,211,196] olarak, 4. pay görüntünün [0,0]. piksel değerleri [52,201,95] olarak elde edilmişti. Denklem 4.4' deki lagrange interpolasyon formülü ile orijinal görüntünün permütasyon uygulanmış [0,0] ve [1,0] piksel değerleri elde edilir.

(x_3, y_3)=(3,142); (x_4, y_4)=(4,52)

$$S = \left[142\,\frac{(x-4)}{(3-4)} + 52\,\frac{(x-3)}{(4-3)}\right] \bmod 251$$

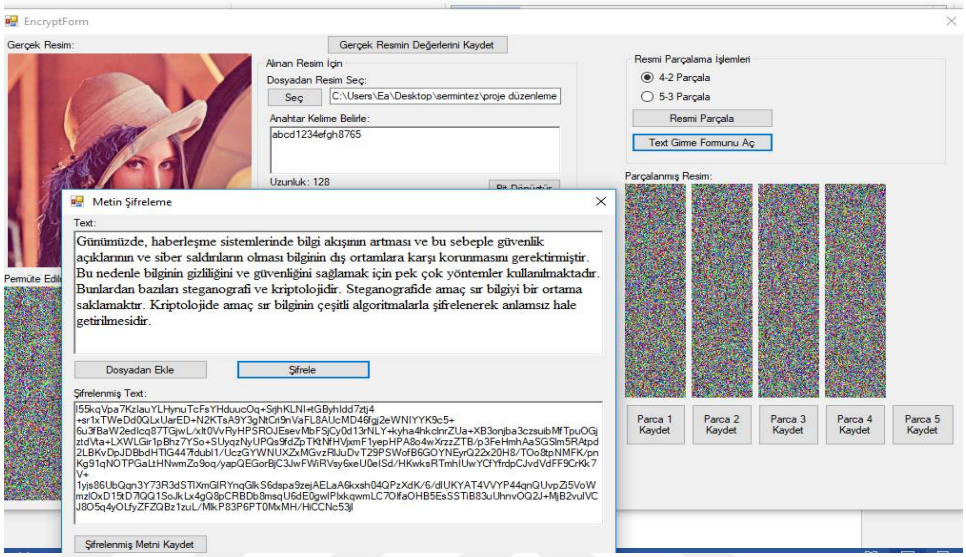
$$S = (-90x + 412) \bmod 251 = (161x + 161)$$

Burada elde edilen sabit sayı permüte edilmiş görüntünün [0,0]. pikselinin kırmızı renk değerini , x' li terimin katsayısı da permüte edilmiş görüntünün [1,0]. pikselinin kırmızı renk değerini vermektedir. Daha sonra bu değerlere ters permütasyon uygulayarak stegolu görüntü değerlerini elde ederiz.

Örneğin bu örnekte (100,200,300) anahtar değerlerine göre çarpma permütasyon uygulanmıştır. Çarpmaya göre tersleri olan (123,187,41) anahtar değerleri ile elde edilen değerler çarpılarak mod 251' e göre hesaplanır. Örneğin (161*123) mod251=225 olarak stegolu [0,0] kırmızı piksel değeri elde edilir. Aynı şekilde diğer renklerin piksel değerleri de elde edilir. Elde edilen değerler tablo 6.3' de verilmiştir.

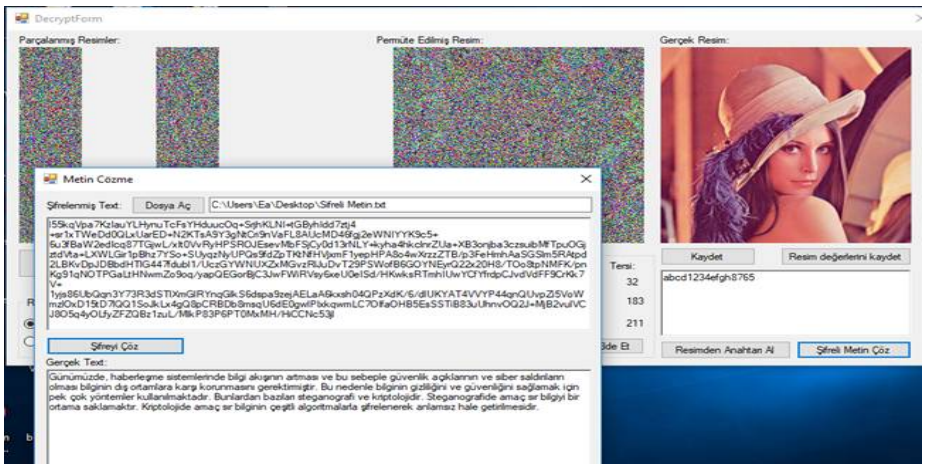
Ayrıca Şekil 6.6' de bir başka uygulama olarak, AES gizli anahtar değeri (abcd1234efgh8765) alınmış ve seçilen görüntünün içine LSB yöntemi ile RGB renk

kanalında mavi kanala gömülmüştür. Çarpma permütasyonu için (102,203,320) anahtar değeri seçilmiştir. Karıştırılan görüntü sonra Thien-Lin SPŞ ile 4 adet pay görüntülere bölünmüştür. (2,4) eşik şeması kullanıldığı için rastgele seçilen 2 pay ile görüntü yeniden elde edildi. Daha sonra gömülen gizli anahtar çıkarılarak şifre çözme işlemi gerçekleştirilmiştir.



Şekil 6.6. AES şifreleme

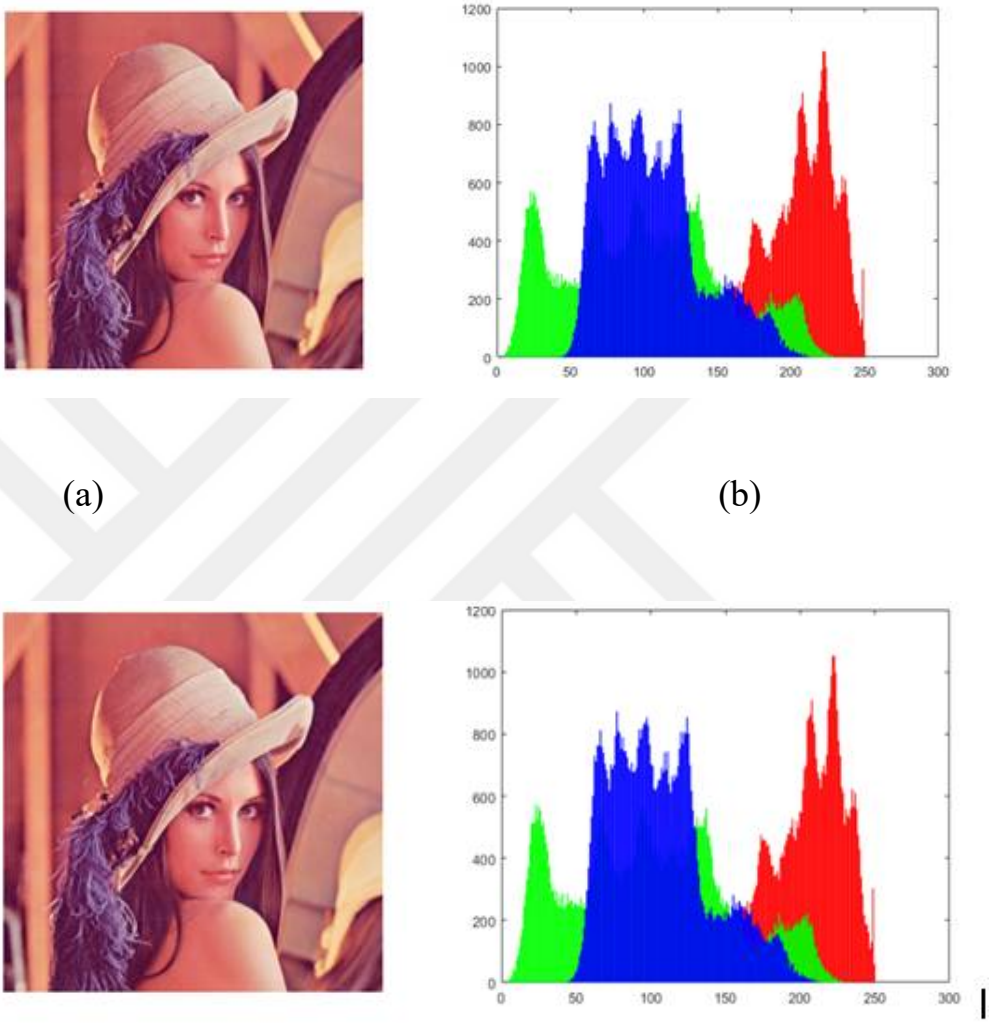
Şekil 6.7' da ise algoritma 2' de verilen işlemler sonucunda gerçekleştirilen uygulamanın ekran görüntüsü verilmiş. Uygulamada 128 bitlik AES şifreleme ve şifre çözme gerçekleştirilmiştir.



