RENKLİ TAŞIYICI VE RENKLİ GİZLİ GÖRÜNTÜLERİN GÖRÜNTÜ ÖZELLİK TABANLI İKİ KATMANLI ŞİFRELEME VE EN ÖNEMSİZ BİT YÖNTEMİ KULLANILARAK FİLİGRANLANMASI

Hüseyin YAŞAR[1], Gamze Hikmet ÖZTERİŞ[2], Murat CEYLAN[3]

[1]T.C Sağlık Bakanlığı, 06434, Ankara, Türkiye

[2]Elit Mühendislik Ltd. Şti., 42030, Konya, Türkiye

[3]Selçuk Üniversitesi, Elektrik-Elektronik Mühendisliği Bölümü, 42030, Konya, Türkiye

mirhendise@gmail.com, **gamzeozteris@gmail.com**, **mceylan@selcuk.edu.tr**

ÖZET

Bu çalışmada, 24 bit RGB formatında 128×128 boyutlarında gizli ve 24 bit RGB formatında 512×512 boyutlarında taşıyıcı görüntüler kullanılarak bir filigranlama uygulaması gerçekleştirilmiştir. Çalışmada kullanılan gizli görüntülerin şifrelenmesinde, görüntü özellik tabanlı iki katmanlı şifreleme kullanılmıştır. Gizli görüntüler öncelikle kırmızı, yeşil ve mavi renk uzaylarına ayrılmıştır. Birinci katman şifrelemede; gizli görüntü renk uzayları, kendi görüntü özellikleri kullanılarak yer değiştirme algoritması ile şifrelenmiştir. Daha sonra gizli görüntü, renk uzaylarının görüntü boyutları yeniden düzenlenerek ikili (binary) formata dönüştürülmüştür. Bu görüntüler ikinci katman şifrelemede; taşıyıcı görüntü özellikleri kullanılarak şifrelenmiş ve taşıyıcı görüntünün kırmızı, yeşil ve mavi renk uzayına en önemsiz bit yöntemi ile filigranlanmıştır. Üç adet taşıyıcı görüntü ve iki adet gizli görüntü kullanılarak yapılan çalışmada görüntüler arasındaki değişimleri ölçmek amacıyla tepe sinyal gürültü oranından (TSGO) yararlanılmıştır. Çalışma sonucunda, 51,13 ile 51,91dB arasında değişen TSGO ile başarılı bir filigranlama gerçekleştirilmiştir. Bu makale, ISDFS 2015'de sunulmuş olup seçilerek bu dergide yayımlanmıştır.

Anahtar Kelimeler: Görüntü özellik tabanlı görüntü şifreleme; filigranlama; RGB taşıyıcı görüntü; RGB gizli görüntü; tepe sinyal gürültü oranı (TSGO)

COLOR COVER AND COLOR SECRET IMAGE BASED TWO-LAYER ENCRYPTION AND LSB BASEB WATERMARKING

ABSTRACT

In this study, a secret (128×128) and cover color image (512×512) (24 bit RGB) based watermarking application was developed. Image feature based on two-layered encoding was used in coding of secret image. Firstly, secret image separated to red, green and blue color space. In the first layer of encoding, secret image color spaces are coded by local change algorithm with individual image features. After that, secret images are transformed to binary image format by rearranging of color space image dimensions. In the second layer encoding, these images are coded using host image features and are watermarked to R, G and B spaces using least significant bit (LSB) method. This study is realized with three host images and two secret images and peak signal-to-noise ratio (PSNR) value is used in order to measure difference between the images. The results have shown that, the with the help of developed software, the watermarking and encryption tasks were successfully developed with 51,3–51,9 dB of PSNR values.

Keywords: Image feature based image encryption; watermarking; RGB host image; RGB secret image; peak signal-to-noise ratio (PSNR)

I. GİRİŞ (INTRODUCTION)

Görüntülerin filigranlanması konusu, 2000'li yıllardan itibaren üzerinde çok yoğun çalışılan bir görüntü işleme alanı haline gelmiştir. Filigranlama çalışmalarında; gizli mesaj veya bilgi içeren görüntüler, çeşitli teknikler kullanılarak taşıyıcı görüntülerle birleştirilmekte ve filigranlanmış yeni görüntüler elde edilmektedir. Filigranlama çalışmalarının birinci amacı taşıyıcı görüntülerde en az bozulma ile filigranlama yapılmasıdır.

Bu çalışmaların ikinci amacı ise filigranlama algoritması tersine işletildiğinde en yüksek doğruluk ile gizli görüntünün yeniden elde edilmesidir. Bu kapsamda filigranlanmış görüntüye; gürültü ekleme veya sıkıştırma gibi uygulamalar yapılması durumunda bile gizli görüntünün kabul edilebilir bir doğrulukla yeniden elde edilmesi istenilmektedir. Ayrıca gizli mesajın niteliğine göre; gizli görüntünün filigranlama yapılmadan önce şifrelenmesi, sık tercih edilen bir yöntemdir. Bu kapsamda; şifrelenecek görüntü özelliklerin şifreleme algoritmasına dahil edilmesi, her görüntü için kendine özgü şifreleme sonuçlarının üretilmesini sağladığı için şifreleme işlemini daha kaotik bir hale getirmektedir. Filigranlama çalışmalarının çeşitlenmesinde çalışmalarda kullanılan gizli ve taşıyıcı görüntülerin formatları etkili olmuştur. Bu kapsamda; literatür çalışmaları, beş başlık altında incelenebilir.

