GÖRÜNTÜ ŞİFRELEME İÇİN SCAN PATERNLERİNİ KULLANAN HİBRİT BİR YÖNTEM

Hasan SAKAL[1],Mehmet YILDIRIM[2]

[1]Kocaeli Üniversitesi, Fen Bilimleri Enstitüsü, Bilişim Sistemleri Mühendisliği, Kocaeli Türkiye

[2]Kocaeli Üniversitesi, Teknoloji Fakültesi, Bilişim Sistemleri Mühendisliği Bölümü, Kocaeli Türkiye

hasansakal@yandex.com, myildirim@kocaeli.edu.tr

Özet

Bu çalışmada, görüntü güvenliğinin sağlanması için kullanılabilecek hibrit bir görüntü şifreleme yöntemi önerilmiş ve bu yöntem bir uygulama ile anlatılmıştır. Normalde herhangi bir görüntüye gürültü ekleme işlemi de görüntü şifreleme olarak kabul edilebilmektedir. Ancak bu şekilde yapılan şifreleme basit filtreler tarafından geri dönüştürülebilir. Önerilen yöntem taşıyıcı görüntü ile şifreleme yapma mantığına dayanmaktadır. Şifreli görüntü elde etmek için, üretilen birşifreleyici görüntü orijinal görüntüye eklenmektedir ve bir tarama yöntemi ile taranarak aşırı derecede bozulmuş şifreli bir görüntü elde edilebilmektedir. Elde edilen şifreli görüntünün, hibrit teknik ile daha fazla bozulmuş bir hale geldiği görülmüştür. Şifreli görüntüyü orijinal hale getirmek için ise ters işlem uygulanmaktadır.

Anahtar Kelimeler:Görüntü Şifreleme, Şifreleme, Zigzag Tarama Paterni.

A HYBRID METHOD USING THE SCAN PATERNS FOR IMAGE ENCRYPTION

Abstract

In this study, a hybrid image encryption method that can be used to provide image security is proposed and described in an application. Normally, adding noise to an image can also be considered as image encryption. However, encryption in this way can be recycled by simple filters. The proposed method is based on the ability to encrypt with the bearer image. To obtain an encrypted image, a cryptographic image is added to the original image, and a scrambled image that is extremely distorted can be obtained by

scanning with a scan method. The resulting encrypted image has become more distorted by hybrid technique. In order to make the encrypted image the original, reverse process is applied.

Keywords: Encryption, Image Encryption, Zigzag ScanPatern.

1. Giriş

Şifreleme bilgi güvenliğinin temel alanlarından biridir. İnternetin hayatımızın her alanına girmesiyle beraber şifrelemeye olan ihtiyaç ve buna paralel olarak şifreleme alanındaki gelişmeler hızla artmaktadır. Günümüz bilgi sistemleri için hayati bir yere sahip olan şifreleme ile uzaktan erişim, sertifika tabanlı kimlik doğrulama, çevrimiçi sipariş ve ödemeler, e-posta ve mesaj güvenliğinin sağlanması vb. ihtiyaçlar karşılanabilmektedir. Bu ihtiyaçların karşılanması; bir depolama biriminde kaydedilen ya da ağ üzerinden iletilen verilere sadece izin verilen kullanıcılar tarafından erişilebilmesi anlamına gelmektedir. Bir depolama biriminde kaydedilen ya da güvensiz ağ ortamında iletilen veriler şifreleme ile okunamaz hale getirilirler. Yetkili kullanıcı veriye eriştiğinde, okunamaz haldeki bu veri uygun şifre çözme anahtarı ile tekrar orijinal haline dönüşür. Bu işlem ile gizli veri, güvensiz iletim ortamlarında yetkisiz erişimlere karşı korunaklı hale gelmektedir.

Araştırmacılar geleneksel metin şifreleme yöntemlerinin görüntü şifreleme yöntemlerinde yetersiz kaldığını ortaya çıkarmıştır. Görüntü verilerinin boyutunun metin verilerine göre çok büyük olması, görüntü verileri için farklı şifreleme yaklaşımlarının ortaya çıkmasına neden olmuştur [1]. Bu yaklaşımlar genel olarak kayıplı görüntü şifreleme algoritmaları ve kayıpsız görüntü şifreleme algoritmaları olmak üzere iki kategoride sınıflandırılmıştır. Kayıplı şifreleme yöntemlerinde şifresi çözülen görüntü az ya da çok bozulmaktadır. Kayıplı şifreleme yöntemi, yüksek görüntü kalitesi gerektirmeyen uygulamalar için kullanılabilir. Bu uygulamalarda kayıplı algoritmalar neticesinde oluşacak bozulmalar kabul edilebilir seviyede olmalıdır.

Diğer taraftan, kayıpsız şifreleme algoritmaları yüksek görüntü kalitesi gerektiren uygulamalarda kullanılmak için daha uygundur. Kayıpsız şifreleme metotlarında orijinal görüntü ile orijinal görüntünün şifrelenmesi ve müteakiben şifresinin çözülmesi neticesinde elde edilen görüntü arasında piksel farkı olmayacağından, görüntünün çözünürlüğü yani kalitesinde eksilme meydana gelmeyecektir.

2.Literatür Taraması

Sinha ve Singh [2] güvenli görüntü iletimi için sayısal imzaların kullanıldığı bir teknik önermiştir. Onların yaklaşımına göre orijinal görüntü kullanılarak elde edilen sayısal imza, orijinal görüntünün kodlanmış haline eklenir. Görüntü kodlama işlemi BCH (Bose, Chaudhuri, Hocquenghem) hata kodu kullanılarak gerçekleştirilir. Son kullanıcıda şifreli görüntünün şifresi çözüldüğünde, sayısal imza görüntünün gerçekliğini doğrulamak için de kullanılabilir. Maniccam ve Bourbakis [3] kayıpsız sıkıştırma ile gri tonlamalı ve ikili görüntülerin şifrelemesini gerçekleştiren kayıpsız bir şifreleme metodu sunmuştur. Bu metod tarama (scan) metodolojisi tarafından üretilen tarama paternlerine dayanmaktadır. Keste [4] görüntülerin RGB değerlerinin yerlerinin değiştirilmesi ve karıştırılmasına yönelik bir yöntem önermiştir. Bu yöntem güvenlik analizi açısından etkili bir yöntemdir. RGB değerlerinin fazlaca değiştirildiği bu yöntem ile görüntünün halihazırda mevcut olan tüm olası saldırılara karşı güvenliği artmıştır.Kushwah ve Shibu [5] blok yer değiştirme ve blok şifreleme tekniği üzerine yeni bir görüntü şifreleme tekniği önermiştir. Çalışmada önerilen görüntü şifreleme algoritmasının güvenliği kullanılan anahtarın uzunluğuna bağlıdır. 128 bit anahtar kullanılan çalışmada, anahtarın orijinal haline ulaşmak veya kripto analizini yapmak herhangi bir bilgisayar korsanı için imkansız gözükmektedir.Xu ve Jiali [6] sundukları çalışmada zigzag dönüşüm metodunu kullanmıştır. Junwale, Annapurna ve Sobha [7] hiper görüntü şifreleme algoritmasına dayalı bir görüntü şifreleme tekniği üzerine çalışma yapmışlardır. Çalışmada blok tabanlı görüntü dönüşümü ve hiper görüntü şifreleme teknikleri kullanılarak görüntü güvenliği için bir yöntem sunulmuştur.