Şekil 6.7. AES Şifre Çözme

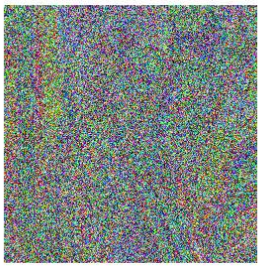
6.1.2. LSB yöntemi ve Thien-Lin Görüntü Sır Paylaşımı Uygulamasının Analizi

Aşağıdaki Şekil 6.8' de 256x256 bmp. Formatında Lena görseli (a) ve bunun histogramı (b), LSB ile gizli anahtar değeri (1234567890) olan gömülü resim (c) ve bunun histogramı (d) ile gösterilmiştir.



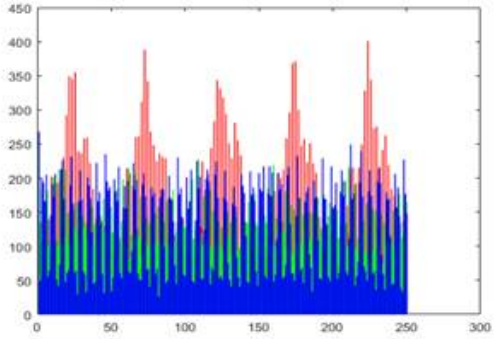
Şekil 6.8. Lena.bmp, (LSB) Stego-Lena bmp ve histogramları

(100,200,300) anahtarına göre permütasyonlu resim (f) ve elde edilen pay1, pay2, pay3 ve pay 4 görüntüleri ve histogramları sırasıyala (g, h, t, k) ile (2-4) payları ile yeniden elde edilen resim histogramı (m) aşağıda şekil 6.9' da verilmiştir.



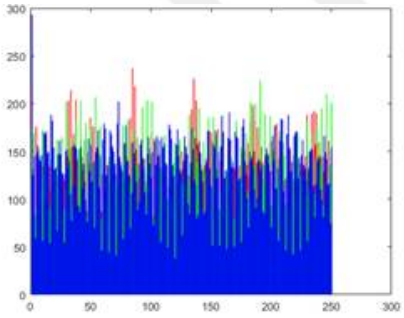
(f)




450
400
350
300
250
200
150
100
50
0
0
50
100
150
200
250
300

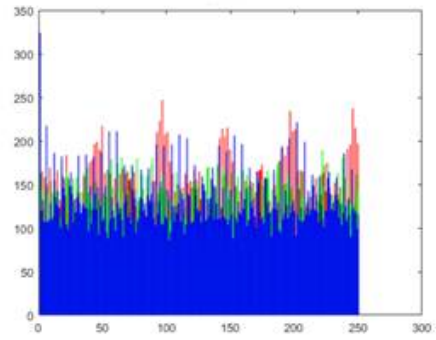
(g)



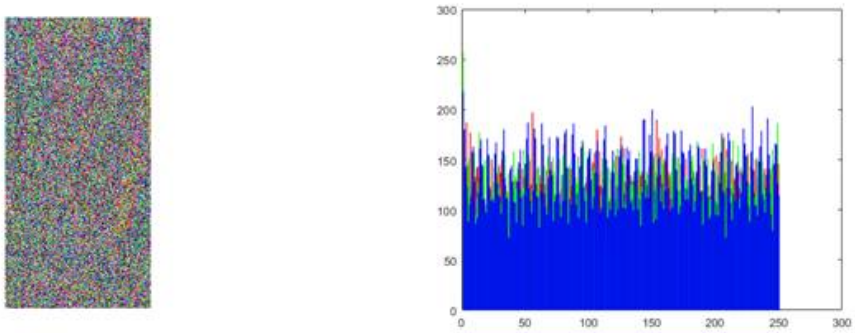

300
250
200
150
100
50
0
0
50
100
150
200
250
300

(h)

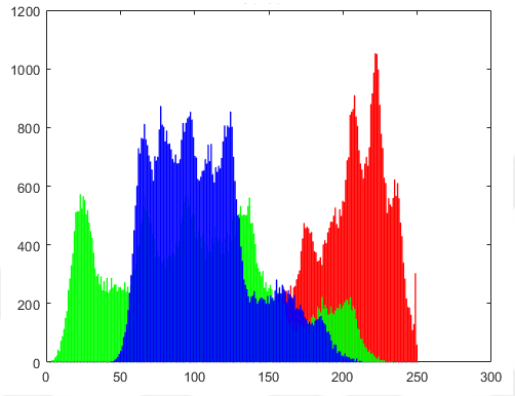



350
300
250
200
150
100
50
0
0
50
100
150
200
250
300

(t)



(k)



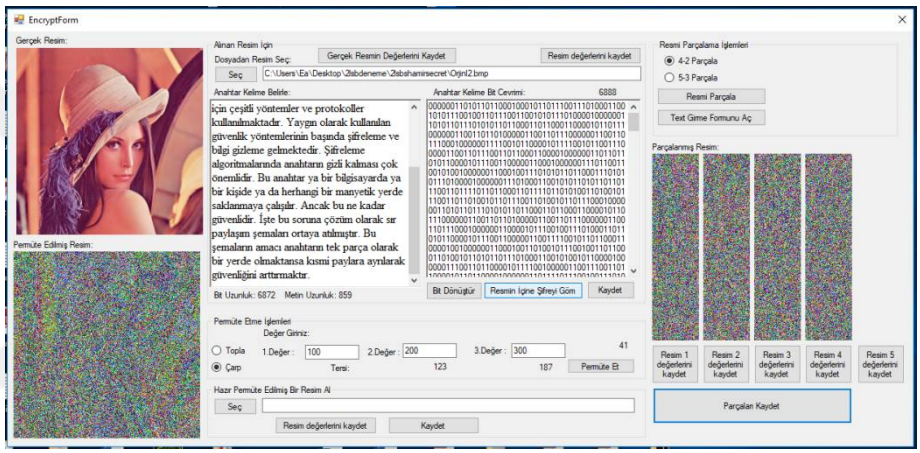
(m)

Şekil 6.9. Permüte edilen resim (f), pay1(g), pay2(h), pay3(t), pay4(k) payları, (1-2) payları ile yeniden elde edilen resim (m) histogram analizi

Yukarıda LSB bilgi gizleme yöntemiyle resmin mavi kanalına veri gömülmüştür. Ve Thien-Lin GSP şemasıyla veri gömülü resim 4 paya bölünmüştür. Şekil 6.8' de (b) ve (d) histogramlarına bakıldığında gözle görülür bir fark sezilmemektedir. Ve daha sonraki adımlarda stego-resme permütasyon işlemi yapılarak 4 paya bölünmüştür. Her pay görüntü tek başına değerlendirildiğinde herhangi bir renkte ya da bir bölgede çok belirgin bir fark görülmemektedir. Yani saldırgan herhangi bir pay görüntünün histogramına baksa bile dikkatini çekecek bir değişiklik bulamayacaktır. Güvenliği sağlayan bir başka durum da tek pay görüntüyle hiçbir bilgiye ulaşılamamasıdır. Uygulamada seçilen dağıtım polinomuna göre en az k=2 adet pay görüntüyle veri gömülü görüntüyü yeniden elde edebiliriz.

6.1.3. 2LSB ile görüntünün mavi kanalına bilgi gizleme ve Thien-Lin GSP Şeması Uygulaması

Yine bölüm 6.1.1' de detaylı olarak anlatıldığı gibi bu bölümde de 2LSB bilgi gizleme yöntemiyle yine seçilen görüntünün mavi kanalına algoritma1' de verildiği gibi 80 bitlik bir şifreleme anahtarı ya da 6872 bitlik bir gizli veri gizlenmiş ve Thien Lin şeması ile pay görüntülere bölünmüştür. Aşağıda şekil 6.10' de 6872 bitlik veri gizlenen uygulamanın ekran görüntüsü verilmiştir. Benzer şekilde 80 bitlik şifreleme anahtarı gömme işlemi de yapılmıştır. 80 bitlik veri gömme için gerçekleştirilen yazılım sonucunda her adımda elde edilen piksel değerler aşağıdaki Çizelge 6.3' de verilmiştir.