1. Gri-seviye taşıyıcı görüntüler ve binary gizli görüntüler kullanılan filigranlama çalışmaları.
2. Gri-seviye taşıyıcı görüntüler ve gri-seviye gizli görüntüler kullanılan filigranlama çalışmaları.
3. RGB taşıyıcı görüntüler ve binary gizli görüntüler kullanılan filigranlama çalışmaları.
4. RGB taşıyıcı görüntüler ve gri-seviye gizli görüntüler kullanılan filigranlama çalışmaları.
5. RGB taşıyıcı görüntüler ve RGB gizli görüntüler kullanılan filigranlama çalışmaları.

Bu gruplandırma başlıklarının sıralaması, filigranlama konusunda literatür çalışmalarının gelişimini de yansıtmaktadır. Bu gelişim sıralamasının oluşmasında, zaman içinde kullanılan görüntülerin siyah-beyaz görüntülerden renkli görüntülere doğru gelişim göstermesi önemli bir etkendir. Son yıllarda; RGB formatındaki taşıyıcı ve gizli görüntülerin kullanıldığı çok sayıda filigranlama çalışması gerçekleştirilmiştir. Yapılan çalışma sonuçlarının birbiri ile karşılaştırılmasında çalışmalarda kullanılan taşıyıcı ve gizli görüntüler ile görüntü boyutları önemlidir. Literatür çalışmalarında filigranlama konusunda ortak bir görüntü veritabanı oluşturulamamıştır. RGB formatındaki taşıyıcı ve gizli görüntülerin kullanıldığı çalışmalarda [1-16]; kullanılan filigranlama teknikleri, taşıyıcı görüntüler, taşıyıcı görüntü boyutları, gizli görüntü boyutları ve çalışma sonucunda elde edilen TSGO değerleri hakkındaki ayrıntılı bilgiler Tablo I'de verilmiştir. Bu çalışmalarda kullanılan görüntüler 24 bit derinliğine sahiptir. Ayrıca; Tablo I'de verilen çalışmalar haricinde, gizli görüntülerin daha düşük bit derinliği ile ifade edildiği filigranlama çalışmaları da [17] gerçekleştirilmiştir. Bununla birlikte; literatürde, taşıyıcı ve gizli görüntülerin bit derinliği, görüntü boyutları hakkında çalışma içinde herhangi bir bilgi yer almayan veya sonuçların değerlendirmesinde performans kriteri kullanılmayan çalışmalarda [18-24] mevcuttur.

II. YÖNTEMLER (METHODS)

2.1. Taşıyıcı ve Gizli Görüntüler

Bu çalışmada, 24 bit RGB formatında ve 512×512 boyutlarında üç adet taşıyıcı görüntü (Lena, Baboon ve Peppers) [25] ve 24 bit RGB formatında ve 128 × 128 boyutlarında iki adet gizli görüntü (ISDF2015 ve Selçuk Üniversitesi Logosu) kullanılmıştır. Çalışmada kullanılan resimler Şekil 1'de verilmiştir. Tablo I'de bu resimler incelendiğinde, bu çalışmada kullanılan taşıyıcı görüntülerin daha önce yapılan çalışmalarda da sıklıkla kullanıldığı görülmektedir.

2.2. Birinci Katman Şifreleme

Gerçekleştirilen filigranlama çalışmasında, ilk olarak gizli görüntülerin birinci katman şifrelenmesi gerçekleştirilmiştir. Bu kapsamda; gizli görüntüler kırmızı, yeşil ve mavi renk uzaylarına ayrılmıştır. 24 bit RGB görüntülerin renk uzaylarına ayrılması ile elde edilen görüntüler 8 bit derinliğinde gri-seviye görüntülerdir.

Şekil 1. a) Gizli Görüntü-1 (ISDFS-2015) b) Gizli Görüntü-2 (Selçuk Üniversitesi Logosu) c) Taşıyıcı Görüntü-1 (Lena) d) Taşıyıcı Görüntü-2 (Baboon) e) Taşıyıcı Görüntü-3 (Peppers)

Daha sonra, renk uzaylarına ayrılmış görüntüler tutulmuştur. Bu aşamada; daha önce Yaşar ve Ceylan [26] tarafından binary görüntülerin görüntü özellik tabanlı şifrelenmesinde kullanılan ve piksel yer değiştirme kategorisinde yer alan şifreleme algoritması gri-seviye görüntülere adapte edilerek kullanılmıştır. Çalışmada kullanılan bu algoritmada öncelikle; görüntülerin 1. satırlarındaki piksel değerleri sayısal olarak toplanmış ve bu toplamın satır boyutu modülüne göre eşdeğeri bulunmuştur. Daha sonra bu satır, kendi satırı için hesaplanan bu modüler eşdeğer kadar sola kaydırılmıştır. Sırasıyla bütün satırlar için aynı işlemin tamamlanmasının ardından sütunlarda aynı yöntemle yukarı yönlü olarak kaydırılmıştır. Bu şifreleme algoritması kısaca şu şekilde özetlenebilir.

1) M × N (Satır × Sütun) boyutundaki 8 bit gri-seviye görüntünün 1. satırındaki matris hücresi değerlerini topla.
2) Toplamın mod M'ye göre eşdeğerini hesapla.
3) Satırı, bu eşdeğer basamak kadar sola (satır başı satır sonundan devam eder kuralına uygun olarak) kaydır.
4) M adet satır için 1-3 nolu basamakları tekrarla.
5) M × N (Satır × Sütun) boyutundaki 8 bit gri-seviye görüntünün 1. sütunundaki matris hücresi değerlerini topla.
6) Toplamın mod N'ye göre eşdeğerini hesapla.
7) Sütunu, bu eşdeğer basamak kadar yukarı (sütun başı sütun sonundan devam eder kuralına uygun olarak) kaydır.
8) N adet sütun için 4-7 nolu basamakları tekrarla.