Görüntü şifreleme alanında yapılan bazı çalışmalar da frekans alanında görüntü şifreleme üzerine gerçekleştirilmiştir. Krikor ve arkadaşları [8] görüntü şifrelemealanında, karakteristik değerler olarak alınan bazı DCT (DiscreteCosineTransform) yüksek frekansları seçen bir yöntem önermiştir. Bu yöntemde ortaya çıkan şifreli bloklar rasgele karıştırılmaktadır. Pia ve Karamjeet [9] 64 bitlik blowfish metodu kullanılan gizli bir anahtar bloğu şifresini kullanarak güvenliği ve performansı artıran bir çalışma sunmuştur. Çalışmada önerilen algoritma 448 bite kadar değişebilen bir anahtar kullanmıştır. Tang [10] DCT tabanlı video ve görüntülere uygulanan ve zigzagpermütasyon olarak adlandırılan bir yöntem önermiştir. Yöntem belirli bir düzeyde gizlilik sağlamaktadır. Younes ve Jantan [11] görüntü dönüşümü ve

tanınmış Blowfish şifreleme ve şifre çözme algoritması birleşimine dayalı, blok tabanlı bir dönüşüm algoritmasını tanıtmıştır. Çalışmada orijinal görüntü, dönüştürülmüş ve Blowfish algoritması kullanılarak şifrelenmiş bloklara ayrılmıştır. Çalışma göstermiştir ki; küçük blok boyutu kullanmak daha az korelasyon ve daha yüksek entropi sonucunu doğurmaktadır. Bir diğer çalışmada da İsmail ve arkadaşları [12] kaos tabanlı şifreleme algoritması üzerine araştırmalar yapmıştır.Mahajan ve Sachdeva [13] AES, DES ve RSA algoritmalarının güvenliklerinin incelenmesi ile ilgili bir çalışma sunmuştur. Çalışmada AES, DES ve RSA algoritmalarının şifreleme ve şifre çözme performanslarının karşılaştırması yapılmıştır. Karşılaştırma neticesinde her bir algoritmanın etkinliği analiz edilmiştir. Benzer bir çalışmada Brindha, Sharma ve Saini [14] iletim esnasında daha fazla güvenlik sağlayan DES algoritması kullanılarak görüntü şifreleme üzerine çalışma yapmıştır. Çalışmada DES ile AES'in karşılaştırması yapılmıştır. Yazarların daha sonraki çalışmaları resimde gömülü metin verilerinin şifrelenmesi üzerine olmuştur. Ghode [15] kayıpsız RGB görüntülerinde şifreleme yapmak için anahtarsız bir yaklaşımönermiştir.Çalışmada; güvenlik seviyesini yükseltmenin yanında depolama kapasitesinin geliştirilmesi de hedef alınmıştır. Askar, Karawia ve Alshamrani [16] görüntülerin kaotik bir ekonomik haritaya dayalı olarak şifrelenmesi için yeni bir algoritma sunmuştur. Çalışma, kaotik kriptografi alanında kaotik bir ekonomik haritayı uygulamak için yapılan ilk girişim idi. Zhang ve Wang [17] bitişik eşlemli harita kafeslerine dayanan yeni bir görüntü şifreleme algoritması önermiştir. Bitişik olmayan eşlenmiş harita kafesleri sistemi, lojistik haritadan veya eşleştirilmiş harita kafeslerinden daha üstün kriptografik özelliklere sahiptir. Gerçekleştirilen simülasyonlarda, önerilen algoritmanın üstün güvenlik ve yüksek verimliliği diğer algoritmalarla kıyaslanmıştır. Devi, Sharma ve Rangra [18] görüntü şifreleme ve şifre çözme için DES, AES ve Blowfish algoritmaları üzerine tartışmıştır. Yazarlar konu ile ilgili çalışmaları araştırıp, bu çalışmalarla ilgili sorun tespiti yapmışlar ve görüntü şifreleme için yararlı olabilecek öneriler sunmuşlardır.

3.Görüntü Şifreleme

3.1.Görüntü şifrelemeye genel bakış

Teknolojik gelişmelerin çok hızlı olması nedeniyle haberleşme, iletişim ve bilgiye erişim gün geçtikçe hızlanmaktadır. Bu gelişmeler paralelinde kişi ve kurumlar,

kişisel ve kurumsal ihtiyaçlarında elektronik ortamı yoğun olarak kullanmaktadırlar. Artık kâğıt ortamında bilgi tutma faaliyetleri sona ermek üzeredir. Önceleri insanlar hatıra defterleri ve şiir defterleri yazar, kişisel fotoğraflarını albümlerde muhafaza ederlerdi. Kurumlar da yazışmalarında, arşiv kayıtlarının saklanmasında, mali gelir-gider tablolarınınhesaplanmasında vs. kâğıt kullanırlardı. Fakat günümüz teknolojilerinde bütün bunları daha kolay bir şekilde yapabilecekleri elektronik ortamlar gelişti ve gelişmeye devam etmektedir. Elektronik ortam; verilerin üzerine kaydedilip saklandığı ortamların genel adıdır. Bu ortamda saklanan bilgiler çok sayıda kişinin erişimine açık olacağından "bilmesi gereken" prensibine göre bu bilgilere kimin erişebileceğini belirlememiz gerekmektedir. Bu ihtiyaç elektronik ortamda güvenlik kavramını ortaya çıkarmıştır. Günlük hayatımızda resimler geniş bir kullanım alanına sahiptir. Yoğun kullanılıyor olmasından dolayı da onların güvenliğinin sağlanması büyük önem kazanmaktadır. Kişisel resimlerimizin saklanması, askeri bir tatbikat görüntülerinin komuta karargahına aktarılması, insansız hava araçlarının istihbari maksatla çektiği görüntülerin ana üsse aktarılması, banka binalarının planlarının muhafazası vb. hususlarda güvenliğe çok önem verilmektedir. Bu güvenliği sağlamanın yollarından birisi ve belki de en önemlisi bu görüntülerin şifrelenmesi ve şifreli halinin saklanması veya gönderilmesidir. Birçok geleneksel ya da modern şifreleme teknikleri text verilerini korumak için tasarlanmışlardır. Fakat resimler text verilerinden farklıdır. Resimleri şifrelemek için geleneksel şifreleme tekniklerini (RSA ve DES gibi) kullanabilmemize rağmen, bu teknikler iki nedenden dolayı görüntü şifrelemesinde kullanılmaya uygun değildir; birincisi resimlerin boyutları text verisinden genellikle daha büyüktür. Bu nedenle resimleri bu yöntemlerle şifrelemek için daha fazla zamana ihtiyaç duyulmaktadır. Diğer neden ise, şifreli resim verisinin şifresi çözüldüğünde, şifresi çözülen resmin orijinal resme birebir eş olması zorunluluğu yoktur. İnsan algısının karakteristiklerine göre resimdeki ufak bozulmalar genellikle kabul edilebilir durumdadır.