Şekil 6.10. 6872 bit veri gömülmüş görüntü için (2,4) Thien-Lin Şeması Uygulaması

Çizelge 6.3. Orijinal, 2LSB-mavi kanala 80 bit(gizli anahtar) gömme, ve permütasyonlu Lena bmp. Görselinin 1x3' lük Piksel Renk Değerleri

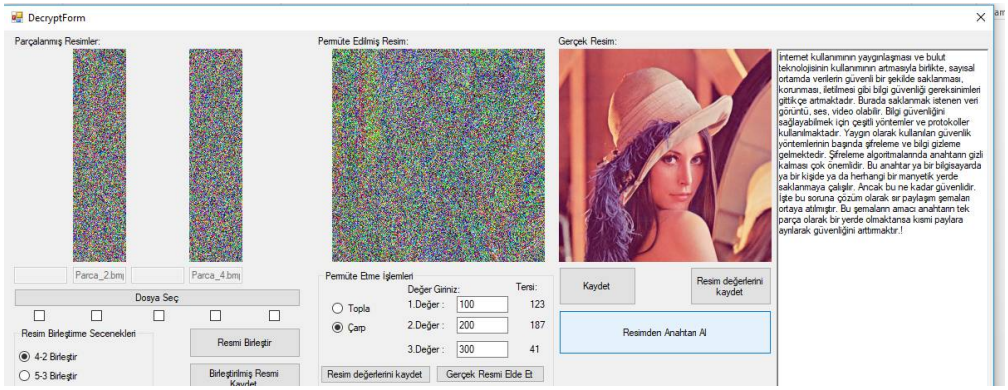
Orijinal Lena bmp. Piksel Renk değerleri	R=223 G=136 B=119 [0,6] piksel	R=219 G=133 B=115 [0,7] piksel	R=218 G=134 B=111 [0,8] piksel
2LSB-Mavi kanala gömme	R=223 G=136 B=118 [0,6] piksel	R=219 G=133 B=114 [0,7] piksel	R=218 G=134 B=108 [0,8] piksel
Permütasyonlu Lena bmp Piksel Renk değerleri	R=212 G=92 B=9 [0,6] piksel	R=63 G=245 B=64 [0,7] piksel	R=214 G=194 B=21 [0,8] piksel
(Pay1-Pay2) ile elde edilen resim piksel değerleri	R=223 G=136 B=118 [0,6] piksel	R=219 G=133 B=114 [0,7] piksel	R=218 G=134 B=108 [0,8] piksel
(Pay3-Pay4) ile elde edilen resim piksel değerleri	R=223 G=136 B=118 [0,6] piksel	R=219 G=133 B=114 [0,7] piksel	R=218 G=134 B=108 [0,8] piksel

Bulunan Pay görüntülerin [0,6],[0,7] ve [0,8] renk piksel değerleri Çizelge 6.4' de verilmiştir.

Çizelge 6.4. 1x3 boyutlu pay görüntülerin renk piksel değerleri

1.Pay Görüntünün Renk Piksel Değerleri	R:24 G:243 B:244 [0,6]piksel	R:124 G:145 B:226 [0,7]piksel	R:22 G:39 B:134 [0,8]piksel
2.Pay Görüntünün Renk Piksel Değerleri	R:187 G:139 B:216 [0,6]piksel	R:136 G:92 B:39 [0,7]piksel	R:99 G:33 B:247 [0,8]piksel
3.Pay Görüntünün Renk Piksel Değerleri	R:99 G:35 B:188 [0,6]piksel	R:148 G:39 B:103 [0,7]piksel	R:144 G:27 B:109 [0,8]piksel
4.Pay Görüntünün Renk Piksel Değerleri	R:11 G:182 B:160 [0,6]piksel	R:160 G:237 B:167 [0,7]piksel	R:205 G:21 B:222 [0,8]piksel

Aşağıda Şekil 6.11' de (k,n)=(2,4) eşik şemasıyla Lagrange interpolasyon yöntemiyle k=2 rastgele pay görüntü ile gizli görüntünün yeniden elde edildiği ve resme gömülü olan gizli bilginin çıkarılması uygulamasının ekran görüntüsü verilmiştir.



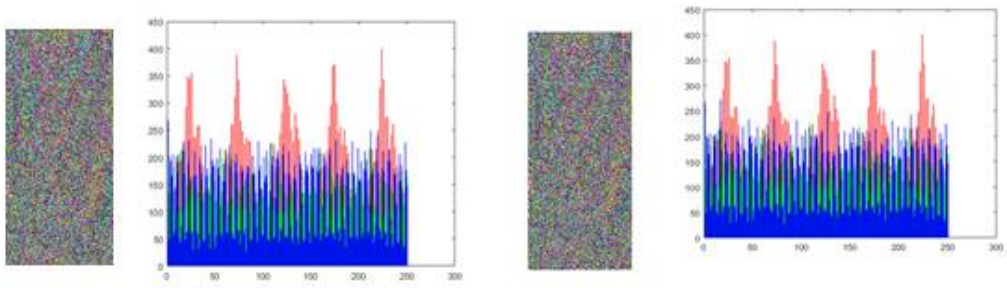
Şekil 6.11. k=2 pay görüntüyle görüntüyü yeniden elde etme ve gömülü gizli bilgiyi çıkarma uygulaması

6.1.4. 2LSB yöntemi ve Thien-Lin Görüntü Sır Paylaşımı Uygulamasının Analizi

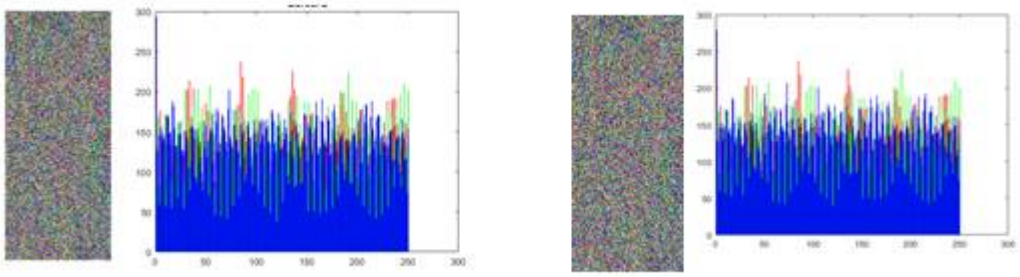
Lena 256x256 bmp. formatında görsele bir uygulamada 2LSB ile 80 bitlik (1234567890) bir gizli anahtar gömülmüş, bir başka uygulamada 6872 bitlik bir deneme metni gömülmüştür. Gömme işleminde RGB katmanında mavi kanal kullanılmış ve her renk kanalı için (100,200,300) anahtarı kullanılarak çarpma permütasyonu yapılmıştır. Daha sonra Thien-Lin GSP şeması uygulanmış. Elde edilen 256x128 piksellik pay görüntüler ve histogramları aşağıdaki şekillerde verilmiştir. Ayrıca PSNR, MSE, SSIM, korelasyon analizleri değerleri Çizelge 6.5' de verilmiştir.



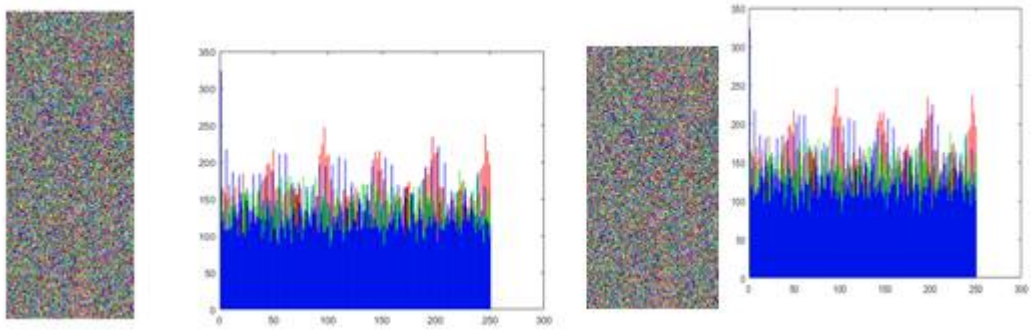
Şekil 6.12. Orijinal ve 2LSB yöntemiyle bilgi gizlenmiş görüntünün permütasyonlu görüntüsü



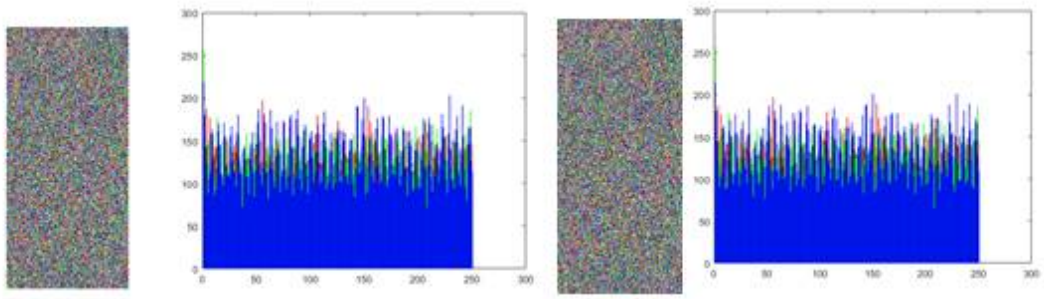
Şekil 6.13. Sırasıyla Pay 1 (80bit) ve (6872 bitlik) metin gömülüye ait histogramlar



