Journal of the Faculty of Engineering and Architecture of Gazi University 34:3 (2019) 1539-1548

Mühendislik Mimarlık Fakültesi Dergisi
Journal of The Faculty of Engineering and Architecture of Gazi University

Elektronik / Online ISSN : 1304 - 4915
Basılı / Printed ISSN : 1300 - 1884

Detection of copy move forgery based on color SURF

Gül Muzaffer* Güzin Ulutaş
Karadeniz Technical University, Faculty of Engineering, Department of Computer Engineering, Trabzon, 61000, Turkey

Highlights:

- Keypoint based copy move forgery detection method in digital images is proposed
- The method is robust to Gaussian blurring, noise addition and rotation attacks.
- The proposed method has higher classification ratios compared to the reference studies.

Keywords:

- Digital image authentication
- Copy move forgery
- SURF

Article Info:

Research Article
Received: 26.07.2016
Accepted: 16.10.2018

DOI:

10.17341/gazimmfd.570422

Correspondence:

Author: Gül Muzaffer
e-mail: gulmuzaffer@ktu.edu.tr
phone: +90 462 377 3256

Graphical/Tabular Abstract

Today the accuracy and reliability of digital images used in many important areas have great importance. One of the most common ways of forgery type that passive methods of digital image authentication techniques deals is copy move forgery. The ease of doing copy move forgery makes it to be seen widely. In this study especially for the color images the more effective copy move forgery detection technique is proposed. The efficiency of this method is reported by making comparison with the SURF-based method that exists in the literature. In addition to this, the proposed method can detect forged images even under rotation, Gauss blurring and noise addition attacks.

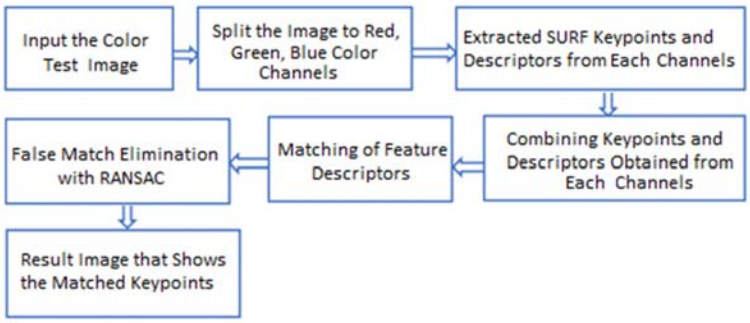


Figure A. Block diagram of the proposed method

Purpose:
The aim of this study is to propose a new robust copy move forgery detection method. The method can be integrated to real time applications due to the using keypoint based approach with higher performance on color images.

Theory and Methods:
SURF based copy move forgery detection method [17] is fail to detect forgeries in case of insufficient number of key points are extracted. To overcome this problem and on color images, efficient than [17] forgery detection method is proposed. The method firstly split input image into RGB color channels. SURF keypoints and feature descriptor vectors obtained from each color channel, then they are combined. To reveal forged regions, the combined descriptors are matched each other. After that, possible false matches are eliminated by using RANSAC algorithm. The experimental results, show that the proposed method has higher performance even under AWGN addition, Gauss blurring and rotation attacks.

Results:
The proposed method is compared with the SURF based [17] and ORB based [18] methods, the results are given two subsection. Firstly the method is compared with [17] using Detection Ratio (DR) metric and average execution time results are reported. It is also some visual results are given in first section. According to these reports the proposed method has higher performance than [17] with little time loss. Secondly the method are compared with [17] and [18] also with using Precision and Recall metrics. It is proven that the method is efficient than them.

Conclusion:
In this study, a new copy move forgery detection method which is more effective in color images is proposed. In the suggested scheme, extraction of the SURF keypoints from each RGB color channels of the forged image provided the advantage of the method.

Journal of the Faculty of Engineering and Architecture of Gazi University 34:3 (2019) 1539-1548

Mühendislik Mimarlık Fakültesi Dergisi
Journal of The Faculty of Engineering and Architecture of Gazi University

Elektronik / Online ISSN : 1304 - 4915
Basılı / Printed ISSN : 1300 - 1884

Renkli SURF tabanlı kopyala yapıştır sahteciliği tespiti

Gül Muzaffer*, Güzin Ulutaş
Karadeniz Teknik Üniversitesi, Bilgisayar Mühendisliği Bölümü, Trabzon, 61080, Türkiye

ÖNEÇIKANLAR

- Sayısal görüntülerde anahtar noktası tabanlı kopyala yapıştır sahteciliği tespiti yöntemi önerilmiştir.
- Yöntem, Gauss bulanıklaştırma, gürültü ekleme ve dönme ataklarına karşı dayanıklıdır.
- Geliştirilen yöntem, referans çalışmalara göre üstün sınıflandırma performansına sahiptir.