3.2. Scan (Tarama) dilini kullanarak görüntü şifreleme

Scan dilini kullanarak yapılan görüntü şifreleme işleminde şifrelemenin yanında sıkıştırma işlemi de yapılır. Yani scan tabanlı algoritmalar hem sıkıştırma hem de şifreleme yapma kabiliyetine sahiptirler. Scan metodu ikili görüntüler üzerinde uygulanan bir yöntemdir. Metodolojinin uygulanmasında gri tonlamalı (grayscale)

görüntüler bit düzlemlerine bölünürler. Algoritmanın temel amacı en az sayıda bit kullanarak sıkıştırmayı yapabilecek iyi bir tarama yolunu bulmaktır. Sıkıştırma işlemi "run-lengthencoding" yöntemi kullanılarak yapılır. Şifreleme işlemi gizli tutulan bir tarama yolu kullanılarak sıkıştırılmış veriye uygulanır.

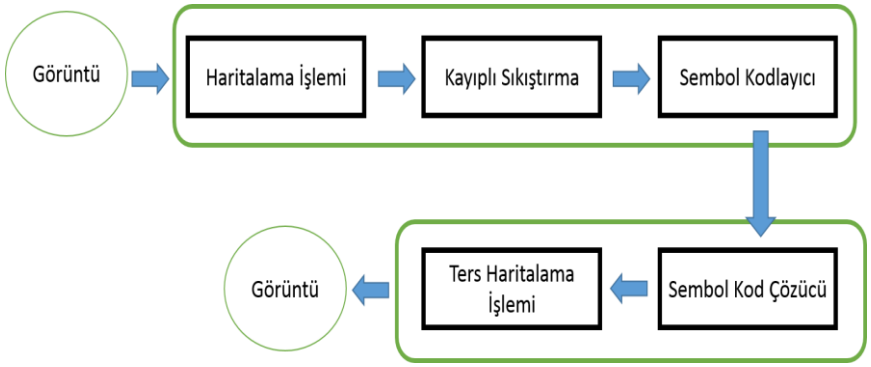
3.2.1. Görüntü sıkıştırma

Görüntü sıkıştırma işlemi;sayısal görüntüyü oluşturmak için gereken veri miktarınıazaltma işlemidir. Bu sayede sıkıştırılmış görüntünün boyutu ilesaklama veiletim gereksinimleri azalarak performans artışı meydana gelir. Sıkıştırmaişlemi aşağıda verilen temel verilerden birinin ya da hepsinin azaltılması yolu ileyapılır:

- Kod Fazlalığı (CodingRedundancy)
- Piksel Fazlalığı (InterpixelRedundancy)
- Görsel Fazlalık (PsychovisualRedundancy)

Kod fazlalığı, optimum kodlamanın yapılmasını ifade eder. Piksel fazlalığı, resminpikselleri arasındaki korelasyondan elde edilir. Görsel fazlalık, insan görme sistemitarafından tanınmayan, görsel olmayan temel bilgileri ifade eder. Görüntü sıkıştırmateknikleri bu fazlalıklardan yararlanarak görüntüyü oluşturan bit sayısını azaltır.Sıkıştırılmış görüntünün tersi işleminde, sıkıştırılmış görüntü üzerinden orijinalgörüntü elde edilir. Sıkıştırma işleminde hedef, görüntü yeniden oluşturulduğundagörsel kalitesi bozulmayacak ve orijinal görüntüye yakın olarak kalacak şekildemümkün olduğunca bitlerin sayısını azaltmaktır. Görüntü sıkıştırma sistemleri iki farklıyapısal blokdan oluşur. Şekil 1'de gösterilen bu bloklar kodlayıcı ve kod çözücübloklarıdır.

Kayıplı ve kayıpsız olmak üzere iki farklı sıkıştırma düzeni vardır. Kayıpsız sıkıştırmada sadece istatistiksel fazlalıktan istifade edilir. Bu yöntemde sıkıştırılan görüntünün orijinal görüntü ile aynı olması muhtemeldir. LZW ya da LZ77 gibi veri sıkıştırma teknikleri GIF, PNG, ve TIFF formatlı görüntülerde kullanılabilmektedir. Doğal görüntüler için sıkıştırma oranı yaklaşık olarak 2:1 olabiliyor iken belge görüntüler için bu oran daha da fazla olabilmektedir. Kayıplı sıkıştırma işlemi ise görüntünün hem istatistiksel hem de algısal yönünden faydalanmaktadır. Bu şekilde sıkıştırılmış görüntü orijinal görüntüye göre bozulmalar içerir. Bu nedenle kayıpsız sıkıştırmaya göre sıkıştırma oranı çok daha yüksektir.



Şekil 1. Görüntü sıkıştırma ve sıkıştırma geri alma işleminin temel blok diyagramı

3.2.2. Scan (Tarama) paterninde sıkıştırma ve şifreleme

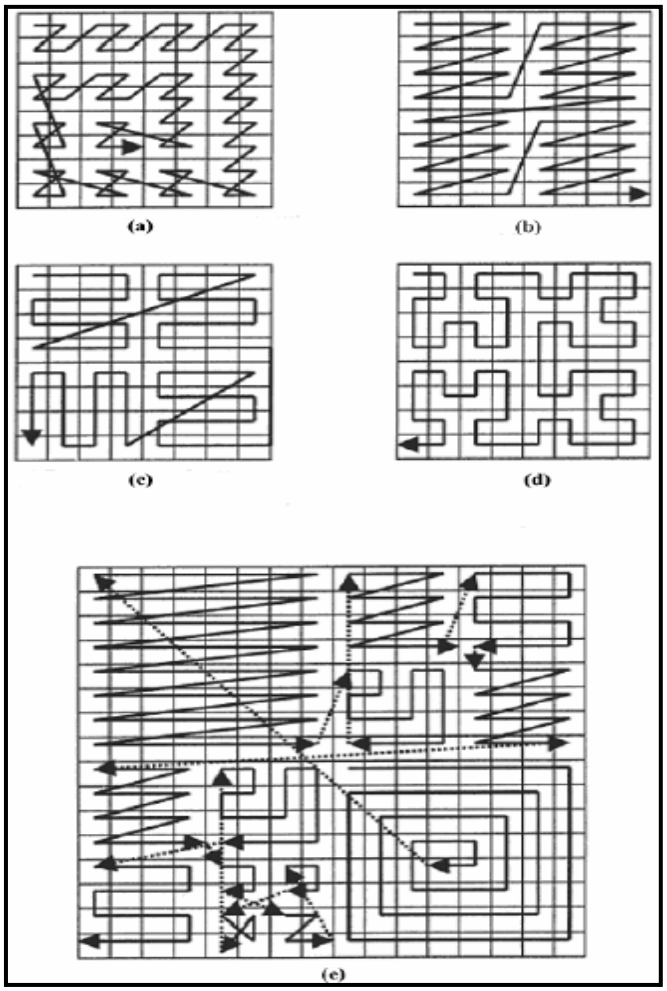
Tarama metodu kullanılarak yapılan sıkıştırma ve şifreleme işlemi ikili görüntülerüzerinde uygulanmaktadır. Tarama yolu üzerindeki bit dizisi ile tarama yolunu temsileden bit dizisi birlikte şifreli ve sıkıştırılmış görüntüyü temsil eder. Buradatarama yollarını temsil eden diziler hakkında dikkat edilmesi gereken bazı anahtarfaktörler mevcuttur. Bu faktörler şunlardır:

- Tarama yolu kısave etkili olmalıdır kitemsil eden bit sayısı da az olsun.
- Pratikte görüntülerin çoğu homojen değildir.Bu yüzden bunlarhomojen olmayantarama yolları kullanılarak taranmalıdır.
- Sıkıştırma işlemi yapılan bazı görüntülerin belli bölgelerinde daha fazla bite ihtiyaç duyulmaktadır. Bu tür bölgeler sıkıştırılmış görüntü içindekendiorijinalbiçiminde muhafaza edilmelidir.