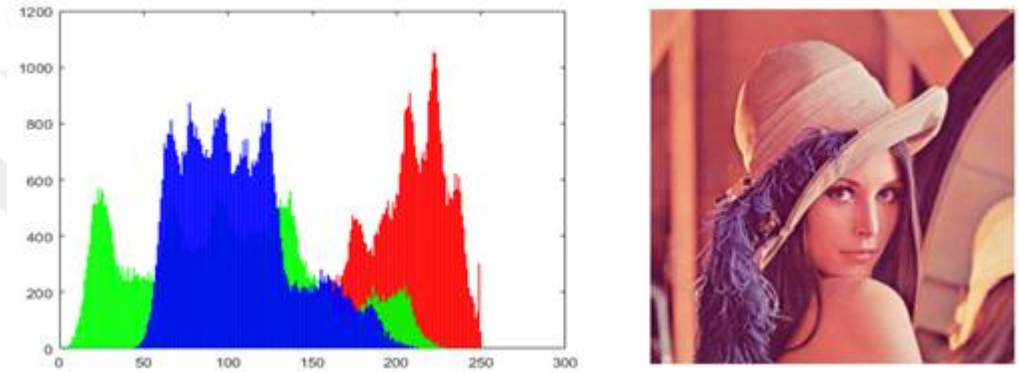
Şekil 6.14. Sırasıyla Pay 2 (80bit)ve (6872 bitlik) metin gömülüye ait histogramlar



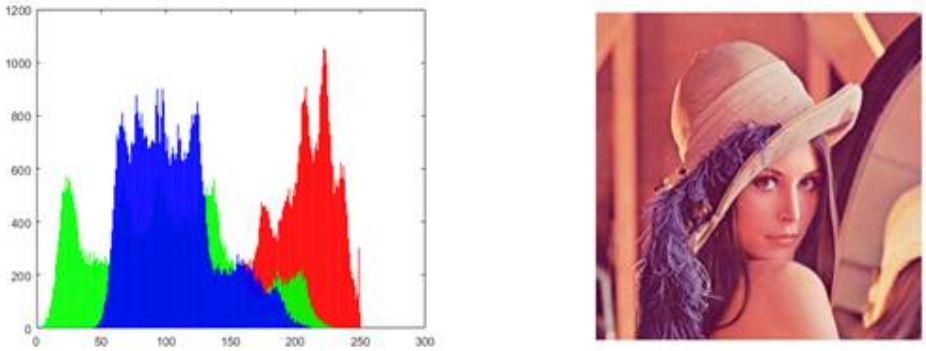
Şekil 6.15. Sırasıyla Pay 3 (80bitlik) ve (6872) bitlik metin gömülüye ait histogramlar



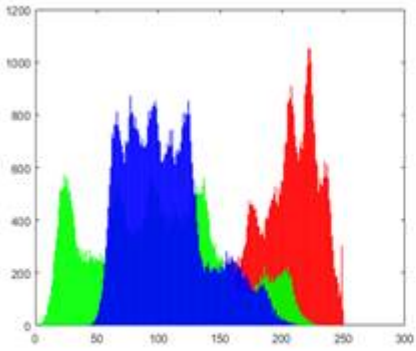
Şekil 6.16. Sırasıyla Pay 4 (80bitlik) ve (6872) bitlik metin gömülüye ait histogramlar



Şekil 6.17. Pay1 ve Pay2 ile elde edilen gizli anahtar (80 bit) gömülü resmin histogramı

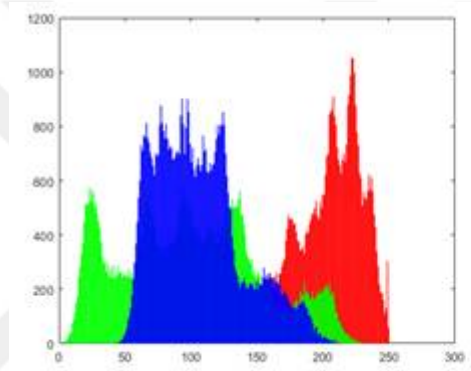


Şekil 6.18. Pay3 ve Pay4 ile elde edilen gizli bilgi gömülü(6872bit) resmin histogramı





Şekil 6.19. 2LSB ile Mavi kanala gizli anahtar (80bit) gömülü resmin histogramı





Şekil 6.20. 2LSB ile Mavi kanala 6872bit gömülü resme ait histogram

Çizelge 6.5. 2LSB yöntemi ile 80bit ve 6872bit gömülü Görüntüler ve Thien-Lin Şeması ile elde edilen görüntülerin PSNR, MSE, SSIM, Korelasyon testi sonuçları

Karşılaştırılan görüntüler	MSE	PSNR(db)	SSIM	Korelasyon
StegoGörüntü(6872bit)(2LSB)-Orij-Görüntü	2.127635	44.8518	0.999273	0.999722
StegoGörüntü(80bit)(2LSB)-Orij-Görüntü	0,000854	78,8137	1	1
StegoGörüntü(80bit)-Orij görüntü (yeşil)	0	Inf(sonsuz)	1	1
Stego Görüntü(80bit)- Orij görüntü (mavi kanal)	0,002563	74,0425	0,999970	0,999999
Pay1 ile Pay2(2LSB)(6872bit metin gömülü)	10521.9110	7.9099	0.001516	-0.006645
Pay2 ile Pay4(2LSB)(6872bit metin gömülü)	10530,2478	7,9064	0,001965	-0,008756
Pay1 ile Pay3(2LSB)(6872bit metin gömülü)	10399.8276	7.9605	0.013981	0.008131
Pay3 ile Pay4(2LSB)(6872bit metin gömülü)	10481.0556	7.9268	0.006455	-0.000831
Pay1 ile Pay2(2LSB)(80 bit anahtar gömülü)	10544,4782	7,9006	0,000411	-0,009039
Pay3 ile Pay4(2LSB)(80bit)	10480,9980	7,9268	0,006906	-0,000256
(Pay1+Pay2) ile (Pay3+Pay4) Yeniden elde edilen görüntülerin karşılaştırılması	0	Inf(sonsuz)	1	1
(Pay1-Pay2)-stego görüntü	0	Inf(sonsuz)	1	1

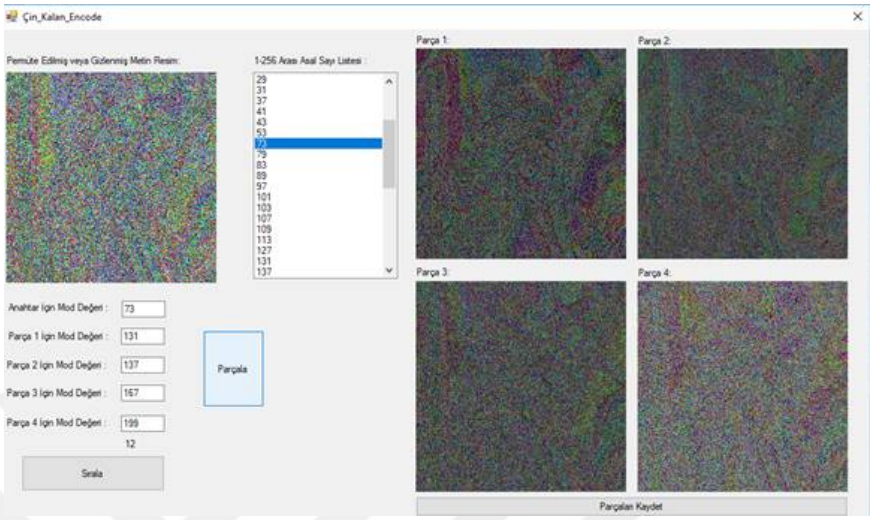
6.2. Kriptografik Anahtarın Veya Gizli Verinin Güvenliğinde Steganografi ile Çin kalan teorisi tabanlı Asmuth-Bloom Şeması ile Görüntü Sır Paylaşımı Uygulaması ve Analizleri

6.2.1. 2LSB ile veri gizlenmiş görüntünün Çin kalan teorisi tabanlı Asmuth-Bloom Şeması ile Görüntü Sır Paylaşım Uygulaması

Bu bölümde Asmuth Bloom'un Çin kalan teorisi tabanlı steganografik gizli görüntü paylaşım şeması ile sıralı farklı asallar kullanarak farklı uygulamalar gerçekleştirilmiş ve analizleri yapılıp değerlendirilmiştir. İlk olarak gizli anahtar veya gizli metin 2LSB yöntemiyle 256x256 boyutundaki Lena.bmp görseline gömülmüş daha sonra (3,4) Asmuth Bloom gizli görüntü paylaşım şeması ile pay görüntülere bölünmüştür. Elde edilen 2LSB uygulanmış görüntünün ve pay görüntülerin PSNR, MSE, SSIM ve Korelasyon ve histogram analizleri yapılmıştır.