Makale Bilgileri
Araştırma Makalesi
Geliş: 26.07.2016
Kabul: 16.10.2018

DOI:
10.17341/gazimmfd.570422

Anahtar Kelimeler:
Sayısal görüntü doğrulama, kopyala yapıştır sahteciliği, SURF

ÖZET

Günümüzde birçok önemli alanda kullanılan sayısal görüntülerin doğruluğu ve güvenilirliği büyük önem arz etmektedir. Sayısal görüntü doğrulama yöntemlerinden pasif yöntemlerin ele aldığı en yaygın sahtecilik türlerinden birisi kopyala yapıştır sahteciliğidir. Kopyala yapıştır sahteciliğinin gerçekleştirilme kolaylığı, bu tür sahteciliğin yaygın bir şekilde görülebilmesine neden olmuştur. Yapılan çalışmada özellikle renkli görüntülerde daha etkin sonuç elde etmek amaçlı bir kopyala yapıştır sahteciliği tespiti yöntemi önerilmiştir. Yöntemin literatürde var olan SURF tabanlı yöntem ile karşılaştırılması yapılarak etkinliği rapor edilmiştir. Bununla birlikte önerilen yöntem ile dönme, Gauss bulanıklaştırma ve gürültü ekleme ataklarına maruz kalmış sahte görüntülerin tespiti de etkin bir şekilde gerçekleştirilebilmektedir.

Detection of copy move forgery based on color SURF

HIGHLIGHTS

- Keypoint based copy move forgery detection method in digital images is proposed
- The method is robust to Gaussian blurring, noise addition and rotation attacks
- The proposed method has higher classification ratios compared to the reference studies

Article Info
Research Article
Received: 26.07.2016
Accepted: 16.10.2018

DOI:
10.17341/gazimmfd.570422

Keywords:
Digital image authentication, copy move forgery, SURF

ABSTRACT

Today the accuracy and reliability of digital images used in many important areas have great importance. One of the most common ways of forgery type that passive methods of digital image authentication techniques deals is copy move forgery. The ease of doing copy move forgery makes it to be seen widely. In this study especially for the color images the more effective copy move forgery detection technique is proposed. The efficiency of this method is reported by making comparison with the SURF-based method that exists in the literature. In addition to this, the proposed method can detect forged images even under rotation, Gauss blurring and noise addition attacks.

*Sorumlu Yazar/Corresponding Author: gulmuzaffer@ktu.edu.tr, guzin@ieee.org / Tel: +90 462 377 3256

1. GİRİŞ (INTRODUCTION)

İnternet kullanımının giderek artması ve görüntü yakalama cihazlarının maliyetindeki düşüşün sonucu olarak sayısal görüntülerin oluşturulması, erişilebilirliği ve iletiminde hızlı bir artış gözlemlenmektedir. Tıp, gazetecilik, hukuk gibi birçok alanda da sayısal görüntülerin kullanımı yaygınlaşmaktadır. Photoshop, GIMP, Corel Draw gibi görüntü düzenleme yazılımlıları ile birlikte sıradan bir insanın bile, tespiti zor olan görüntü sahteciliği yapabilmesi, kullanımı yaygınlaşan görüntülerin doğruluğunu sorgulanır hale getirmiştir.

Görüntü sahteciliğinin tarihi, 1840'lı yıllarda Hippolyte adlı kişinin intihara teşebbüs ettiğini gösteren Şekil 1'de verilen sahte görüntünün üretilmesiyle başlamıştır. Bu kişi aslında 1839 yılında Daguerre ve Talbot tarafından ileri sürülen bir görüntü değiştirme yöntemini önermiş olup kendisinden önce yöntemin başkalarınca önerilmesi durumunu protesto etmek amacıyla bu şekilde önceden elde edemediği popülariteyi kazanmayı amaçlamıştır [1].

Şekil 1. İlk sahte görüntü (First forged image)

Sayısal görüntü güvenilirliğini kontrol etmek amacıyla literatürde birçok görüntü doğrulama yöntemi önerilmiştir. Genel olarak bu yöntemler aktif ve pasif doğrulama yöntemleri olmak üzere iki ana kategoride değerlendirilmektedir [2]. Aktif yöntemler kendi içerisinde sayısal damgalama ve sayısal imzalama olmak üzere iki alt kategoriye ayrılmaktadır. Damga veya imza bilgisinin görüntü oluşturulurken görüntünün içerisine yerleştirilmesi işleminin özel donanımlı kameralar veya sonradan yetkili yazılımlarca yapılmasına ihtiyaç duyulması, bu yöntemin dezavantajı olarak ortaya çıkmaktadır. Ayrıca internet ortamında damga veya imza bilgisi içermeyen resimlerin varlığı, aktif yöntemlerin bu görüntülerin doğrulanması amacıyla kullanımını imkânsız hale getirmektedir.