Şifreleme algoritması arka arkaya birden çok kez tekrarlanabilir. Şekil 2'de çalışmada kullanılan bir adet gizli görüntünün (ISDFS-2015) kırmızı, yeşil ve mavi renk uzay görüntüleri ve şifreleme algoritmasının 1, 5 ve 10 kez çalıştırılması ile elde edilen görüntüler verilmiştir. Şekil 2, şifreleme algoritmasının bir kez çalıştırılması durumunda bile ne kadar etkili olduğunu görsel olarak ortaya koymaktadır. Ayrıca çalışmanın *Sonuçlar* bölümünde sayısal bilgileri verilen, gizli görüntüler ve gizli görüntülerin birinci katman şifreleme ile şifrelenmiş halleri arasındaki TSGO değerleri de bu durumu destekler niteliktedir.

Çalışmada görüntülerin bu algoritmanın 10 kez işletilmesi ile elde edilen versiyonları kullanılmıştır. Ancak; gizli görüntülerin kırmızı, yeşil ve mavi renk uzaylarının algoritmanın farklı sayılarda işletilmesi ile elde edilen versiyonlarının birleşimi olarak ifade edilmesi de mümkündür.

2.4. İkinci Katman Şifreleme

Çalışmanın ilk aşaması olan birinci katman şifreleme ile, gizli görüntülerin kendi görüntü özellikleri birinci katman şifrelemeye tabi kullanılarak şifreleme gerçekleştirilmiştir. İkinci katman şifrelemede ise gizli görüntüler, filigranlamanın gerçekleştirileceği taşıyıcı görüntünün özellikleri kullanılarak şifrelenmektedir. Bu aşamada dikkat edilmesi gereken en önemli husus ikinci katman şifrelemede kullanılacak taşıyıcı görüntü özelliklerinin, işlemlerin tersine çevrilmesi sırasında herhangi bir sorun yaşanmaması için, filigranlanmış görüntüden bozulmadan elde edilebilmesidir. Bu filigranlama çalışmasında, yöntem olarak en anlamsız bitin değiştirilmesi kullanılmıştır. Bu sebeple, taşıyıcı ve filigranlanmış görüntülerin 0.5 eşikleme sabiti ile eşiklenmesi durumunda elde edilecek binary formatlı görüntüler aynı olacaktır. Bu noktadan hareketle; ikinci katman şifrelemede, taşıyıcı görüntünün kırmızı, yeşil ve mavi renk uzaylarının eşiklenmesi ile elde edilen binary formatlı eşiklenmiş görüntülere ait özelliklerden yararlanılmıştır. İkinci katman şifrelemede öncelikle, 24 bit RGB formatındaki taşıyıcı görüntüler kırmızı, yeşil ve mavi renk uzaylarına ayrılmıştır. Daha sonra bu görüntüler, 0.5 eşikleme sabiti ile eşiklenmiştir. Bu aşamada elde edilen görüntüler 512×512 boyutlarında olup binary formattadır. Çalışmada ikinci katman şifreleme Eşitlik (1) ile gerçekleştirilmiştir.

$$l(i,k)=\begin{cases} g(i,k), f(i,k)=2m+1, m\in\{0,1,2,.....\} \\ \overline{g(i,k)}, f(i,k)=2m, m\in\{0,1,2,.....\} \end{cases} \quad (1)$$

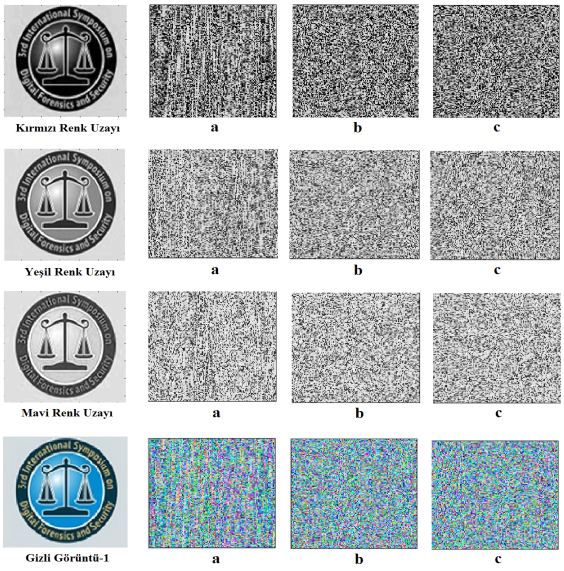
Eşitlik (1)'de, *f(i,k)*; taşıyıcı görüntü renk uzaylarının eşiklenmesi ile elde edilen binary görüntü matrisini, *g(i,k)*; birinci katman şifrelemesi yapılmış ve binary formata dönüştürülmüş gizli görüntü matrisini, *l(i,k)*; ikinci katman şifreleme sonuç matrisini ifade etmektedir. Bu aşamada; taşıyıcı görüntünün sırasıyla kırmızı, yeşil ve mavi renk uzayının eşiklenmesi ile elde edilen görüntüler, birinci katman şifrelemesi yapılmış ve binary formata dönüştürülmüş gizli görüntülerin kırmızı, yeşil ve mavi renk uzaylarının ikinci katman şifrelenmesinde kullanılmıştır. Eşitlik (1)'e göre, matrisler üzerinde aynı koordinatlar için eşiklenmiş taşıyıcı görüntü matris değeri tek ise gizli görüntü değeri aynen korunarak sonuç matrisine atanırken, çift ise gizli görüntü değerinin tersi alınarak sonuç matrisine atanmaktadır. Bu bağıl şifreleme çok daha karmaşık biçimlerde de gerçekleştirilebilir.

2.3. RGB Gizli Görüntülerin Binary Formata Çevrilmesi

2011 yılında Al-Gindy ve arkadaşları [9] tarafından, RGB gizli görüntülere ait piksel değerlerinin 10'luk taban yerine binary (ikili) formatta ifade edilmesi ve elde edilen binary sayıların bazı önemli bitleri kullanılarak filigranlama yapılmasına yönelik bir çalışma gerçekleştirilmiştir.