Tarama paternleri; basit, genişletilmiş ve yaygın tarama paterni olarak gruplandırılırlar.Yukarıda belirtilen faktörler göz önüne alınırsa, yaygın taramanın sıkıştırma ve şifreleme içindaha uygun olacağını söylemek mümkündür. Basit tarama ve genişletilmiş taramakısa ve etkilidir. Fakat homojen olmayan görüntülerde bu tarama yöntemleri homojenolmayan etkili bir tarama yolu sağlayamaz. Şekil 2'de basit, genişletilmiş ve yaygıntarama paternleri gösterilmektedir.

Sıkıştırma ve şifreleme taramasında dört temel tarama paterni kullanılır. Bunlar;

- Sürekli Raster tarama
- Sürekli çapraz
- Sürekli dik
- Sarmal

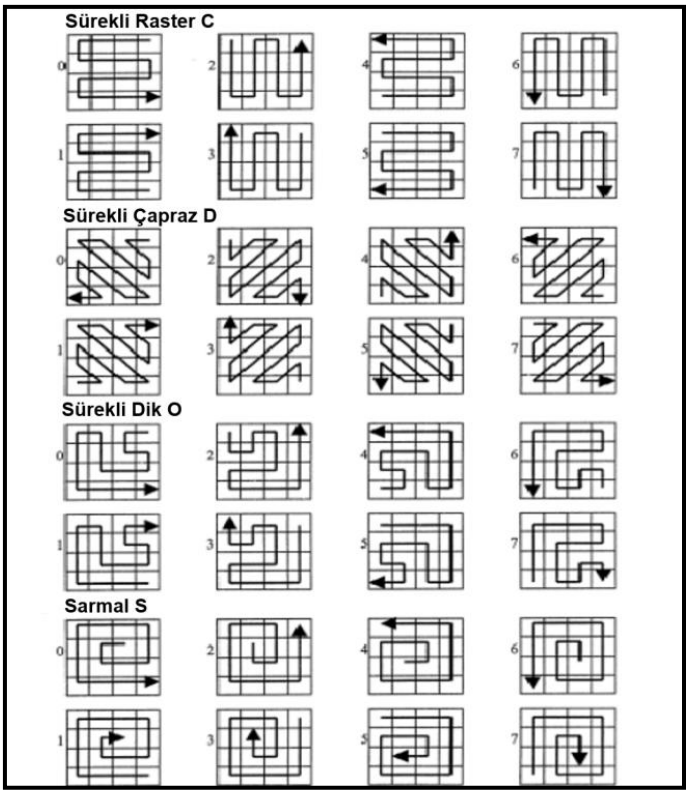


Şekil 2. Basit tarama (a ve b), genişletilmiş tarama(c ve d) ve yaygın tarama paternleri (e) [19]

Tüm bu tarama paternleri0-7'den başlayan sekiz dönüşüme sahiptir. 1,3,5 ve 7dönüşümleri sırasıyla 0,2,4 ve 6'nın ters dönüşümleridir. Şekil 3'de sıkıştırma veşifreleme taraması için temel tarama paternleri gösterilmektedir.

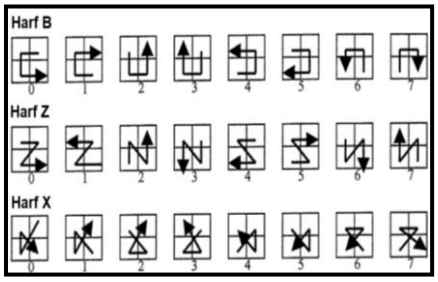
Çoğu görüntünün farklı bölümleri için farklı tarama türlerine ihtiyaç duyulur. Sıkıştırma ve şifreleme taraması bir görüntünün ardışık dört alt bölgeye bölünmesine olanak tanır ve bu alt bölgelerin tümü ayrı ayrı taranır. Bir görüntü bölümlere ayrıldığı zaman, alt bölgelerin taranma sırası bölüm paternleri tarafından belirlenir. Üç adet bölüm paterni vardır. Bunlar:

- Harf B (Letter B)
- Harf X (Letter X)
- Harf Z (Letter Z)



Şekil 3. Sıkıştırmaveşifrelemetaramasıiçintemeltarama paternleri [19]

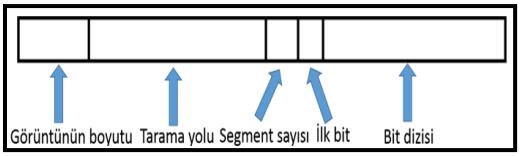
Bu paternlerin her biri aynı zamanda başlangıcı 0-7 olan sekiz dönüşüme sahiptir vetemel tarama paternlerindeolduğu gibi 1,3,5 ve 7 dönüşümleri 0,2,4 ve 6'nın tersdönüşümleri olmaktadır. Şekil 4'de sıkıştırma ve şifreleme taramasının bölümpaternleri gösterilmektedir.



Şekil 4. Bölüm paternleri [19]

Sıkıştırılmış bir görüntü Şekil 5'de gösterilen beş bileşenden oluşmaktadır. Bubileşenler şunlardır:

- Görüntünün boyutu
- Sıkıştırma için kullanılan tarama yolu
- 0 ve 1'lerden oluşan segmentsayısı
- Tarama yolundaki ilk bit
- Tarama yolundaki bit dizisi