Pasif görüntü doğrulama yöntemlerinde, görüntünün doğrulanması işleminde görüntüden elde edilen istatistiksel özellikler kullanılarak görüntü doğrulaması gerçekleştirilmekte ve görüntü haricinde herhangi bir ek bilgiye ihtiyaç duyulmamaktadır [3]. İlgili yöntemlerin görüntü doğrulama işlemi için ek bir bilgiye ihtiyaç duymaması son zamanlarda araştırmacıların dikkatini bu yöne çekmiştir. Pasif görüntü doğrulama, görüntü birleştirme sahteciliği tespiti ve kopyala yapıştır sahteciliği tespiti olmak üzere iki alt kategoriye ayrılmaktadır. Görüntü birleştirme sahteciliği, farklı görüntülerden elde edilen görüntü parçalarının birleştirilmesiyle yapılan sahtecilik türüdür [4].

Pasif yöntemlerin tespit etmeye çalıştığı en popüler görüntü sahteciliği yöntemi, kopyala yapıştır sahteciliğidir [5]. Bu sahtecilik yönteminde görüntülenmesi istenmeyen nesnelerin gizlenmesi veya nesnelerin çoğaltılması amacıyla, belirli bir o bölgenin kopyalanarak aynı görüntüye yapıştırılmasıyla gerçekleştirilir. Şekil 2'de kopyala yapıştır sahteciliğine dair bir örnek verilmiştir.

Şekil 2. a) Orijinal görüntü b) Sahte görüntü
(a) Original image b) Forged image)

Kopyala yapıştır sahteciliği uygulanmış görüntünün yapısal analizi gerçekleştirildiğinde kopyalanıp yapıştırılan bölgeler arasında yüksek oranda benzerlik gözlemlenmektedir. Bu fikirden yola çıkarak kopyala yapıştır sahteciliğinin tespitine ilişkin ilk çalışma 2003 yılında gerçekleştirilmiştir [6]. Bu çalışmada görüntü 8x8 büyüklüğündeki karesel bloklara ayrılmış ve oluşturulan her bir bloğa Ayrık Kosinüs Dönüşümü (AKD) uygulanması ile özellik vektörleri elde edilmiştir. Bloklardan üretilen özellik vektörlerinin leksikografik olarak sıralanmasının ardından, komşu vektörlerin birbirlerine olan benzerliğinin Öklid uzaklığı ile hesaplanmasıyla benzer özelliğe sahip bloklar belirlenmiş olur. Yapılan bu çalışma, sahte görüntünün JPEG sıkıştırmaya maruz kalması durumunda sonuç verirken, döndürme ve ölçekleme ataklarına karşı dayanıksızdır. Popescu vd. görüntünün ayrılan bloklarından [6]'da önerilen yöntem ile elde edilen özellik vektör boyutunun küçültülmesi ve doğrulama esnasındaki işlem karmaşıklığının azaltılması için Temel Bileşen Analizini (TBA) kullanmıştır [7]. Deneysel sonuçlar yöntemin Toplanır Beyaz Gauss Gürültüsü (AWGN), JPEG sıkıştırması ve bulanıklaştırma ataklarına karşı dayanıklı olduğunu göstermiştir. Luo vd. tarafından 2006 yılında önerilen çalışmada bloklara ait özellik vektörleri üretilirken blokların yoğunluk bilgisinden faydalanılmıştır [8]. Görüntü bloklarının RGB (kırmızı, yeşil ve mavi) renk kanallarına ait ortalama yoğunlukları ve bazı yön bilgileri ile birlikte *1x7* boyutlu özellik vektörleri elde edilmiştir. Çalışmada önerilen yöntemin gürültü, bulanıklaştırma ve bunların kombinasyonu şeklinde uygulanan ataklara karşı da daha dayanıklı olduğu bildirilmiştir. Mahdian vd. tarafından