TABLO I. LİTERATÜR ÇALIŞMALARINA AİT BİLGİLER

Çalışma ve Çalışma Yılı	Metot	Taşıyıcı Görüntü	Taşıyıcı Görüntü Boyutları (RGB)	Gizli Görüntü Boyutları (RGB)	TSGO (dB)
Xing ve Tan [1] Yıl: 2007	Tekil değer ayrışımı ve Arnold dönüşümü	Lena	512 × 512	64 × 64	33.4874
Amir ve ark. [2] Yıl: 2007	Bağımsız bileşen analizi	Lena	512 × 512	120 × 120	----
Zhong ve ark. [3] Yıl: 2008	Lorenz kaotik şifreleme ve Arnold dönüşümü	Lena	512 × 512	52 × 52	----
Yong ve ark. [4] Yıl: 2009	Ayrık kosinüs dönüşümü ve kör filigranlama algoritması	Lena	512 × 512	64 × 64 64 × 64	41,0354 41,2335
Zhong ve Zhu [5] Yıl: 2009	Ayrık kosinüs dönüşümü ve çok katmanlı Arnold dönüşümü	Baboon	512 × 512	64 × 64	----
Golea ve ark. [6] Yıl: 2010	Tekil değer ayrışımı	Lena, House vb. (11 görüntü)	512 × 512	8 × 8 16 × 16 32 × 32	32,5755-35,9606 33,0856-44,2581 42,9759-52,7325
Basu ve ark. [7] Yıl: 2010	Bit düzlem indeksi modülasyonu ve bit değişimi	Palms, Animal vb. (11 görüntü)	256 × 256	----	32,018-46,726
Wei ve Weijiang [8] Yıl: 2010	Dörtlü hızlı Fourier dönüşümü ve ayrık kosinüs dönüşümü	Lena	512 × 512	32 × 32	43,2602
Al-Gindy ve ark. [9] Yıl: 2011	Gizli görüntülerin RGB'den binary tipe dönüştürülmesi ve ayrık kosinüs dönüşümü	Lena, Pepper ve Baboon	512 × 512	32 × 32	37,144-42,087
Golea ve ark. [10] Yıl: 2011	Tekil değer ayrışımı ve genetik optimizasyon algoritması	Lena ve House	512 × 512	----	33,9333-38,9288 38,6803-40,8365
Su ve ark. [11] Yıl: 2012	Tam sayılı dalgacık dönüşümü	Lena, Pepper, Baboon ve Plane	512 × 512	64 × 64	55,8415-55,8774
Bedwal ve Kumar [12] Yıl: 2013	RGB haritalama ve bit değişimi	Lena, Pepper ve Baboon	256 × 256 512 × 512	128 × 128 256 × 256	40,92-41,10 40,88-41,12
Su ve ark. [13] Yıl: 2013	İki seviyeli ayrık kosinüs dönüşümü	Lena, Pepper, Baboon ve Plane	512 × 512	64 × 64	34,0312-34,9512
Gupta ve ark. [14] Yıl: 2014	Yüksek değerli bit değişimi	Lena, Pepper, Baboon ve Jet	512 × 512	64 × 64 180 × 180	42,4312-51,4612
Pradhan ve ark. [15] Yıl: 2014	Ayrık kosinüs dönüşümü ve iki boyutlu Arnold haritalama	Barbara	512 × 512	64 × 64	41,09-45,15
Chen ve ark. [16] Yıl: 2014	Dörtlü hızlı Fourier dönüşümü	Lena, Baboon vb. (10 görüntü)	512 × 512	32 × 32	37,255-37,679



Şekil 2. Şifreleme Algoritmasının İşletilmesi Sonucu Oluşan Görüntü a) 1 Kez b) 5 Kez c) 10 Kez

Gerçekleştirilen filigranlama çalışmasının ikinci aşamasında; bu temel fikir üzerinden hareket edilerek RGB gizli görüntülerin, görüntü boyutları değiştirilmiş ve binary formata dönüştürülmüştür. Binary formatlı sayılarda sırasıyla bitler, kendinden sonraki bitlerin toplamı kadar bilgi taşır. Örneğin; 8 bitlik bir sayıda birinci en anlamlı bit bilginin % 50'sini, ikinci en anlamlı bit bilginin % 25'ini, üçüncü en anlamlı bit %12,5'ini taşır. Bunun bir diğer anlamı, 8 bitlik bir sayıda bilginin %87,5'lik kısmının ilk üç en anlamlı bit ile, kalan %12,5'lik kısmının ise kalan beş bit ile taşındığıdır. Bu sebeple, önemli bitlerin saklanması (ilk üç bit) diğer bitlerin saklanmasından daha önemlidir. Bu noktadan hareketle, bu çalışmada birinci en anlamlı bitler 5'er kez, ikinci ve üçüncü en anlamlı bitler 3'er kez, diğer bitler ise 1'er kez tekrarlanarak dönüştürme gerçekleştirilmiştir. Bu tekrarlama sayıları keyfi olarak seçilmiş olup bu sayıların farklı kullanılması da mümkündür. RGB formatlı görüntülerin kırmızı, yeşil ve mavi uzayları; birinci katman şifrelemeden sonra, görüntü boyutları değiştirilerek binary formata dönüştürülmüştür. Şekil 3, bu işlemi anlatmaktadır. Bu işlem sonunda; 128×128 boyutlarındaki görüntülerin yeni boyutları, 512×512 olarak düzenlenmiştir. Boyutların yeniden düzenlenmesi sırasında, RGB gizli görüntülere ait verilerde herhangi bir kayıp yaşanmamıştır.