Şekil 5. Sıkıştırılmış bir görüntünün bileşenleri

4. Görüntü Şifreleme İçin Önerilen Yöntem

Bu çalışmada, görüntü şifreleme için hibrit bir yöntem önerilmektedir. Yöntem; taşıyıcıgörüntü ile şifreleme yapma mantığına dayanmaktadır.Uygulama, Matlabprogramı kullanılarak hazırlanmıştır. Uygulamadaşifreleme metodu olarak, tarama (scan) yöntemine göre oluşturulan şifreleyici görüntüve tarama paternlerinin kullanıldığı hibrit bir teknik kullanılmıştır. Uygulanan yöntemtarama yöntemi gibi literatürde mevcut bir yöntemi içeriyor olsa da, şifreleme içinkullanılan şifreleyici görüntü ve hibrit yöntem çalışmaya yenilik katmaktadır. Şifreleyicigörüntü oluşturmak için 8 bit değere sahip alfanümerik anahtar kelime kullanılmıştır.Şifreli görüntü elde etmek için, üretilen bu şifreleyici görüntü orijinal görüntüye eklenir.Aşırı derecede bozulmuş şifreli bir görüntü elde edebilmek için şifreleyici görüntü ileorijinal görüntü birleştirildikten sonra tarama yöntemi ile şifreli görüntü elde edilir. Elde edilen şifreligörüntünün, hibrit teknik ile daha fazla bozulmuş bir hale geldiği görülmüştür. Şifreligörüntüyü orijinal hale getirmek için ise ters işlem uygulanır.Şifreleme işlemi görüntü bilgilerinin herhangi bir filtre ile geri dönüştürülemeyecekşekilde değiştirilmesi anlamına gelmektedir. Normalde herhangi bir görüntüye gürültüekleme işlemi de görüntü şifreleme olarak kabul edilebilmektedir. Ancak buşekilde yapılan şifreleme basit filtreler tarafından geri dönüştürülebilir. Bu nedenle, buçalışmada kullanılan teknikte ilk önce, hariçten girilen bir şifre vasıtasıylaoluşturulan şifreleyici görüntü ile görüntü piksellerinin ve satırların yönü değiştirilmektedir.Daha sonra şifreleyici görüntü, orijinal görüntü için bir anahtar olarak uygulanmaktadır.Uygulamanın şifreleme bölümü için işlem basamakları aşağıda sıralanmıştır:

- Şifrelenecek görüntününuygulamayaeklenmesi
- Şifreleyici görüntü oluşturmakiçin şifrenin girilmesi
- Girilen şifreile 4'e 8kod vetarama paternikullanılarak şifreleyicigörüntününoluşturulması

- Şifreleyici görüntüileorijinalgörüntünün birleştirilmesi
- Taramapaterni kullanılarakşifrelemenin yapılması

Uygulamanın şifre çözme bölümü için işlem basamakları aşağıda sıralanmıştır:

- Şifreyi çözmek için parolanın girilmesi
- Şifreligörüntüyeterstarama paterninin uygulanması
- Girilen şifre ile4'e 8 kodve taramapaternikullanılarakşifreleyici görüntününoluşturulması
- Şifreli görüntüdenşifreleyicigörüntünün çıkarılması ve orijinal görüntüneldeedilmesi

Uygulamada, şifreleme ve şifre çözme performansını karşılaştırabilmek maksadıylaPSNR (PeakSignaltoNoiseRatio-Tepe Gürültü Sinyal Oranı) hesaplaması kullanılmıştır.PSNR, görüntüler arasında en yüksek sinyal gürültü oranı hesaplaması olarak ifadeedilebilir. İki görüntü arasında PSNR ölçümü desibel olarak ifade edilir. PSNR oranı;orijinal ile işlenmiş veya sıkıştırılmış görüntü arasındaki kalite ölçümü içinkullanılmaktadır. PSNR değerinin yüksek olması elde edilen görüntünün kalitesininyüksek olduğu anlamına gelmektedir. PSNR hesaplaması şifreli görüntü ile anagörüntü arasındaki tepe gürültü oranını karşılaştırmaktadır. Şifreli görüntü ile anagörüntünün PSNR'ı çok düşük ve şifresi çözülen görüntü ile ana görüntünün PSNR'ıçok yüksek olmalıdır.

4.1. 8'e 4 kod kullanarak şifreleyicigörüntü oluşturma

Bu çalışmada 8'e 4 kod olarak adlandırılan bir yöntem kullanılmıştır. Bu koddördü 1 ve dördü 0'dan oluşan 8 bit uzunluğunda bir koddur. Ayrıca her dörtlü grup2 adet 0 ve 2 adet 1'den oluşacak şekilde düşünülmüştür. Tablo1'de 8'e 4 kodşartını taşıyan tüm olasılıklar gösterilmiştir. Ayrıca bu tabloda gösterildiği üzere herkod bir alfanümerik karaktere atanmıştır. Alfabedeki 26 harf (Türkçe karakterbarındıran harfler kullanılmamıştır) ve bir basamaklı 10 sayı ile oluşturulan 36alfanümerik karakter sayesinde, her alfanümerik karaktere benzersiz bir kod atamakiçin daha uygun bir durum oluşmuştur.Farklı anahtar kelimeler girildiğinde, her anahtar kelime orijinal görüntünün boyutunaeşit boyutta bir matris formunda alınır. Eğer anahtar kelimeninboyutu çok küçük ise aynı anahtar kelime, boyutu orijinal görüntünün boyutuna eşitoluncaya kadar tekrar edilir. Tablo1'de gösterilen 8'e 4 kod ve alfanümerikkarakterler kullanılarak şifreleyici görüntü oluşturulur. Anahtar kelimeye

bağlı olarakoluşturulan bu şifreleyici görüntü, şifreli bir görüntü elde etmek için orijinal görüntüyeeklenmek üzere kullanılır.

Parolanın resme eklenmesi işlemini, girilen parolanın "parola" olduğu varsayılarak şu şekilde özetlenebilir. Uygulama yazılımı hariçten girilen parolanın her harfinin binary karşılığını Tablo 1'den bulur ve her harfin binary değerini desimal değere dönüştürür.

Tablo 1. Alfanümerik karakterleri ile birlikte 8'e 4 kodlarının 36 muhtemel kombinasyonu [20]

SL NO.	BIN	HEX	DEC	ALPHA NUMERIC
1	00110011	33	51	A,a
2	00110101	35	53	B,b
3	00110110	36	54	C,c
4	00111001	39	57	D,d
5	00111010	3A	58	E,e
6	00111100	3C	60	F,f
7	01010011	53	83	G,g
8	01010101	55	85	H,h
9	01010110	56	86	I,i
10	01011001	59	89	J,j
11	01011010	5A	90	K,k
12	01011100	5C	92	L,L
13	01100011	63	99	M,m
14	01100101	65	101	N,n
15	01100110	66	102	O,o
16	01101001	69	105	P,p
17	01101010	6A	106	Q,q
18	01101100	6C	108	R,r
19	10010011	93	147	SS
20	10010101	95	149	T,t
21	10010110	96	150	U,u
22	10011001	99	153	V,v
23	10011010	9A	154	W,w
24	10011100	9C	156	X,x
25	10100011	A3	163	Y,y
26	10100101	A5	165	Z,z
27	10100110	A6	166	0
28	10101001	A9	169	1
29	10101010	AA	170	2
30	10101100	AC	172	3
31	11000011	C3	195	4
32	11000101	C5	197	5
33	11000110	C6	198	6
34	11001001	C9	201	7
35	11001010	CA	202	8
36	11001100	CC	204	9

Örnek parola: " parola "

Binary karşılığı:

01101001 00110011 01101100 01100110 01011100 00110011

p a r o l a

Desimal karşılığı:

105 51 108 102 92 51

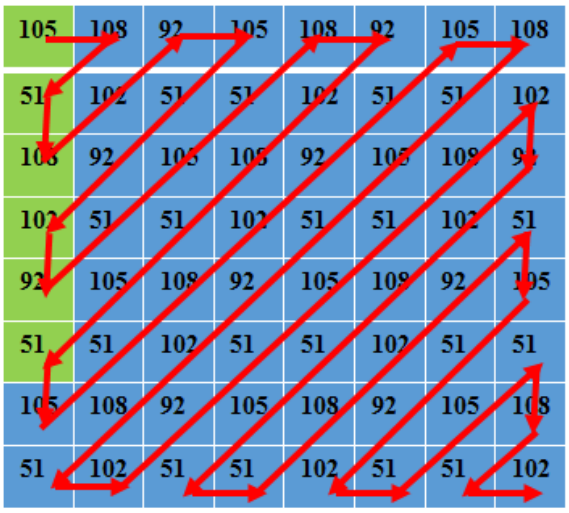
p a r o l a

Bu şekilde elde edilen dizi (105, 51, 108, 102, 92, 51) Şekil 6'da gösterildiği gibi orijinal görüntünün boyutuna eşit bir matris elde edilene kadar tekrar edilir ve müteakiben zigzag tarama paterni ile taranır. Bu işlem neticesinde Şekil 7'deki şifreleyici görüntü matrisi oluşmuş olur.

Oluşan şifreleyici görüntü matrisinin boyutu orijinal görüntüye eşit olduğundan ikisi arasında birleştirme işlemi yapılabilmektedir. Birleştirme işlemi her iki matrisin aynı lokasyondaki elemanları arasında yapılmaktadır. Bu birleştirme işlemi ile hariçten girilen parola orijinal resme eklenmiş olur.

Şekil 8'de aynı resim üzerinde farklı anahtar kelimeler kullanılarak oluşturulan 3 farklı şifreleyici görüntü verilmiştir. Bu şifreleyici görüntüler için sırasıyla şu anahtar kelimeler (parolalar) kullanılmıştır:

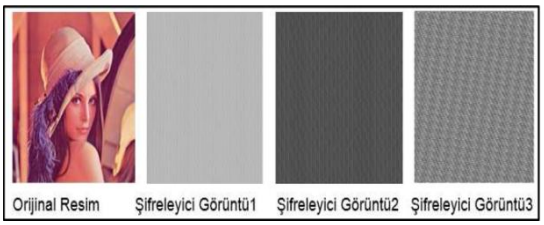
- Parola 1: 123456
- Parola 2: fenbilimleri
- Parola 3: 1yukseklisans2tez15



Şekil 6. Şifreleyici görüntünün oluşturulması

105	92	102	102	92	51	51	92
108	102	108	92	102	108	51	102
51	92	51	51	108	102	108	51
108	51	105	105	51	92	102	105
102	105	51	108	102	102	92	51
92	51	105	51	92	108	51	108
105	108	51	105	51	51	105	51
51	92	108	51	105	105	51	102

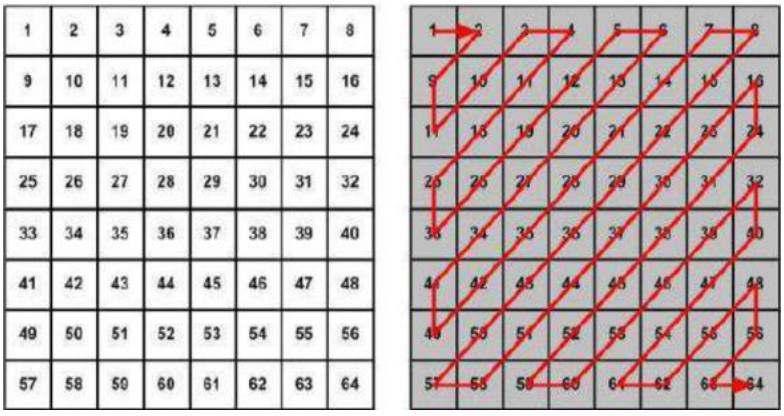
Şekil 7. Şifreleyici görüntü matrisi



Şekil 8. Farklı parolalar kullanılarak oluşturulmuş şifreleyici görüntüler

4.2. Şifreleme için kullanılan yöntem

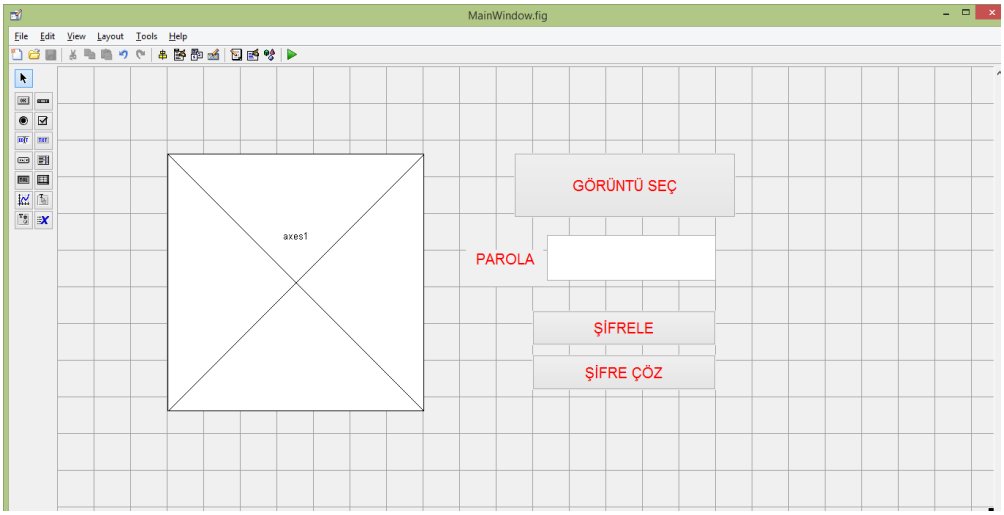
Uygulamada "Çift Tarama" yöntemi kullanılmıştır. "Çift Tarama" yönteminde şifreleyicigörüntü ilk önce şifrelenmiş, daha sonra orijinal görüntüyle birleştikten sonra oluşangörüntü yeniden şifrelenmiştir. Bu şifrelemede zigzag tarama yöntemi kullanılmıştır.Zigzag tarama yönteminin uygulanışı Şekil 9'da gösterilmektedir.