Bulanık momentler kullanılarak bulanıklaştırma ataklarına karşı dayanıklı bir yöntem önerilmiştir. Her bir bloktan 1x72 boyutlu özellik vektörleri elde edilmiştir [9]. Elde edilen özellik vektörlerinin boyut büyüklüğünden dolayı yazarlar eşleştirme zamanını iyileştirmek için özellik tanımlayıcı vektörlerin boyutlarını TBA kullanarak azaltmışlardır. Sonuçlarda [6, 7]'deki çalışmalara göre özellikle bulanıklaştırma atağı durumunda daha yüksek performansa sahip olduğu gösterilmiştir. Önerilen yöntemin ayrıca AWGN ve kayıplı JPEG sıkıştırma ataklarına karşı dayanıklı olduğu bildirilmiştir. Kang vd. kopyala yapıştır sahteciliği tespitinde Tekil Değer Ayrışımı (Singular Value Decomposition, SVD) yöntemini kullanmayı önermiştir [10]. Yöntem Gauss bulanıklaştırma, gürültü ekleme ve kayıplı JPEG sıkıştırmaları durumlarında bile kopyala yapıştır sahteciliğini gerçekleştirebilmektedir. Huang vd. tarafından Ayrık Kosinüs Dönüşümü (AKD) tabanlı kopyala yapıştır sahteciliği yöntemi önerilmiştir [11]. Bravo-Solorio vd. bloklara ait özellik vektörleri çıkarmak için Fourier dönüşümünün korelâsyon katsayılarını kullanmışlardır [12]. Li vd. dönmeden bağımsız yerel ikilik örüntü (rotation invariant Local Binary Patterns, LBP) tekniğini kullanarak, ayrılan bloklardan özellik vektörleri elde etmiş ve ardından eşleşme işlemi gerçekleştirmiştir [13]. Önerilen yöntemin JPEG sıkıştırma, gürültü ve bulanıklaştırma gibi atakların yanı sıra dönmeye ve ters çevirme ataklarına karşı da dayanıklı olduğu gösterilmiştir. Lee vd. tarafından yön histogramı (Histogram Of Gradient, HOG) bilgisi kullanılarak görüntünün bloklarına dair özellik vektörleri elde edilerek kopyala yapıştır sahteciliği tespiti yapılmıştır [14]. Çalışmanın aynı görüntüde çoklu kopyala yapıştır sahteciliği tespiti yapabildiği ortaya konulmuştur. Ayrıca küçük dereceli dönme, bulanıklaştırma, parlaklık değişimi ve renk azaltma gibi ataklara karşı da dayanıklı olduğu belirtilmiştir.

Yukarıda bahsedilen literatürdeki yöntemlerde görüntünün dairesel veya karesel bloklara ayrılmasının ardından bu bloklara ait özellik vektörlerinin çıkarılmasının ardından bunların eşleşme işlemi gerçekleştirilir. İçerdikleri ortak çalışma yapısından dolayı bu yöntemler literatürde, blok tabanlı kopyala yapıştır sahteciliği tespiti yöntemleri olarak adlandırılmaktadır. Blok tabanlı yöntemlerde görüntüye ait bütün blokların özellik vektörleri çıkarıldığından hesaplama maliyeti yüksek olmaktadır. Araştırmacılar bu problemin üstesinden gelmek için anahtar noktası tabanlı yöntemleri önermişlerdir. Huang vd. 2008 yılında kopyala yapıştır sahteciliği tespitinde SIFT (Scale Invariant Feature Transform) algoritmasını kullanarak anahtar noktalarının elde edilmesini önermişlerdir [15]. Daha sonra Amerini vd. SIFT algoritmasının kullanıldığı daha kapsamlı bir çalışma gerçekleştirmişlerdir [16]. Xu vd. ise kopyala yapıştır sahteciliği tespiti için görüntüden anahtar noktalarının elde edilmesi işleminde SURF algoritmasının kullanılmasını önermişlerdir [17]. Bu yöntemin dönme, ölçekleme, gürültü ekleme, bulanıklaştırma gibi ataklara karşı dayanıklı olduğu deneysel sonuçlar ile birlikte ortaya konmuştur. Zhu vd. ise anahtar noktalarının elde edilmesinde ORB algoritmasını kullanmışlardır [18]. ORB algoritmasının ölçek bağımsız olmaması durumunu iyileştirmek adına bu çalışmada Gauss ölçek uzayı oluşturulmuştur.

Bu çalışmada renkli görüntülerde daha etkin bir kopyala yapıştır sahteciliği tespiti yapan ve blok tabanlı yöntemlere göre daha hızlı çalışan bir şemaya sahip, anahtar noktası tabanlı yeni bir yöntem önerilmesi hedeflenmiştir. SURF algoritmasının hızlı bir şekilde çalıştığı literatürde bilinmektedir [19] ve kopyala yapıştır sahteciliği tespitinde kullanımı görülmektedir [17] . Ancak kopyala yapıştır sahteciliği tespiti için yeterli sayıda anahtar noktası elde edilememesi durumunda etkin bir sahtecilik tespiti yapılamamaktadır. Bu problemin üstesinden gelebilmek ve [17]'deki yönteme göre, çok az süre kaybı ile daha etkin bir kopyala yapıştır sahteciliği tespiti yapmak hedeflenmiştir. Önerilen yöntem ilk olarak renkli test görüntüsünü RGB renk kanallarına ayırır. Her bir renk kanalından elde edilen SURF anahtar noktaları ve özellik tanımlayıcı vektörleri birleştirilmiştir. Birleştirilen özellik tanımlayıcıların eşleşme işlemi gerçekleştirerek sahte bölgelerin eşleştirilmesi yapılmaktadır. Elde edilen deneysel sonuçlar önerilen yöntemin literatürdeki benzer çalışmalara göre, dönme, AWGN, Gauss bulanıklaştırma atakları altında bile daha yüksek performansa sahip olduğunu göstermektedir [17, 18].