2.5. Filigranlama

Gizli görüntünün filtreleme, kesme ve gürültü ekleme gibi saldırılara karşı kalıcılığına göre filigranlama yöntemleri; dayanıklı, kırılgan ve yarı-kırılgan olmak üzere üç gurupta incelenebilir [27]. Kırılgan filigranlamada; filigranlanmış görüntüye basit bir işlem uygulandığında gizli görüntü kolaylıkla yok olmakta veya bozulmaktadır. Kırılgan filigranlama genellikle veri doğrulama amacıyla kullanılmaktadır [27]. Kırılgan filigranlama çalışmalarında taşıyıcı görüntüye ait piksel değerlerinin değiştirilmesi sıklıkla kullanılan bir yöntemdir. Bu çalışmada, şifrelenmiş ve binary formata dönüştürülmüş gizli görüntünün kırmızı, yeşil ve mavi renk uzayları, sırasıyla taşıyıcı görüntünün kırmızı, yeşil ve mavi renk uzaylarına en önemsiz bitin değiştirilmesi yöntemi kullanılarak filigranlanmıştır.

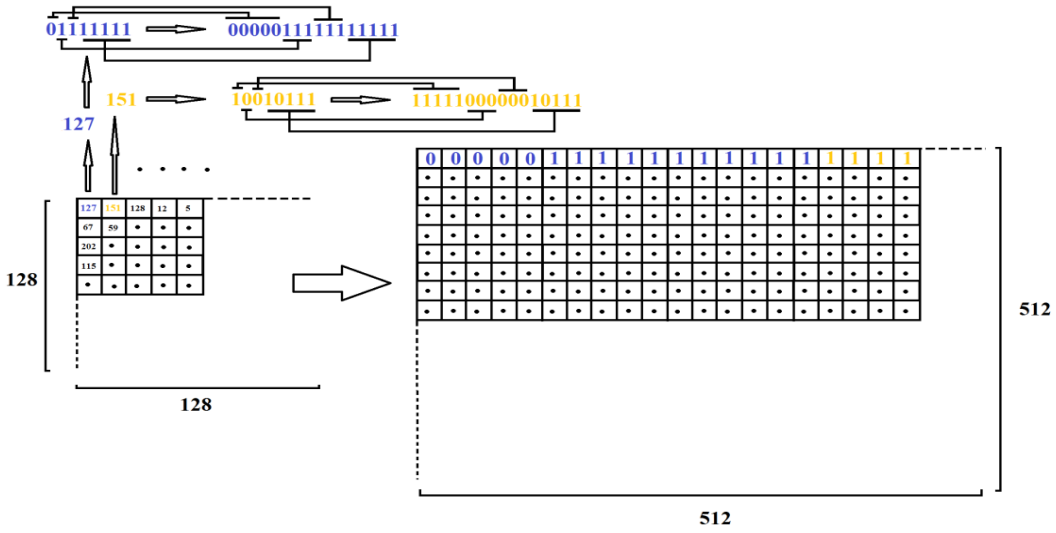
2.6. Sonuçların Değerlendirilmesinde Kullanılan Performans Kriterleri

Gri-seviye formatında ve M×N boyutlarında *f* referans görüntüsü ve *g* test görüntüsü olmak üzere iki görüntü arasındaki karesel ortalama hata (KOH), Eşitlik (2) ile hesaplanır.

$$KOH(f,g)=\frac{1}{MN}.\sum_{i=1}^{M}\sum_{j=1}^{N}(f_{i,j}-g_{i,j})^2 \qquad (2)$$

RGB formatında ki görüntüler kırmızı, yeşil ve mavi olmak üzere üç renk uzayına sahiptir. İki RGB görüntü arasındaki KOH hesaplanırken her renk uzayı Eşitlik (2) kullanılarak kendi arasında değerlendirilir ve elde edilen KOH değerleri toplanarak 3'e bölünür. 24 bit iki RGB görüntü arasındaki tepe sinyal gürültü oranı (TSGO) ise Eşitlik (3) ile hesaplanır. Eşitlik (3)'den de anlaşılacağı üzere KOH değeri sıfıra yaklaşırken TSGO sonsuza yaklaşır. Bu durum test görüntüsü ile referans görüntünün maksimum derecede örtüştüğünü gösterir.

$$TSGO=10.\log_{10}\left(\frac{255^2}{(KOH(K)+KOH(Y)+KOH(M))/3}\right) \qquad (3)$$



Şekil 3. 128×128 Boyutlarındaki Gizli Görüntünün Kırmızı, Yeşil Ve Mavi Renk Uzaylarının Görüntü Boyutları Değiştirilerek 512×512 Boyutlarında Binary Formatlı Görüntüye Dönüştürülmesi

Bu çalışmada, RGB taşıyıcı görüntüler ile filigranlanmış görüntülerin karşılaştırılmasında ve RGB gizli görüntüler ile birinci katman şifreleme ile şifrelenmiş görüntülerin karşılaştırılmasında TSGO kullanılmıştır.