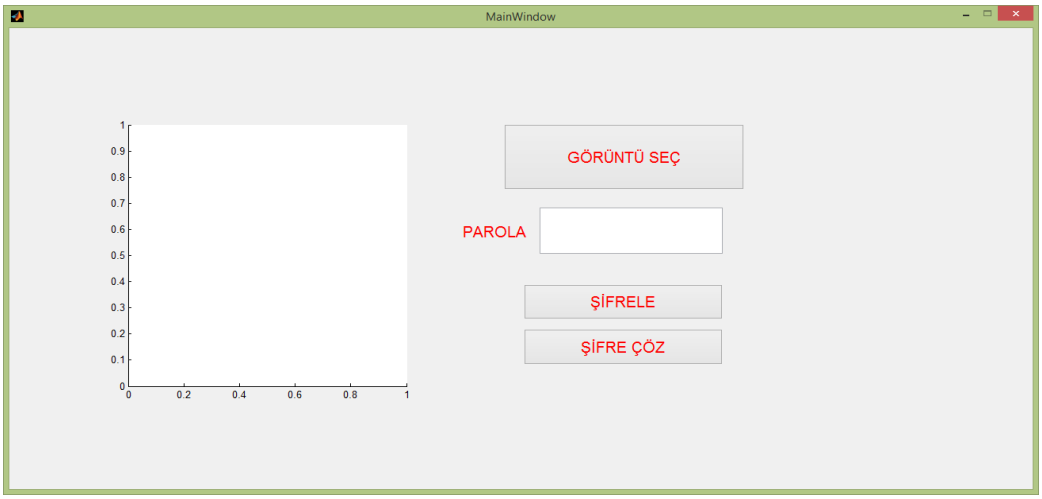
Şekil 9. Zigzag tarama yönteminin uygulanışı

4.3. Geliştirilen şifreleme yöntemi içinuygulama yazılımı

Uygulama yazılımında, şifrelemesi yapılacak görüntünün seçilmesi ve girilen parolaya göre şifreleyici görüntü ve şifrelenmiş görüntü oluşturulması maksadıyla Matlab GUI kullanılarak Şekil 10'daki ara yüz oluşturulmuştur.



Şekil 10. Uygulamanın .fig dosyası



Şekil 11. Uygulamanın çalışan görüntüsü

Ara yüzde görüntü seçme, şifreleme ve şifre çözme işlemlerini yaptırmak amacıyla 3 adet "pushbutton", seçilen, şifrelenen ve şifresi çözülen görüntünün gösterilmesi amacıyla 1 adet "axes" ve şifreleyici görüntüde kullanılacak parolanın girilmesi amacıyla 1 adet "edittext" kullanılmıştır.

4.4. Uygulama yazılımının çalışması

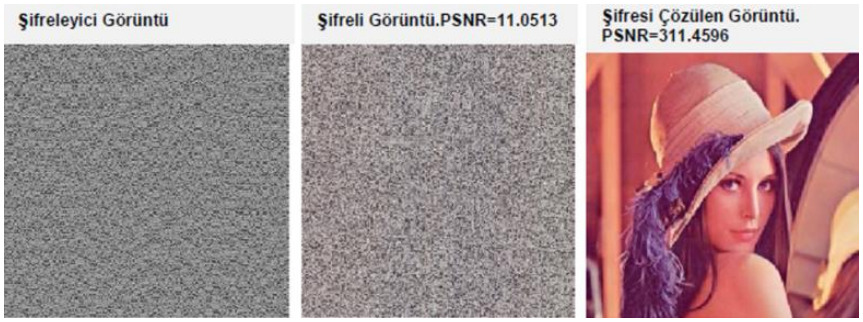
Uygulama çalıştırıldığında Şekil 11'deki görüntü ekrana gelmektedir. Kıyaslamayapmak maksadıyla kullanılacak farklı parolalar ve bu parolalarda oluşacak şifreligörüntü ve bu görüntülere ait PSNR oranları aşağıda gösterilmiştir (Şekil 12, Şekil 13, Şekil 14, Şekil 15).

- Parola 1: 123456
- Parola 2: fenbilimleri
- Parola 3: 1yuksek2tez15

Şekil 12. Orijinal Lena görüntüsü

Şekil 13. Parola 1 ile yapılan şifreleme ve şifre çözme işlemi neticesinde elde edilengörüntü

Şekil 14. Parola 2 ile yapılan şifreleme ve şifre çözme işlemi neticesinde elde edilen görüntü



Şekil 15. Parola 3 ile yapılan şifreleme ve şifre çözme işlemi neticesinde elde edilengörüntü

Yukarıdaki şifrelemelerde kullanılan 3 farklı paroladan ilk parola sadece rakamlardan,ikinci parola sadece harflerden ve üçüncü parola da rakam ve harflerin

karışımındanoluşmaktadır. Yapılan şifreleme ve şifre çözme işlemleri neticesinde elde edilengörüntülerin PSNR oranları incelendiğinde parola olarak sadece rakam kullanılarakyapılan şifrelemede PSNR oranı 310, sadece harf kullanılarak yapılan şifrelemedePSNR oranı 316 ve rakam ile harfin karışımı parola kullanılarak yapılan şifrelemedePSNR oranı 311 çıkmıştır. Buradan sadece harf kullanılarak yapılan şifreleme ve şifreçözme işlemi neticesinde elde edilen görüntü kalitesinin en yüksek olduğu, sadecerakam kullanılarak yapılan şifreleme ve şifre çözme işlemi neticesinde elde edilengörüntünün kalitesinin en düşük olduğu ve rakam ile harf karışımı parola kullanılarakyapılan şifreleme ve şifre çözme işlemi neticesinde elde edilen görüntü kalitesinin isediğer ikisinin arasında bir kalitede olduğu görülmektedir. Burada yapılan kıyaslama buüç görüntü arasında yapılan bir kıyaslama olduğundan; kalite olarak düşük sonuçveren görüntünün kalitesinin de kabul edilebilir seviyede olduğu söylenebilir.

Bu çalışmada, mevcut tarama paterni kullanılarak yapılan şifrelemedekigüvenlik seviyesi artırılmıştır. Bunu yapmak için mevcut tarama paternine ilave olarak,belirlenen bir parola neticesinde elde edilen şifreleyici görüntü kullanılmıştır.Uygulamada sadece tarama paterni kullanılarak yapılan şifreleme ve şifre çözmeişlemi neticesinde elde edilen görüntüler Şekil 16'da verilmiştir.

Şekil 16. Mevcut tarama yöntemi ile yapılan şifreleme ve şifre çözme işlemi neticesinde elde edilen görüntü

Mevcut tarama yöntemi kayıpsız sıkıştırma ve şifreleme sağlayan bir yöntemdir. Fakat tarama yönteminin güvenliği kullanılan tarama paterninin gizliliğine bağlıdır. Sadece tarama paterni kullanılarak yapılan şifrelemedeki bozulma bu çalışmada önerilen hibrit yönteme göre daha azdır. Hibrit yöntem ile önerilen yapıdaki şifreleyici görüntü ile çift tarama metodu, şifreli görüntüdeki bozulmayı arttırmıştır. Bu sayede önerilen hibrit yöntem ile şifreli resimdeki bozulma miktarı ile beraber güvenlik seviyesi de arttırılmıştır.

5. Sonuçlar

Günümüzde internet hemen hemen hayatımızın her alanına girmiş bulunmaktadır. İnternet vasıtasıyla birçok işimizi halledebilmekteyiz; örneğin e-posta yoluyla iletişim, bankacılık işlemleri, dosya depolaması yapma, bir ürün hakkında bilgi edinme, iş başvurusu yapma gibi pek çok amaç için interneti kullanmaktayız. Bu büyük platformda, uygulamaları kullanırken kendi kişisel bilgilerimizi (kredi kartı numaramız, e-posta şifremiz, özlük bilgilerimiz vs.) ortama sunmak veya ağ üzerinden dosya, e-posta vb. yüklemeler yapmak durumunda kalmaktayız. Bunların yanında kişisel ya da kurumsal işlemlerde kullanılan görüntüler internet ortamında gün geçtikçe artmaktadır. Bu görüntülerden bazıları herkesin görmesinde sakıncaolmayan görüntüler olmakla birlikte kimi görüntüler ise başkasının görmesi veya ele geçirmesi durumunda zaafiyet yaratacak türden görüntüler olabilmektedir.