Çalışmanın geri kalanında, önerilen yönteme ait detaylar ve yöntemde kullanılan algoritmalardan ikinci bölümde bahsedilecektir. Üçüncü ve dördüncü bölümde ise sırasıyla önerilen yönteme ait deneysel sonuçlar ve çalışmaya ait elde edilen genel sonuçlar verilecektir.

2.ÖNERİLEN YÖNTEM (PROPOSED METHOD)

Literatürdeki SURF tabanlı kopyala yapıştır sahteciliği tespiti yöntemleri görüntünün gri seviyeye dönüştürülmesi (Rx0.3+Gx0.59+Bx0.11) ön işleminden sonra çalışmaktadır. Gri seviyeye dönüştürülen görüntüden SURF algoritması ile anahtar noktası ve bu anahtar noktaları elde edilmekte ve bu anahtar noktalarının özellik tanımlayıcıları üretilmektedir [17].

Yapılan çalışmada *NxMx3* büyüklüğündeki renkli sahte görüntünün, gri seviyeye dönüştürüldüğü durumda anahtar nokta olabilecek piksellerin kaybedilmemesi amacıyla görüntünün kırmızı, yeşil ve mavi ana renklerine göre tonlanmasıyla oluşan RGB renk kanallarından faydalanılması önerilmiştir. Şekil 3a'da ataksız sahte bir renkli görüntünün gri seviyesinden elde edilen SURF anahtar noktaları Şekil 3b'de RGB bileşenlerinden elde edilen SURF anahtar noktalarının birleşimi gösterilmiştir. Görüntünün gri seviyeye dönüştürülmesinin ardından 1240 adet anahtar nokta elde edilirken, RGB renk kanallarının her birinden elde edilen toplam anahtar sayısı 3717 olmaktadır.

Önerilen yöntemde görüntü RGB renk kanallarına ayrılmakta ve bu kanalların her birine SURF algoritması uygulanmaktadır. Daha sonra elde edilen anahtar noktalarının ve özellik tanımlayıcı vektörlerinin

birleştirilmesi gerçekleştirilmektedir. Böylece anahtar nokta sayısı kadar *64* boyutlu özellik tanımlayıcıları elde edilir. Bu üç kanaldan *k, y, m* adet anahtar noktası elde edildiği durumda olur özellik tanımlayıcı vektörler *D=(k+y+m)x64* boyutlu bir matriste tutulur. Daha sonra bu özellik tanımlayıcı vektörlerinin eşleştirilmesi gerçekleştirilmiştir. Son adım olarak eşleşme işleminden sonra varsa hatalı eşleşmelerin yok edilmesi için Random Sample Consensus (RANSAC) algoritması kullanılmıştır. Önerilen yöntemin blok diyagramı Şekil 4.'te verilmiştir.