III. DENEYLER VE SONUÇLAR (EXPERIMENTS AND RESULTS)

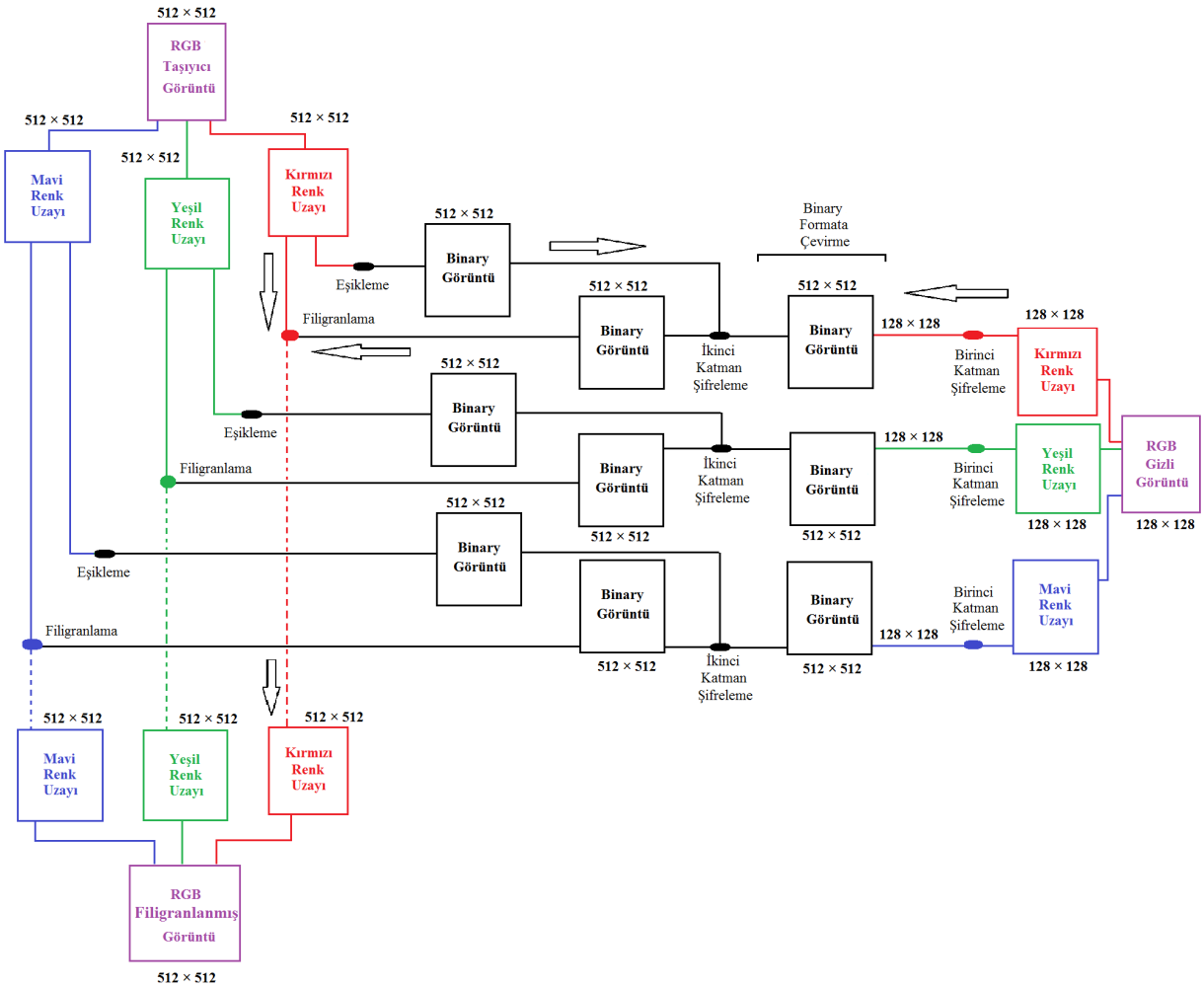
3.1. Deneyler

Gerçekleştirilen filigranlama çalışmasında öncelikli olarak 128×128 boyutlu 24 bit RGB formatlı gizli görüntülerin kırmızı, yeşil ve mavi renk uzaylarına 10 kez birinci katman şifreleme algoritması uygulanmıştır. Elde edilen şifrelenmiş 8 bit gri-seviye gizli görüntü renk uzaylarının görüntü boyutları yeniden düzenlenerek, görüntüler 512×512 boyutlu binary formatlı görüntülere dönüştürülmüştür. Bu aşamadan sonra 512×512 boyutlu 24 bit RGB formatlı taşıyıcı görüntüler renk uzaylarına ayrılmıştır. Elde edilen her bir renk uzayı 0.5 eşikleme sabiti için eşiklenmiştir.

Elde edilen binary görüntüler gizli görüntülerin ikinci katman şifrelenmesinde kullanılmıştır. Çalışmanın son aşamasında gizli görüntülerin kırmızı, yeşil ve mavi renk uzayı karşılığı binary görüntüler sırasıyla taşıyıcı görüntülerin kırmızı, yeşil ve mavi renk uzaylarına en önemsiz bitin değiştirilmesi yöntemi kullanılarak filigranlanmıştır. Sistemin genel çalışmasını anlatan blok diyagram Şekil 4'de verilmiştir. Şekil 4'de blok diyagramı verilen algoritma tersine işletildiğinde filigranlanmış görüntülerden gizli görüntüler tam doğrulukla yeniden elde edilebilmektedir.

3.2. Sonuçlar

Çalışmada, 24 bit RGB formatında ve 512×512 boyutlarında üç adet taşıyıcı görüntü (Lena, Baboon ve Peppers) ve 24 bit RGB ve 128×128 boyutlarında iki adet gizli görüntü (ISDFS-2015 ve Selçuk Üniversitesi Logosu) kullanılmıştır. Gizli görüntülerin, birinci katman şifreleme algoritmasının 1, 5 ve 10 kez işletilmesiyle şifrelenmiş halleri ve orijinal hallerinin karşılaştırılması sonucu elde edilen TSGO değerleri Tablo II'de verilmiştir.



Şekil 4. Filigranlama Algoritması Blok Diyagramı

Bir adet taşıyıcı görüntü (Lena) ve iki adet gizli görüntü için çalışma sonucunda elde filigranlanmış görüntüler Şekil 5'de görülmektedir. Bütün taşıyıcı ve gizli görüntüler kullanılarak çalışmada elde edilen filigranlanmış görüntüler ve orijinal taşıyıcı görüntüler arasındaki TSGO değerleri ise Tablo III'de verilmiştir. Çalışmada, filigranlama işlemi tersine işletildiği zaman gizli görüntüler tam doğrulukla yeniden elde edilmiştir.