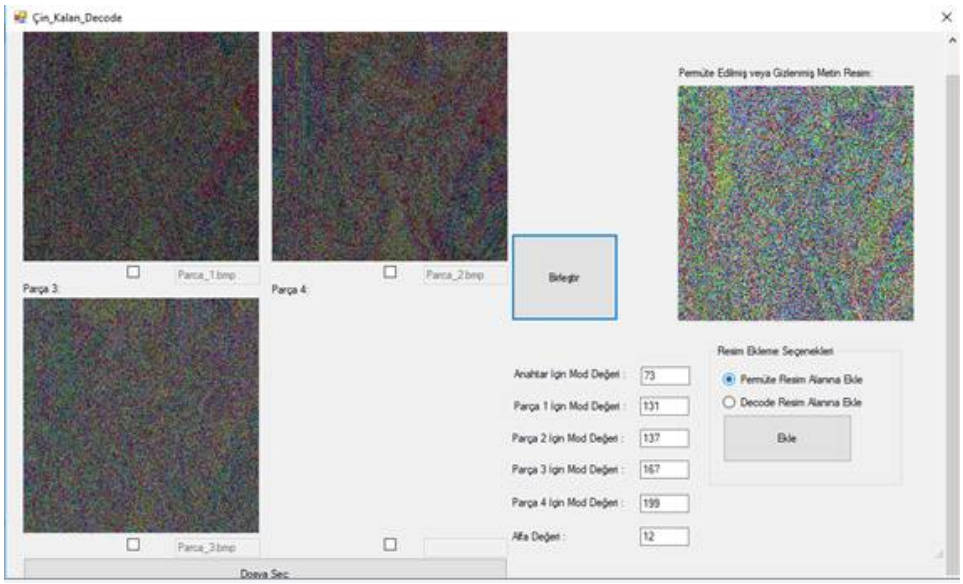
2LSB yöntemiyle 80 bitlik bir gizli anahtar seçilen Lena.bmp görseline gömülmüş. Ve daha sonra bu resme her (RGB) renk katmanı için (100,200,300) değerleri ile çarpma permütasyonu uygulanmış. Dağıtım için özel seçilen asallar

olarak (75,131,137,167,199) ve rastgele seçilen α=12 kullanılmıştır. Ve n=4 pay görüntüye bölünmüştür. Gerçekleştirilen uygulamanın ekran görüntüsü Şekil 6.21' de verilmiştir.



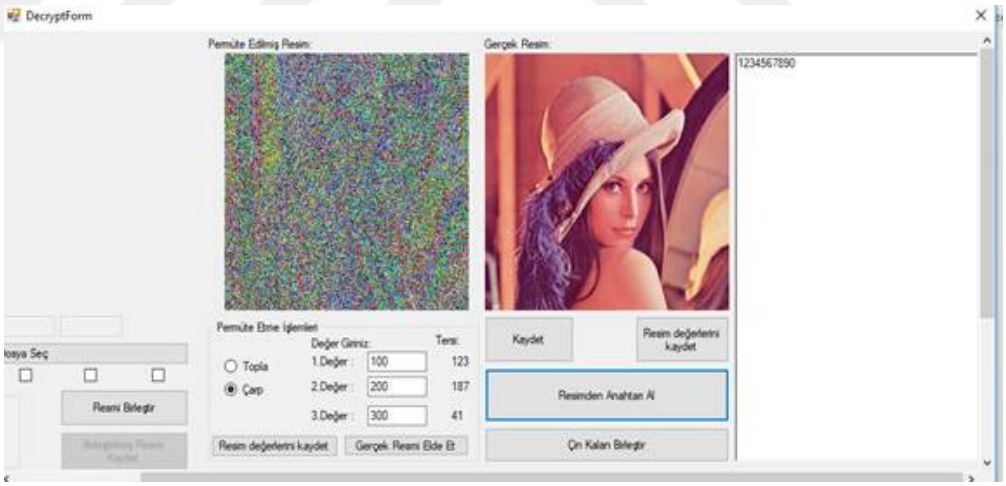
Şekil 6.21. 80 bit gizli veri gömülü stego-görüntüsüne seçilen asallarla Çin kalan Teorisi tabanlı Asmuth- Bloom GSP şeması ile n=4 Pay görüntüye bölünmesi

Dağıtım kısmından sonra en az k=3 adet rastgele seçilen pay görüntülerden, örneğin aşağıdaki şekil 6.22' de gösterildiği gibi (1-2-3) pay görüntüleriyle önce permütasyonlu görüntü daha sonra ters permütasyonla veri gömülü görüntü elde edilir.



Şekil 6.22. Çin Kalan Teoremini kullanarak (1-2-3) Pay görüntüleri ile permütasyonlu görüntünün elde edilmesi

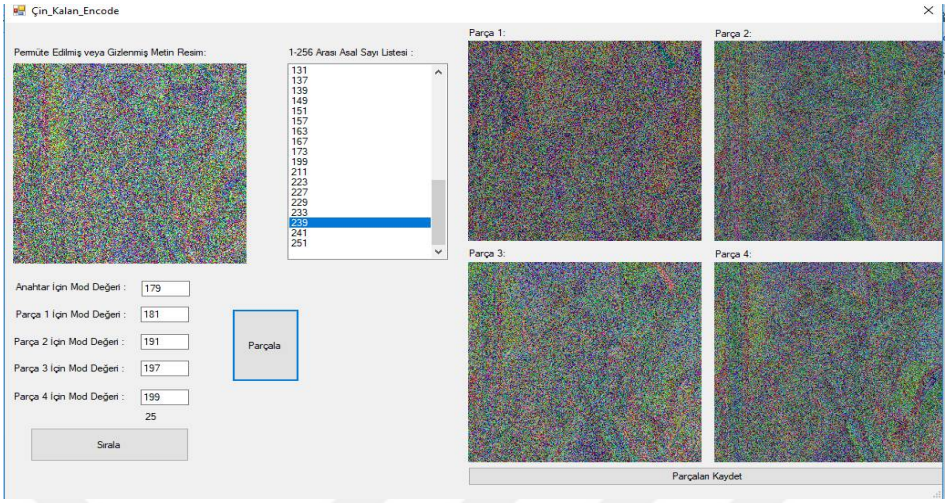
En son olarak aşağıdaki şekil 6.23' de gösterildiği gibi gömülü veriye ve stego görüntüye ulaşılır.



Şekil 6.23. Stegolu görüntü ve gizli verinin elde edilmesi

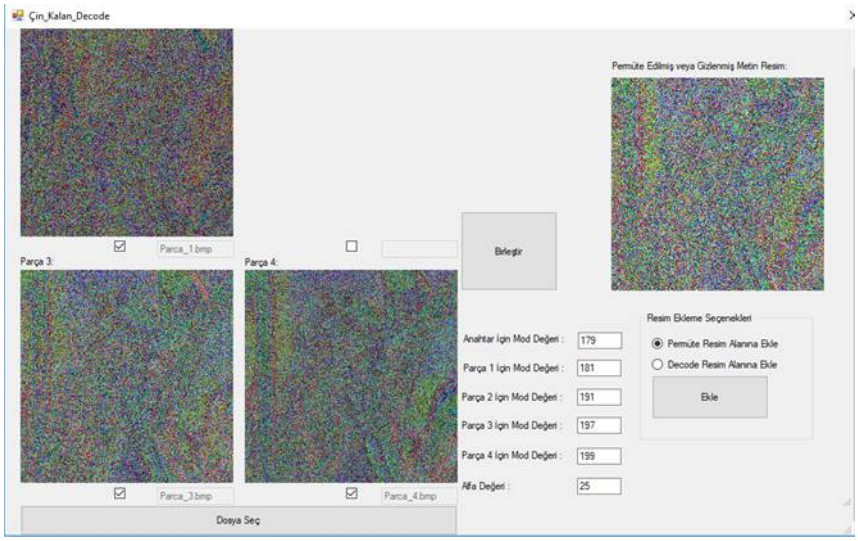
Yine benzer şekilde 2LSB yöntemiyle 6872 bitlik bir gizli metin seçilen Lena.bmp görseline gömülmüş. Ve daha sonra bu resme her (RGB) renk katmanı için (100, 200, 300) değerleri ile çarpma permütasyonu uygulanmış. Dağıtım için özel seçilen asallar olarak (179, 181, 191, 197, 199) ve rastgele seçilen α=25

kullanılmıştır. Ve n=4 pay görüntüye bölünmüştür. Gerçekleştirilen uygulamanın ekran görüntüsü Şekil 6.24' de verilmiştir.