2.1. SURF Anahtar Noktalarının Çıkarılması
(Extraction of SURF Keypoints)

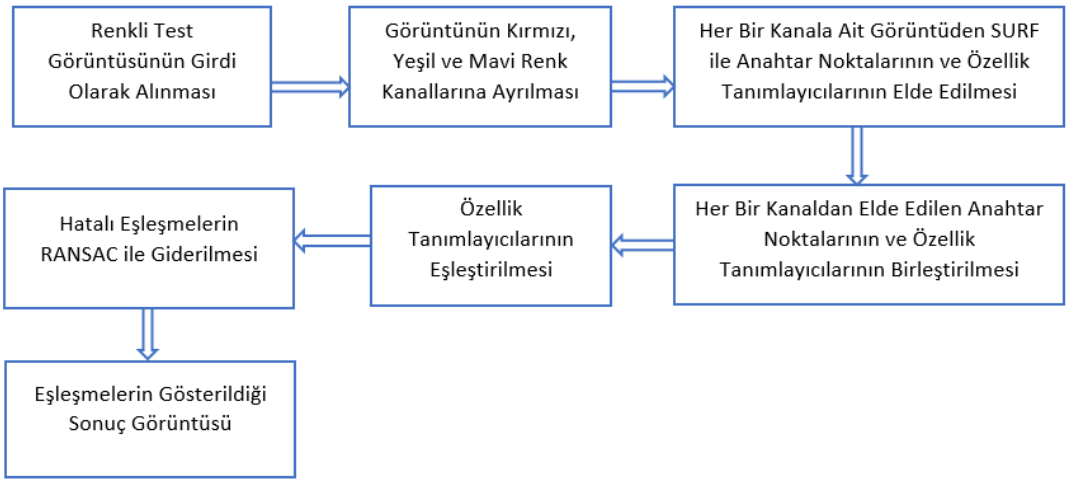
Hızlandırılmış Dayanıklı Öznitelikler (Speeded up Robust Feature, SURF) algoritması, bir görüntüde döndürme, ölçekleme ve ötelemeden bağımsız olarak yerel özellik noktalarının belirlenmesi için ilk olarak 2006 yılında Herbert Bay tarafından geliştirilen özellik çıkarma algoritmasıdır [19]. SURF algoritmasının temeli tümlev görüntülere ve Hessian matrisi ile birleştirilmiş konvolüsyon işlemine bağlıdır. Eş. 1'de verilen Hessian matrisinin farklı görüntü bölgesi ortaya çıkarma özelliğinden yararlanarak görüntüdeki anahtar noktalar bulunur. Tümlev görüntü yaklaşımı ise hesaplama süresini oldukça düşürmektedir. Hessian matris determinantı ölçüt olarak kullanılarak bölgeler arasındaki değişimler hakkında bilgi edinilmektedir.

$$H = \begin{bmatrix} L_{xx}(x,\sigma) & L_{xy}(x,\sigma) \\ L_{xy}(x,\sigma) & L_{yy}(x,\sigma) \end{bmatrix} \quad (1)$$

Burada L_{xx} Eş. 2'de görüldüğü gibi ikinci derece türevin konvolüsyon sonucudur ve L_{xy} ve L_{yy} 'de benzer şekilde elde edilir.

$$L_{xx}(x,\sigma) = I(x) * \frac{d^2}{dx^2} g(\sigma) \quad (2)$$

Şekil 3. a) Gri seviye görüntüden elde edilen anahtar noktaları (Anahtar nokta sayısı: 1240) b) RGB renk kanallarından elde edilen anahtar noktaları (Anahtar nokta sayısı: 3717) ((a)Obtained keypoints from gray level image (Number of keypoimts: 1240) (b) Obtained keypoints from RGB channells (Number of keypoimts count:3717)



Şekil 4. Önerilen yöntemin blok diyagramı (The block diagram of the proposed method)

Hessian matrisi için kullanılan Gauss filtresi, $g(\sigma)$ uygulanmadan önce ayrıklaştırılıp kırpılması gerekmektedir. SURF algoritması bu süzgeçleri kutu süzgeçlerle birlikte kullanmaktadır. Ölçek uzayının oluşturulmasında kullanılan kutu filtrelerinin en alt seviyesi *9x9* boyutunda σ = *1.2* değerli Gauss filtresi kullanılarak oluşturulmuş kutu filtresi bulunmaktadır. Oluşturulan ölçek-uzay yapısında Hessian determinantlarının sonuçlarına göre özellik noktaları çıkarılmaktadır. Ardışık üç ölçekten 3x3'lük alanlar seçilerek toplamda 3x3x3=27 tane piksel arasında en yüksek gradyan değerine sahip piksel özellik noktası olarak belirlenmektedir.

2.2. Özellik Tanımlayıcıların Çıkarılması
(Extraction of Descriptors)

Özellik noktalarına tanımlayıcı atama işleminde ilk adım olarak anahtar noktası merkez olacak şekilde karesel alanlar oluşturulur. Özellik noktasının bunduğu ölçek *s* olarak alındığında bu karesel alanların büyüklüğü *20s* olacak şekilde alınmalıdır. Belirlenen bu alan daha sonra büyüklüğü *5s* olacak şekilde *4x4'*lük karelere bölünür. Bu *4 x 4'*lük alanlara Haar dalgacık filtresi yatay ve dikey şekilde uygulanarak *x* ve *y* yönündeki türevler hesaplanmaktadır ve sırasıyla *dx* ve *dy* elde edilmektedir (filtre boyutu *2s*'dir). Ayrıca tanımlayıcının kutupsal yoğunluk değişimleri hakkında bilgi de tutması için bu yanıtların mutlak değerlerinin ($|dx|$ ve $|dy|$) toplamları da elde edilir. Böylece her alt bölge dört boyutlu tanımlayıcı vektöre sahip olmuş olur. v= ($\sum dx, \sum dy, \sum|dx|, \sum|dy|$). Her *4 x 4* boyutlu alt vektör için bu dört boyutlu vektör çıkartılır. Dolayısıyla *4 x (4 x 4)=64* boyutlu özellik tanımlayıcı vektör oluşturulmuş olur. Şekil 3'deki örnek sahte görüntüye ait ayrılan kırmızı yeşil ve mavi renk kanallarından, SURF algoritmasıyla sırasıyla *1195*, *1284*, *1238* adet anahtar noktaları elde edilmiş olup, her bir anahtar noktasına ait de *64* boyutlu özellik tanımlayıcı vektörleri çıkarılmıştır. Bu özellik tanımlayıcılarının birleştirilmesiyle *3717 x 64*'lük bir özellik vektörü elde edilmiştir.