TABLO II. BİRİNCİ KATMAN ŞİFRELEME ALGORİTMASI İLE ŞİFRELENMİŞ GİZLİ GÖRÜNTÜLERE AİT TSGO SONUÇLARI

Gizli Görüntüler	Algoritmanın Tekrarlanma Sayısı		
	1	5	10
ISDFS2015	7,56 dB	7,62 dB	7,61 dB
Selçuk Ü. Logosu	9,80 dB	9,77 dB	9,77 dB

TABLO III. FİLİGRANLANMIŞ GÖRÜNTÜLERE AİT TSGO SONUÇLARI

Gizli Görüntüler	Taşıyıcı Görüntüler		
	Lena	Baboon	Peppers
ISDFS2015	51,47 dB	51,21 dB	51,91 dB
Selçuk Ü. Logosu	51,73 dB	51,41 dB	51,13 dB

IV. TARTIŞMA (DISCUSSION)

Bu çalışmanın birinci katman şifreleme aşamasında, daha önce Yaşar ve Ceylan [26] tarafından binary gizli görüntülerin şifrelenmesinde kullanılan ve piksel yer değiştirme kategorisinde yer alan şifreleme algoritması RGB görüntülere adapte edilerek kullanılmıştır. Şifreleme algoritmasının bir kez çalıştırılması durumunda bile ne kadar etkili olduğunu gösteren bulgular Şekil 2'de verilmiştir. Ayrıca Tablo II'de verilen TSGO sonuçları da bu durumu destekler niteliktedir. Bu çalışma ile ortaya konan iki katmanlı şifreleme yapısı hem gizli görüntü hem de taşıyıcı görüntü özelliklerini kullanarak şifreleme yapması sebebiyle her gizli ve taşıyıcı görüntü için farklı sonuçlar üretmektedir. Bu durum statik şifreleme matrisleri veya standart yer değiştirme permütasyonları kullanılarak yapılan şifrelemelere göre şifreleme işleminin güvenliğini üst düzey bir noktaya taşımaktadır.

Bu filigranlama çalışması ile elde edilen ve Tablo III'de verilen filigranlama sonuçları, Tablo I'de ayrıntılı sonuçları verilen literatür çalışmaları ile karşılaştırıldığında etkili bir filigranlama çalışması gerçekleştirildiği görülmektedir. Çalışma sonuçları, sadece Golea ve ark. [6] ile Su ve ark. [11] tarafından gerçekleştirilen çalışmalarda elde edilen sonuçların gerisinde kalmıştır. Ancak bu literatür çalışmalarında [6, 11] kullanılan gizli görüntü boyutları (32×32 ve

Şekil 5. Filigranlanmış Görüntü Örnekleri

64×64), bu çalışmada kullanılan gizli görüntü boyutlarından (128×128) daha küçüktür. Bu çalışmalar ile tam bir karşılaştırma yapmak amacıyla çalışmada gizli görüntülerin bu boyutlarda (32×32 ve 64×64) kullanılması durumunda elde edilecek TSGO sonuçları hesaplanmıştır. Gizli görüntülerin 64×64 boyutlarında kullanılması durumunda 56,96 dB ile 57,61dB arasında, 32×32 boyutlarında kullanılması durumunda 62,59dB ile 63,21dB arasında değişen TSGO değerleri ile filigranlanma gerçekleştirilmektedir. Bu sonuçlar Golea ve ark. [6] ile Su ve ark. [11] tarafından gerçekleştirilen çalışmalarda elde edilen sonuçlardan daha yüksektir.

SEMBOLLER VE KISALTMALAR

f(i,k)	Taşıyıcı görüntü renk uzaylarının eşiklenmesi ile elde edilen binary görüntü matrisi
g(i,k)	Birinci katman şifrelemesi yapılmış ve binary formata dönüştürülmüş gizli görüntü matrisi
l(i,k)	İkinci katman şifreleme sonuç matrisi
f	KOH referans görüntüsü
g	KOH test görüntüsü
M	Görüntü satır uzunluğu
N	Görüntü sütun uzunluğu
TSGO	Tepe Sinyal Gürültü Oranı
KOH	Karasel ortalama Hata
PSNR	Peak Signal-to-Noise Ratio
LSB	Least Significant Bit

V. KAYNAKLAR (REFERENCES)

[1]. Xing, Y. ve Tan, J., "A color watermarking scheme based on Block-SVD and Arnold transformation", **Workshop on Digital Media and its Application in Museum & Heritage**, Çongçing, Çin, 3-8, 10-12 Aralık 2007.

[2]. Amir, M., Adib, A. ve Aboutajdine, D., "Color images watermarking by means of independent component analysis", **Int. Conf. on Electronics, Circuits and Systems**, Marakeş, Fas, 347-350, 11-14 Aralık 2007.

[3]. Zhong, Q., Zhu, Q. ve Zhang, P., "A spatial domain color watermarking scheme based on chaos", **Int. Conf. on Apperceiving Computing and Intelligence Analysis**, Çengdu, Çin, 137-142, 13-15 Aralık 2008.

[4]. Yong, Z., Li-Cai, L., Qi-Shen, L. ve Ze-Tao, J., "A blind watermarking algorithm based on block DCT for dual color images", **Int. Symp. on Electronic Commerce and Security**, Nanchang, Çin, 213-217, 22-24 Mayıs 2009.

[5]. Zhong, Q. ve Zhu, Q., "A DCT domain color watermarking scheme based on chaos and multilayer Arnold transformation", **Int. Conf. on Networking and Digital Society**, Cilt 2, Guiyang, Çin, 209-212, 30-31 Mayıs 2009.