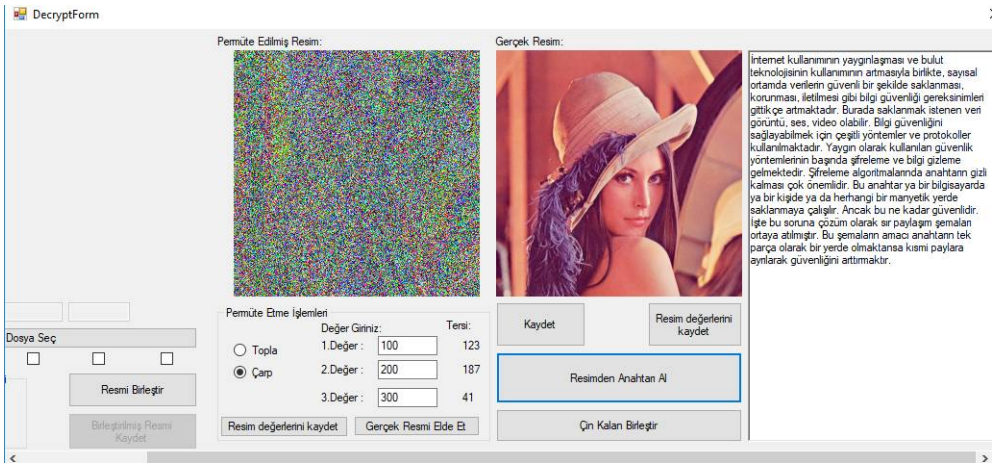
Şekil 6.24. 6872 bit gizli veri gömülü stego-görüntüsüne seçilen asallarla Çin kalan Teorisi tabanlı Asmuth- Bloom GSP şeması ile n=4 Pay görüntüye bölünmesi

Dağıtım kısmından sonra en az k=3 adet rastgele seçilen pay görüntülerden, örneğin aşağıdaki Şekil 6.25' de gösterildiği gibi (1-3-4) pay görüntüleriyle önce permütasyonlu görüntü daha sonra ters permütasyonla veri gömülü görüntü aşağıdaki Şekil 6.26'da gösterildiği gibi elde edilmiştir.



Şekil 6.25. Çin Kalan Teoremini kullanarak (1-3-4) Pay görüntüleri ile permütasyonlu görüntünün elde edilmesi

En son olarak aşağıdaki şekil 6.26’ daki gibi gizlenmiş veriye ve stego görüntüye ulaşılır.



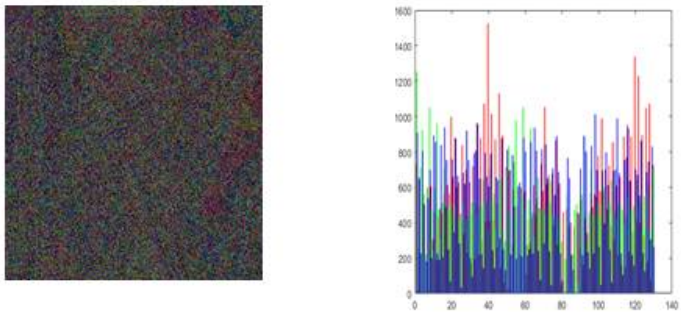
Şekil 6.26. Stegolu görüntü ve gizli verinin elde edilmesi

6.2.2. 2LSB ile Veri Gizlenmiş Görüntünün Çin Kalan Teorisi Tabanlı Asmuth-Bloom Şeması ile Görüntü Sır Paylaşımının Analizi

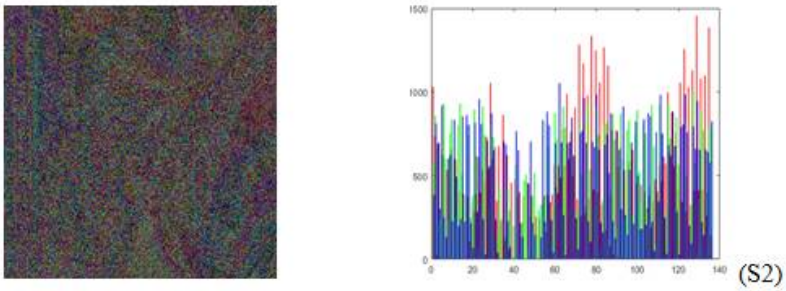
Lena 256x256 bmp. formatında görsele bir uygulamada (73, 131, 137, 167, 199) asalları ve α=12 seçilerek 2LSB ile 80 bitlik (1234567890) gizli anahtar gömülmüştür. Bir başka uygulamada yine aynı görsele (179, 181, 191, 197, 199) asalları ve α=25 seçilerek 6872 bitlik bir deneme metni gömülmüştür. Gömme işleminde RGB katmanında mavi kanal kullanılmış ve her renk kanalı için (100, 200, 300) anahtarı kullanılarak çarpma permütasyonu yapılmıştır. Daha sonra Asmuth Bloom' un Çin kalan teorisi tabanlı GSP şeması uygulanmış. Elde edilen 256x256 boyutlu pay görüntüler ve histogramları aşağıdaki şekillerde verilmiştir. Ayrıca PSNR, MSE, SSIM, korelasyon analizleri değerleri Çizelge 6.6’ de verilmiştir.

Çizelge 6.6. 2LSB yöntemi ile 80bit ve 6872bit gömülü Görüntüler ve Asmuth-Bloom GSP şeması ile elde edilen görüntülerin PSNR, MSE, SSIM, Korelasyon testi sonuçları

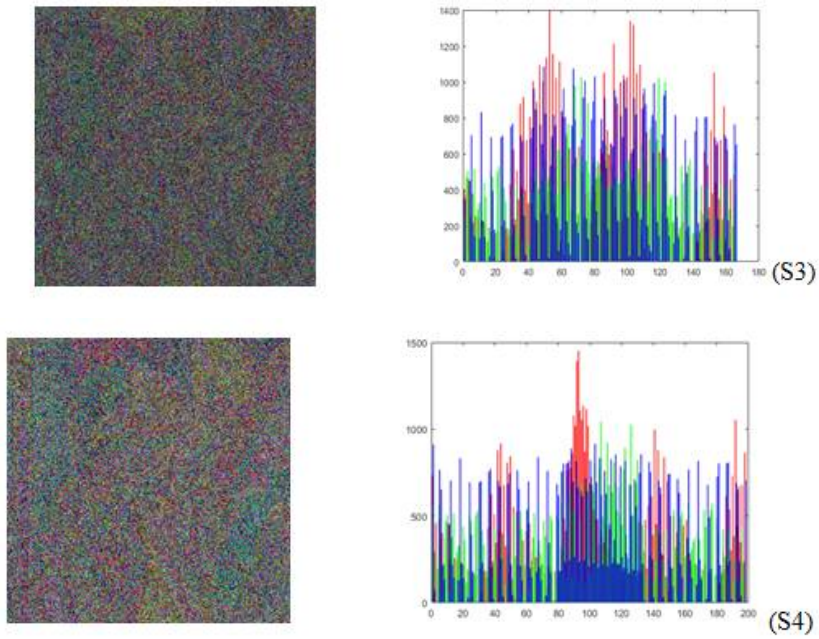
Karşılaştırılan Görüntüler	MSE	PSNR(db)	SSIM	CORR
(2LSB)80 bit gömülü-Orijinal Görüntü	0.000854	78.8137	1	1
(2LSB)6872 bitgömülü-Orijinal görüntü	2.127635	44.8518	0.999273	0.999722
Pay1-Pay2(80bit gömülü)	4205.96	11.8922	0.319000	-0.336610
Pay3-Pay4(80 bit gömülü)	1563.05	16.1910	0.710600	0.731180
Pay1-Pay2(6872bit gömülü)	3026.17	13.3218	0.498623	0.680360
Pay1-Pay3(6872bit gömülü)	11524.20	7.5146	0.012970	-0.016480
Pay1-Pay4(6872bit gömülü)	14834.02	6.4182	0.111400	0.262240
Pay3-Pay4(6872bit gömülü)	6656.32	9.8980	0.348000	0.361340
Pay2-Pay3(6872bit gömülü)	5118.32	11.0390	0.356800	0.420200
Pay2-Pay4(6872bit gömülü)	5667.72	10.5960	0.571500	0.707040
(1-3-4) Paylarıyla yeniden elde edilen – Orijinal Görüntü(80bit gömülü için)	0.000854	78.8137	1	1
(1-3-4) Paylarıyla yeniden elde edilen – Orijinal Görüntü(6872 bit gömülü için)	2.127635	44.8518	0.999273	0,999998
(1-3-4)ile(2-3-4) (80bit) yeniden elde edilen gör. ve (1-3-4) ile (1-2-3)(6872bit)	0	Inf(sonsuz)	1	1