2.3. Özellik Tanımlayıcıların Eşleştirilmesi
(Matching of Descriptors)

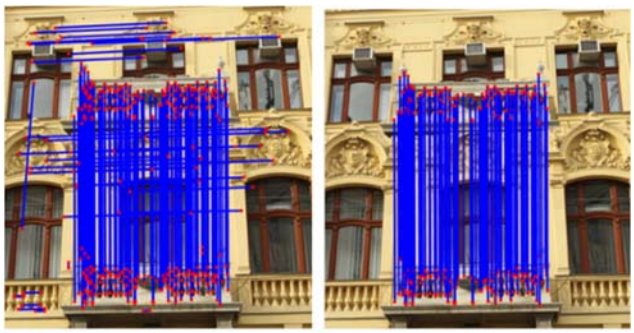
Eşleşme işleminde görüntüden elde edilen SURF anahtar noktalarına ait çıkarılan 64 boyutlu her bir özellik vektörünün diğer özellik vektörleri ile skaler çarpım değerleri hesaplanır ve çarpım matrisinde tutulur, *çarpım*={ $ç_1, \dots, ç_i$ }. Hesaplanan bu değerlerin ters kosinüsleri hesaplanarak elde edilen açı değerleri ve ilgili indisleri sıralanır, d=sort ($cos^{-1}(ç_i)$). Elde edilen sıralı d=$\{d_1 \dots d_n\}$ dizisi için en yakın komşular arasındaki oran önceden belirlenmiş T eşik değerine göre kontrol edilir, $d_i / d_{i+1} < T$. Bu şartı sağlayan vektör çiftlerine ait indislere sahip olan özellik vektörleri eşleştirilir.

2.4. RANSAC İle Hatalı Eşleşmelerin Elenmesi
(Elimination of Outliers with RANSAC)

Bir önceki adımda yapılan eşleşme sonucunda ortaya çıkan yanlış eşleşmeler RANSAC algoritması kullanılarak yok edilmiştir. RANSAC (Random Sample Consensus), yüksek oranda yanlış eşleşmelere sahip veri setindeki hataları minimize etmek için Fischler tarafından önerilen tekrarlamalı bir yöntemdir [20]. Bu yöntemde rastgele eşleşen belli sayıda anahtar noktaları seçilerek Eş. 3'de verilen H dönüşüm(transformasyon) matrisinin parametreleri hesaplanmaktadır.

$$H\begin{bmatrix}x_i\\y_i\end{bmatrix} = \begin{bmatrix}x_j\\y_j\end{bmatrix} \quad (3)$$

Transformasyon matrisi parametreleri ile eşleşen anahtar noktaları arasındaki Öklid uzaklık değerinin γ eşik değerinden küçük olması durumunda eşleşen noktaları doğru eşleşme (inlier) olarak ifade edilirken, büyük olması durumunda (aykırı durum) ise bu eşleşen noktalar hatalı eşleşme (outlier) olarak kabul edilir ve eşleşme matrisinden çıkartılır. Çalışmada γ=0.001 olarak alınmıştır. RANSAC algoritmasının kullanımı ile birlikte hatalı eşleşmelerin giderildiği bir örnek Şekil 5'de verilmiştir. Şekil 5a'daki hatalı eşlemeler elenerek Şekil 5b'deki sonuç görüntü elde edilmiş olur.



Şekil 5. a) RANSAC öncesi eşleştirme sonucu b) RANSAC sonrası eşleştirme sonucu
((a) Matching result before RANSAC (b)Matching result after RANSAC)