İnsanlar internet üzerinde ve sosyal paylaşım sitelerinde resimlerini paylaştığı gibi, kurumlar da uygulamalarında bilgi sistemlerine geçiş yapmakta ve bu uygulamaların bazılarında resimler kullanmaktadır. Örnek verecek olursak; askeri bir birliğin komuta merkezine istihbari değer taşıyan görüntüler gönderilmesi, bankaların planlarını sanal ortamda saklaması, özel resimlerimizin bizden başkalarının ulaşamayacağı şekilde depolanması kişiler ve kurumlar için son derece önem arz etmektedir. Bu ihtiyaçlar ışığında kişiler ve kurumlar gizlilik ve güvenliklerini sağlayacak tedbirlere ihtiyaç duymaktadır.

Veri güvenliğinin sağlanması hususunda çok sayıda çalışma yapılmıştır. Bu çalışmalardan bazıları görüntü güvenliğinin sağlanması alt başlığı üzerine olmuştur. Bu çalışmalar ışığında yapılan bu çalışmada kaynakçada da gösterilen makale ve tezlerden faydalanılmıştır. Çalışmanın uygulama safhasında, görüntü şifreleme metodu olarak kullanılan hibrit yapı çalışmaya farklılık katmıştır. Diğer çalışmalarda belirtilen sayısal imza mantığı, bu çalışmada şifreleyici görüntü oluşturmak için kullanılmış ve bu şifreleyici görüntü ile orijinal görüntünün karıştırılarak şifrelenmesi aşamasında da çift tarama metodu kullanılmıştır. Önerilen yöntem için bir uygulama yazılımı geliştirilmiştir. Uygulama yazılımı Matlab'da yazılmıştır. Karşılaştırma yapabilmek için üç farklı alfanümerik şifre kullanılmış ve PSNR oranlarına bakılmıştır. Harf kullanılarak oluşturulan alfanümerik şifrede şifreleme kalitesi daha yüksek bulunmuştur.

Sonuç olarak, görüntü şifreleme alanında literatürde bulunan yöntemler, yapılan çalışmalar neticesinde artmaya devam etmektedir. Güvenlik alanındaki tehditlerin çokluğu bu tür çalışmaları hayati öneme haiz bir konuma getirmektedir. Bu çalışmanın da görüntü güvenliğinin sağlanması yönünde yapılan araştırmalara ışık tutması beklenmektedir.

Kaynaklar

[1] Saraf K.R, Jagtap V.P, Mishra A. K. Textand Image En-cryptionDecryption Using Advanced EncryptionStandard,*Inter-nationalJournal of EmergingTrends&Technology in ComputerScience (IJETTCS)*, 3(3), 118-126.

[2] Sinha A, Singh K. A Techniquefor Image Encryption Using DigitalSignature*ElsevierOpticsCommunicationsJournal*, 2003, 218(4-6), 229-234.

[3] ManiccamS,BourbakisN.LosslessImageCompressionandEncryption Using SCAN,*ElsevierPatternRecognitionJournal*,2001, 34(6), 1229-1245.

[4] Keste Q. A. Image Encryptionbased on the RGB PIXEL TranspositionandShuffling, I*. J. Computer Network and Information Security*, DOI: 10.5815/ijcnis.2013.07.05.

[5] Kushwah K, Shibu S. New Image EncryptionTechniqueBased On Combination of BlockDisplacementandBlockCipherTechnique,*International Journal of ComputerScienceand Information Technologies*, 2013, 4(1), 61 – 65.

[6]Xu X, Jiali F.ResearchandImplemention ofImageEncryptionAlgorithmBasedon ZigzagTransformationandInnerProduct PolarizationVector,*IEEEInternationalConferenceonGranularComputing*,DOI: 10.1109/GrC.2010.11.

[7] Junwale P, Annapurna R. M, Sobha G. A Review on Image EncryptionTechniquebased on Hyper Image EncryptionAlgorithm,*International Journal of Advanced Research in ComputerScienceand Software Engineering*, 2013,**3**(11), 614-618.

[8]KrikorL,BabaS,ArifT,ShaabanZ. Image Encryption UsingDCTandStreamCipher,*EuropeanJournalofScientificResearch*,2009, 32(1),47-57.

[9] Pia S, Karamjeet S. Image EncryptionAndDecryption Using BlowfishAlgorithmInMatlab,*International Journal of Scientific&EngineeringResearch*, 2013, 4(7).

[10] TangL.MethodsforEncryptingandDecryptingMPEGVideoDataEfficiently,*4thACMInternationalConferenceon Multimedia*, DOI: 10.1145/244130.244209.

[11] AliM,YounesBandJantan A.ImageEncryptionUsingBlock-BasedTransformationAlgorithm,*IAENGInternationalJournalofComputerScience*,2008, 35(1), 15-23.

[12] Ismail IA,AminM,DiabH.ADigital ImageEncryptionAlgorithmBasedA CompositionofTwoChaoticLogisticMaps,*InternationalJournalofNetworkSecurity*, 2010, 11(1), 1-10.

[13] Mahajan P, Sachdeva A. A Study of EncryptionAlgorithms AES, DES and RSA for Security, *Global Journal of ComputerScienceandTechnology Network, Web & Security (GJCSTNWS)*,2013 13(15).

[14] Brindha K, Sharma R, Saini S. Use of SymmetricAlgorithmfor Image Encryption,*International Journal of InnovativeResearch in ComputerandCommunicationEngineering*, 2014 2(5), 4401-4407.

[15] Ghode P.S. A KeylessApproachtoLossless Image Encryption, *International Journal of Advanced Research in ComputerScienceand Software Engineering (IJARCSSE.)*, 2014 4(5), 1459-1467.

[16] Askar S.S, Karawia A.A, Alshamrani A. Image EncryptionAlgorithmBased on ChaoticEconomic Model,*Hindawi Publishing Corporation, Mathematical Problems in Engineering*, 2015, 1(1), 10.

[17] Zhang Y.Q,Wang X.Y. A New Image EncryptionAlgorithmBased on Non-AdjacentCoupledMapLattices, *AppliedSoft Computing*, 2015, 26(1), 10–20.

[18] Devi A, Sharma A,Rangra A. A Review on DES, AES andBlowfishfor Image Encryption&Decryption,*Aarti Devi et al, / (IJCSIT) International Journal of ComputerScienceand Information Technologies*, 2015, 6(3), 3034-3036.

[19]SnehashısJ.ImageCompressionandEncryptionUsingScanPattern,MasterThesis,NitRorkela,DepartmentofElectronicsandCommunication,Rourkela,2014.

[20] Sunil K. M., Kiran K., Anand U. H., Image Encryption Using Modified 4 out of 8CodeandChaoticMap, *International Journal of Computer Applications*, 2013,74(11), 1-6.