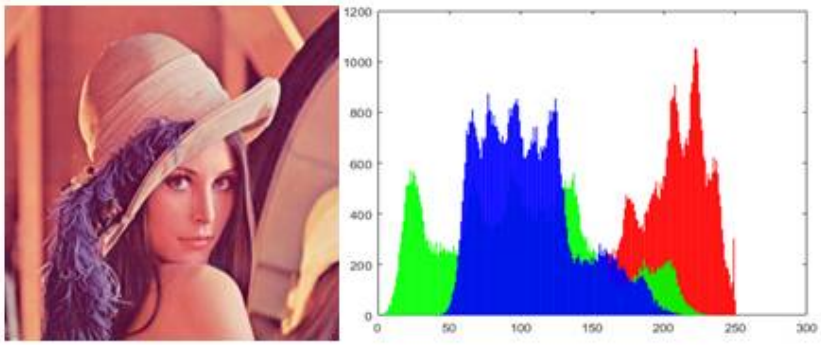
(S1)



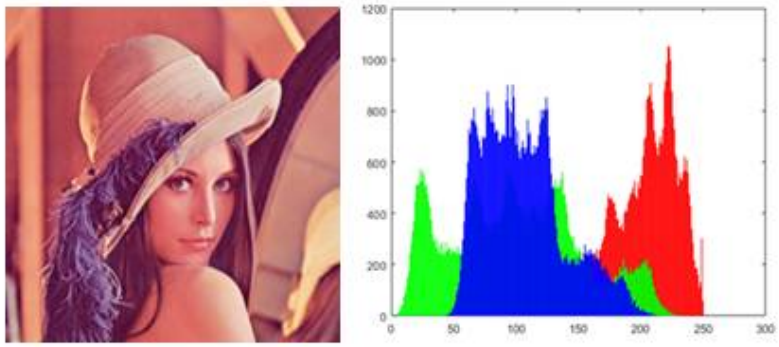
(S2)



Şekil 6.27. Asmuth-Bloom GSP şemasıyla elde edilen pay görüntülerin histogramları



Şekil 6.28. 80 bit veri gömülü olan (1-3-4) Pay görüntüleri ile elde edilen görüntünün histogramı



Şekil 6.29. 6872 bit veri gömülü olan (1-3-4) Pay görüntüleri ile elde edilen görüntünün histogramı

BÖLÜM 7

SONUÇ VE ÖNERİLER

Teknolojinin gelişmesiyle birlikte gizli bilgi iletimindeki güvenlik açıkları ve siber saldırıların artması bu bilginin dış ortamlara karşı korunmasını gerektirmektedir. Özellikle askeri, istihbarat ve bankacılık gibi gizli ve güvenli bilgi akışının zorunlu olduğu açıktır. Bu nedenle bilginin gizliliğini ve güvenliğini sağlamak için pek çok yöntemler kullanılmaktadır. Bunlardan bazıları steganografi ve kriptolojidir. Steganografide amaç gizli bilgiyi bir ortama en iyi ölçütlere göre saklamaktır. Yani saldırganın herhangi bir şey fark etmemesini sağlamaktır. Kriptolojide amaç gizli bilgiyi bir anahtar ile şifrelenerek karmaşık hale getirmektir. Burada da güvenlik için anahtarın korunması gerekmektedir. Bunların yanında kriptografik anahtar yönetiminde Sır Paylaşım Şemalarından faydalanılır. Amaç gizlenmesi gerekli olan anahtar ya da gizli bilgi tek bir yetkilide ya da ortamda saklanmaktansa birçok yetkiliye dağıtarak güvenliği arttırmaktır.

Bu tezde yukarıda bahsi geçen farklı güvenlik yöntemleri birlikte kullanılarak gizli veri ya da şifreleme anahtarının güvenliği iki seviyede sağlanmıştır. Saklama işlemi için görüntü steganografi kullanılmıştır. Özellikle şifrelemede kullanılan gizli anahtarın ya da sır bilginin güvenliği için LSB ve 2LSB bilgi gizleme yöntemi ile birlikte Thien-Lin yöntemine göre sır görüntü paylaşım şeması ve Asmuth-Bloom' un Çin Kalan Teorisi tabanlı sır görüntü paylaşım şemasının uygulaması yapılmıştır. Ayrıca benzer şekilde aynı yöntemler kullanılarak seçilen bir gizli anahtar ile 128 bitlik bir AES şifreleme ve şifre çözme uygulaması gerçekleştirilmiştir.

Gizli anahtar olarak kullanılmak üzere seçilen değer, Lena.bmp resmine LSB ve 2LSB bilgi gizleme yöntemleri ile RGB renk kanalında sadece mavi kanala gömülmüştür. Elde edilen yeni görüntülerin 2LSB için PSNR değeri 78,8137, MSE

değeri 0,000854, SSIM ve korelasyon (CC)değeri 1 olarak ölçülmüştür. Yani yapılan gizleme işlemi ile elde edilen yeni görüntünün orjinale çok benzediği söylenir. İki görüntü kıyaslandığında hem yapılan ölçüm sonucu hem histogramları hem de insan gözüyle ayırt edilemeyeceği gösterilmiştir.

Bu aşamadan sonra uygulanan Thien-Lin GSP şeması ile stego-görüntü pay görüntülere bölünerek gizli anahtarın güvenliği bir kat daha arttırılmıştır. Elde edilen Pay1 ve Pay2 görüntüleri kıyaslandığında PSNR değeri 7,9006, MSE değeri 10544,47, SSIM değeri 0,00041, CC değeri -0,0090; Pay3 ve Pay4 görüntüleri kıyaslandığında PSNR değeri 7,9268, MSE değeri 10480,99, SSIM değeri 0,0069 ve CC değeri -0,00025 olarak hesaplanmıştır. Bu sonuçlara göre elde edilen pay görüntülerin birbirlerinden oldukça farklı olduğu söylenir. Ayrıca payların histogramlarını da değerlendirdiğimizde göze çarpan herhangi bir farklılık sezilmemektedir. Dolayısıyla saldırgan bu paylardan bir tanesini bile ele geçirse gizli veriye hiçbir şekilde ulaşamayacaktır. Gizli veri ancak kullanılan (k,n) şemasına göre k adet pay ile elde edilebilir. k adet pay saldırganın eline geçse dahi burada kullanılan polinom katsayılarının RGB renk kanalında her bir renk için (0-255) aralığında rastgeleliği, permütasyon için kullanılan anahtar değeri, hangi steganografik yöntem kullanıldığı gibi zorluklar gizli veriye ulaşmada gücü gösterir. Böylece bu yöntemlerin birlikte kullanılmasıyla gizli verinin güvenli bir şekilde saklanmasına katkı sağladığını söyleyebiliriz.

Aynı şekilde daha büyük bir gizli veri saklamak istediğimizde yapılan uygulama sonucunda 2LSB için PSNR değeri 44.8518 dB, MSE değeri 2.127635, SSIM değeri 0.999273 ve CC değeri 0.999722 olarak hesaplanmıştır. Yine 6872 bitlik bir veri gömüldüğünde dahi stego-görüntünün orijinal görüntüye çok benzediğini söyleyebiliriz. Çünkü 50 dB civarı PSNR değeri değişimin insan gözüyle fark edilemeyecek derecede küçük olduğunun göstergesidir. Yine Tablo 6.7' de paylar arasındaki değerler incelendiğinde, paylar arasındaki benzerliğin olmadığı söylenir. Çünkü düşük PSNR ve yüksek MSE' ye sahiplerdir.

Benzer şekilde aynı veri gömülmüş stego resme Çin Kalan Teorisi tabanlı Asmuth-Bloom GSP şeması uygulanmıştır. Elde edilen değerler Tablo 6.8' de verilmiştir. Buna göre yine pay görüntüler arasında ilişki yoktur. Ayrıca histogramlarına bakıldığında yine her bir payda gözle fark edilir bir fark yoktur. Ancak seçilen rastgele sıralı asallara ve seçilen asallara göre uygun aralıktaki rastgele

α’ ya göre pay görüntülerin benzerlikleri değişmektedir. Bu yöntemde de saldırgan tek payı ele geçirse dahi gizli bilgi hakkında hiçbir şey elde edemez. (k,n) şemasında k adet pay görüntüyü ele geçirse dahi kullanılan asalların ve α’ nın rastgeleliği Asmuth Bloom şemasının güvenilirliğini göstermektedir.

Dolayısıyla her iki yöntemle yapılan değerlendirmeler sonucunda hem Steganografik yöntemlerin kullanılması hem de Görsel Sır Paylaşım Şemalarının kullanılması kriptografik anahtarın güvenliğinin sağlanmasında oldukça etkilidir. Her iki yöntemin kendi içinde sağladıkları güvenlik mekanizmaları güvenliği iki kat daha arttırmaktadır.