[6]. Goléa, N. E., Seghir, R. ve Benzid, R., "A bind RGB color image watermarking based on singular value decomposition", **Int. Conf. on Computer Systems and Applications**, Hammamet, Tunus, 1-5, 16-19 Mayıs 2010.

[7]. Basu, D., Sinharay, A. ve Barat, S., "Bit plane index based fragile watermarking scheme for authenticating color image", **Int. Conf. on Integrated Intelligent Computing, Bangalore**, Hindistan, 136-139, 5-7 Ağustos 2010.

[8]. Wei, Z. ve Weijiang, W., "Color watermarking algorithm based on modified QFFT and DCT", **Int. Conf. on Optoelectronics and Image Processing**, Cilt 1, Haiko, Hindistan, 328-331, 11-12 Kasım 2010.

[9]. AI-Gindy, A., Younes, H., Shaheen, A. ve Elsadi, H., "A graphical user interface watermarking technique for the copyright protection of colour images using colour watermarks", **Int. Symp. on Signal Processing and Information Technology**, Bilbao, İspanya, 354-358, 14-17 Aralık 2011.

[10]. Goléa, N. E., Melkemi, K. E. ve Melkemi, M, "A novel multi-objective genetic algorithm optimization for blind RGB color ımage watermarking", **Int. Conf. on Signal-Image Technology and Internet-Based Systems**, Dijoni, Fransa, 306-313, 28 Kasım-1 Aralık 2011.

[11]. Su, Q., Niu, Y., Liu, X. ve Zhu, Y., "A blind dual color images watermarking based on IWT and state coding", **Optics Communications**, Cilt 285, 1717-1724, 2012.

[12]. Bedwal, T. ve Kumar, M., "An enhanced and secure ımage steganographic technique using RGB-Box mapping", **Confluence 2013: The Next Generation Information Technology Summit (4th Int. Conf.)**, Noida, Hindistan, 385-393, 26-27 Eylül 2013.

[13]. Su, Q., Niu, Y., Liu, X. ve Yao, T., "A novel blind digital watermarking algorithm for embedding color image into color image", **Optik**, Cilt 124, 3254-3259, 2013.

[14]. Gupta, P. K., Roy, R. ve Changder, S., "A secure image steganography technique with moderately higher significant bit embedding", **Int. Conf. on Computer Communication and Informatics**, Coimbatore, Hindistan, 1-6, 3-5 Ocak 2014.

[15]. Pradhan, C., Saha, B. J., Kabi, K. K., Arun ve Bisoi, A. K., "Blind watermarking techniques using DCT and Arnold 2D cat map for color images", **Int. Conf. on Communications and Signal Processing**, Melmaruvathur, Hindistan, 26-30, 3-5 Nisan 2014.

[16]. Chen, B., Coatrieux, G., Chen, G., Sun, X., J. L. Coatrieux, J. L. ve Shu, H., "Full 4D quaternion discrete Fourier transform based watermarking for color images", **Digital Signal Processing**, Cilt 28, 106-119, 2014.

[17]. Kunhu, A. ve Al-Ahmad, H., "A new watermarking algorithm for color satellite images using color logos and hash functions", **Int. Conf. on Computational Intelligence, Communication Systems and Networks**, Madrid, İspanya, 251-255, 5-7 Haziran 2013.

[18]. Benhocine, A., Laouamer, L., Nana, L. ve Pascu, A., "A new approach against color attacks of watermarked images", **Int. Conf. on Intelligent Information Hiding and Multimedia Signal Processing**, Harbin, Çin, 969-972, 15-17 Ağustos 2008.

[19]. Li, C. ve Li, Y., "Random index modulation based fragile watermarking scheme for authenticating colour images", **Int. Conf. on Intelligent Information Hiding and Multimedia Signal Processing**, Harbin, Çin, 16-19, 15-17 Ağustos 2008.

[20]. Jadhav, S. D. ve Bhalchandra, A. S., "Digital color image watermarking by means of blind source separation", **Int. Conf. on Control, Automation, Communication and Energy Conservation**, Perundurai, Hindistan, 1-4, 4-6 Haziran 2009.

[21]. Masud Karim, S. M., Rahman, M. S. ve Hossain, M. I., "A new approach for LSB based image steganography using secret key", **Int. Conf. on Computer and Information Technology**, Dakka, Bangladeş, 286-291, 22-24 Aralık 2011.

[22]. Dagar, S., "RGB based dual key image steganography", **Confluence 2013: The Next Generation Information Technology Summit (4th Int. Conf.)**, Noida, Hindistan, 316-320, 26-27 Eylül 2013.

[23]. Bairagi, A. K., Mondal, S. ve Debnath, R., "A robust RGB channel based image steganography technique using a secret key", **Int. Conf. on Computer and Information Technology**, Khulna, Bangladeş, 81-87, 8-10 Mart 2014.

[24]. Ghosal, S. K. ve Mandal, J. K., "Binomial transform based fragile watermarking for

image authentication", **Journal of Information Security and Applications**, Cilt 19, 272-281, 2014.

[25]. http://homepages.cae.wisc.edu/~ece533/images/ (Erişim Tarihi: 25.02.2015).

[26]. Yaşar, H. ve Ceylan, M., "RGB görüntülerin bit değişimi ve ripplet-I dönüşümü tabanlı şifreleme ile filigranlanması", **Uluslararası Bilgi Güvenliği ve Kriptoloji Konferansı**, İstanbul, Türkiye, 49-54, 17-18 Ekim 2014.

[27]. Lee, S. J. ve Jung, S. H., "A survey of watermarking techniques applied to multimedia", **Int. Symp. on Industrial Electronics**, Cilt 1, Busan, Güney Kore, 272-277, 12-16 Haziran 2001.