Bunun gibi birçok farklı steganografik yöntemler, sır paylaşım şemaları, şifreleme yöntemleri ve kodlama teorisi gibi alanların birlikteliği ile daha güvenilir sistemler yapılabileceği öngörülmektedir.

KAYNAKLAR

Arda, D., & Buluş, E. (2009,Ekim). *Çin Kalan Teoremini kullanan bir Gizlilik Paylaşım Şeması*. IV.İletişim Teknolojileri Ulusal Sempozyumu, Çukurova Üniversitesi, Adana. http://www.emo.org.tr/ekler/879793f11053b53_ek.pdf

Arda, D., Buluş, E., Akgün, F., & Yerlikaya, T. (2008,Kasım). *Secret Sharing Scheme in Cryptographic Key Management Problem.* International Scientific Conference *UNITECH.* Gabrovo.

Arda, D., Demirbilek, S., & Kavak, S. (2017). The Effect Of Steganography And Secret Image Sharıng Scheme To The Securıty Of Cryptographıc Key. *Journal of International Scientific Publications*,*11*,474-483.

Asmuth, C., & Bloom, J. (1983). Modular Approach to Key Safeguarding. *IEEE Transactions on Information Theory*, *29*(2),208-210.

Baker , J., Lin , T., Shahi , S., & Jayaram, N. (2011). Draft:New ground motion selection procedures and selected motions for the PEER transportation research program.

Blakley, G. R. (1979). Safeguarding cryptographic keys . *National Computer Conference*, 48,313-317.

Chen, Y.-K., Cheng, F.-C., & Tsai, P. (2011). A gray-level clustering reduction algorithm with the least PSNR. *Expert Systems with Applications*, *38*(8),10183-10187.

Cimato, S., De Prisco, R., & De Santis, A. (2007). Colored visual cryptography without color darkening. *Theoretical Computer Science*, *374*(3),261-276.

Daemen, J., & Rijmen, V. (2002). *The Desing of Rijndal: AES- The advanced encrption standard*. Heidelberg: Springer.

Demirci, B. (2016). *Görüntü Steganografi Metotlarının ve Performanslarının Karşılaştırılması*. (Yüksek Lisans Tezi). Selçuk Üniversitesi/Fen Bilimleri Enstitüsü, Konya.

Denning, R. D. (1982). *Cryptography and Data Security.* Massachusetts: Addison-Wesley Publishing Company.

Elgamal, T. (1985). A public key cryptosystem and a signature scheme based on discrete logarithms. *IEEE Transactions on Information Theory*, *31*(4),469 - 472.

Erdoğan, M., & Yılmaz, G. (2008). *Soyut Cebir ve Sayılar Teorisi.* İstanbul: Beykent Üniversitesi Yayınevi.

FIBS PUB-197. (2001). *Advenced Encryption Standard*. 08.04.2019 tarihinde https://it.ojp.gov/NISS/iepd/443 adresinden erişildi.

Forouzan , B. A. (2008). *Cryptography and Network Security.* New York: McGraw-Hill.

Johnson, N., & Katzenbeisser, S. (2000). *Information Hiding Techniques for Steganography and Digital Watermarking*. Boston: Artech House.

Kaya, K., Selçuk, A. A., & Tezcan, Z. (2006). Threshold Cryptography Based on Asmuth- Bloom Secret Sharing. *Computer and Information Sciences 4263*(3), 935-942.

Koblitz, N. (1987). Elliptic Curve Cryptosystems. *Mathematıcs Of Computatıon,48*, 203-209.

Memon, N., & Wong, P. W. (1998). Protecting Digital Media Content. *Communications of the ACM*,*41*, 34-43.

Mignotte, M. (1983). How to Share a Secret. *Cryptography - EUROCRYPT,149*(82), 371-375.

Naor, M., & Shamir, A. (1995). Visual Cryptography. *Advances in Cryptology-Eurocrypt'94,950*, 1-12.

Pang, L. J., & Wang, Y. M. (2005). A new (t, n) multi-secret sharing scheme based on Shamir's secret sharing. *Applied Mathematics and Computation*, *167*(2),840-848.

Petitcolas, F. A., Anderson, R. J., & Kuhn, M. G. (1999). Information Hiding-A Survey. *Proceedings of the IEEE*, *87*(7),1062 - 1078.

Popa, R. (1998). *An Analysis of Steganographic Techniques*. (Master's thesis). The "Polytechnic" University of Timisoara, Timisoara, Romenia.

Rivest, R. L., Shamir, A., & Adleman, L. M. (1978). A method for obtaining digital signatures and public-key cryptosystems. *Communications of the ACM*, *21*(2),120-126.

Schoenmaker, B. (2011). *Lecture Notes Part 1 Crytographic Protocols.*The Netherlands:

Sellars, D. (1999). An Introduction to Steganography.

Shamir, A. (1979). How to Share a Secret. *Communications of the ACM*, *22*(11), 612-613.

Sivaram, M., Devi, D., & Steffi, A. (2012). Stenography of Two LSB Bits. *International Journal of Communications and Engineering,1*(1), 82-87.

Stinson, D.R. (2002). *Cryptography : Theory and Practice. Second Adition*. New York: CRC/C&H.

Şahin Mesut, A., & Arda, D. (2009). *Renkli Görüntü Dosyaları Üzerinde Gizlilik Paylaşımı Uygulaması.* IV İletişim Teknolojileri Sempozyumu, Çukurova Üniversitesi, Adana. http://www.emo.org.tr/ekler/96f735d3704fb4b_ek.pdf

Öztürk, E., Şahin Mesut, A., & Mesut, A. (2011). *LSB Ekleme Yönteminde Bilgi Gizleme İçin Tek Renk Kanal Kullanımının Güvenliğe Etkileri*. 4. Ağ ve Bilgi Güvenliği Sempozyumu, Atılım Üniversitesi, Ankara. http://abg.emo.org.tr/index.php?etkinlikkod=156

Tanchenko, A. (2014). Visual-PSNR measure of image quality. *Journal of Visual Communication and Image Representation*, *25*(5),874-878.

Taşdemir, Ş. (2010). *Dijital Görüntü Analiz Yöntemi İle Siyah Alaca İneklerde Vücut Ölçülerinin Belirlenmesi Ve Canlı Ağırlığının Tahmin Edilmesi*. (Doktora Tezi) Selçuk Üniversitesi/ Fen Bilimleri Enstitüsü, Konya.

Thien, C., & Lin, J.-C. (2002). Secret image sharing. *Computers & Graphics*, *26*(5),765-770.

Trappe, W., & Washington, L. (2006). *Introduction to Cryptography with Coding Theory,Second Edition.* USA: Pearson Education, Inc. Pearson Prentice Hall.

Ulutaş, G., Ulutaş, M., & Nabiyev, V. (2011). Medical İmage Security And EPR Hiding Using Shamir's Secret Sharing Scheme. *Journal of Systems and Software*,*84*(3), 341-353.

Wang, H., & Wang, S. (2004). Cyber Warfare: Steganography vs. Steganalysis. *Communıcatıons Of The Acm*, *47*(10), 76-82.

Wang, Z., Bovik, A., Sheikh, H., & Simoncelli, E. (2004). Image Quality Assessment: From Error Visibility to Structural Similarity. *IEEE Transactıons On Image Processıng, 13*(4), 1-14.

Westfeld, A., & Pfitzmann, A. (2000). Breaking the Steganographic Utilities EzStego, Jsteg,Steganos, and S-Tools—and Some Lessons Learned. *Attacks on Steganographic Systems*.1-16

Zhu, B., Bao, F., Deng, R., & Kankanhalli, M. (2005). Efficient and robust key management for large mobile ad hoc networks. *Computer Networks*, *48*, 657-682.

ÖZGEÇMİŞ

Sermin KAVAK, 1992 yılında Edirne'de doğdu. Liseyi Edirne'de 2010 yılında tamamladı. Aynı yıl Marmara Üniversitesi Matematik Bölümünü kazandı. 2014 yılında fakülteyi bitirip formasyon eğitime başladı. 2015 yılında pedagojik formasyonunu tamamladı. 2015 yılında Trakya Üniversitesi Fen Bilimleri Enstitüsünde Hesaplamalı Bilimler alanında yüksek lisansa başladı. 2017 yılında Gençlik Spor Bakanlığı'nda yurt idare memuru olarak çalışmaya başladı.

TEZ ÖĞRENCİSİNE AİT TEZ İLE İLGİLİ BİLİMSEL FAALİYETLER

Uluslararası Hakemli Dergilerde Yayınlanan Makaleler

Arda, D., Demirbilek, S., & Kavak, S. (2017). The Effect Of Steganography And Secret Image Sharıng Scheme To The Securıty Of Cryptographıc Key. *Journal of International Scientific Publications*, ISSN 1314-7269, Volume 11.