3. DENEYSEL SONUÇLAR (EXPERIMENTAL RESULTS)

Önerilen yöntemin oluşturulan veri seti üzerindeki performans sonuçlarına ait örnek görsel sonuçlar ve ortalama sonuçlar bu bölümde verilmiştir. Elde edilen sonuçlar literatürdeki SURF anahtar noktası tabanlı ve ORB anahtar noktası tabanlı çalışmalarla karşılaştırılmıştır [17, 18]. Elde edilen sonuçlar iki alt başlık halinde verilmiştir. İlk alt başlıkta önerilen yöntemin SURF tabanlı [17] çalışma ile karşılaştırması yapılarak örnek görsel sonuçlar ve Tespit Oranı (*TO*) metriği açısından değerlendirme verilmiştir. Önerilen yöntemin çalışma zamanına dair deneysel sonuçlar da yine bu kısımda rapor edilmiştir. İkinci alt başlıkta ise yöntemin precision (keskinlik) ve recall (hassasiyet) metrikleri ile sınıflama performans değerlendirmesi yapılarak litaratürdeki [17, 18] çalışmalarla karşılaştırması gerçekleştirilmiştir. Deneysel sonuçlar, önerilen yöntemin i7 Core 2. 3 GHz işlemcili Windows 7 işletim sistemli dizüstü bilgisayarda, Matlab R2015a ortamında kodlanan yöntemin testi ile elde edilmiştir [21].

Önerilen yöntemin performans analizi için Comofod veri tabanındaki 512x512 boyutlu orijinal ve sahte görüntülerden faydalanılmıştır [22]. Veri tabanından seçilen 40 görüntünün her birine, GIMP açık kaynak kodlu görüntü düzenleyici program yardımıyla, 30 ve 90 derece dönme atağı uygulanmıştır. Ataksız sahte görüntülere ise pencere boyutu w=[*3x3*] olmak üzere $\sigma=0.5$ ve $\sigma=2$ değerleri ile bulanıklaştırma ve SNR değerleri 20 dB ve 40 dB olacak şekilde AWGN (Additive White Gaussian Noise) atağı ayrı ayrı uygulanarak toplam 240 adet sahte görüntü oluşturulmuştur.

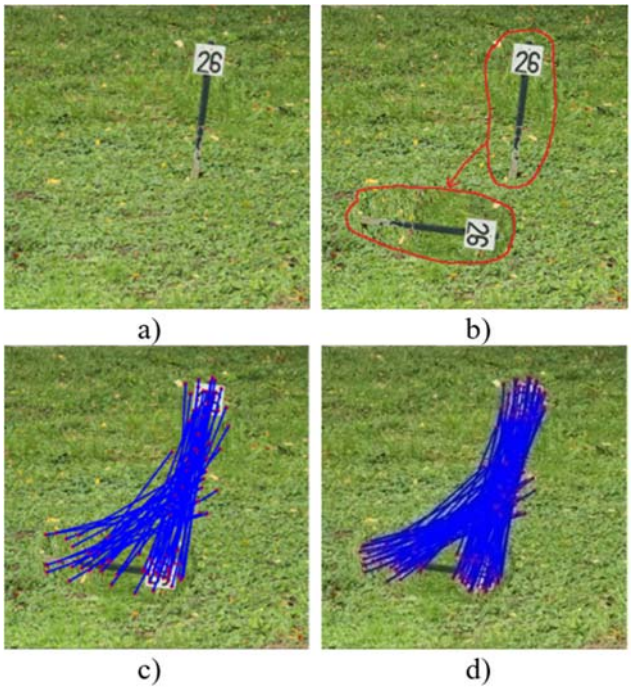
3.1. Tespit Oranı Metriği Sonuçları ve Görsel Sonuçlar
(Results of Detection Rate Metric and Visual Results)

Çalışma için oluşturulan veri seti üzerinde önerilen yöntemin literatürdeki SURF tabanlı [17] yöntem ile kopyala yapıştır sahteciliği tespiti kapasitesini karşılaştırmak için Tespit Oranı (*TO*) metriği kullanılmıştır. Bu metrik, *NxM* boyutlu test görüntüsünün sahtecilik tespiti kapasitesini değerlendirmektedir. *TO* metriği kopyalanıp yapıştırılan bölgelerdeki eşleşen anahtar nokta sayısının o bölgelerdeki piksel sayısına oranıdır [23]. Bu oranın *NM/100* ile çarpılmasıyla da bu metriğin görüntü boyutundan bağımsızlığı sağlanmıştır. K_F, kopyalanan ve yapıştırılan bölge içinde tespit edilen anahtar nokta sayısını, $|F|$ kopyalanan bölgedeki piksel sayısını belirtmek üzere bu oran Eş. 4'deki gibi hesaplanmaktadır. Yüksek *TO* değerleri daha doğru tespit sonuçlarını ifade etmektedir. Tespit Oranı metriği sahte görüntüye ait maskeye bağlı, eşleşen anahtar nokta sayısı ile ilgili değerlendirme sonucunu vermektedir. Maske boyutunun küçük olması durumunda eşleşen anahtar nokta sayısının daha az olmasının negatif etkisini göz önünde bulunduran bir metriktir. Bu açıdan diğer metriklere göre anahtar noktası tabanlı yöntemler için avantaja sahiptir. Bu avantajı göz önüne alınarak değerlendirme sonuçları bu metrik ile verilmiştir.

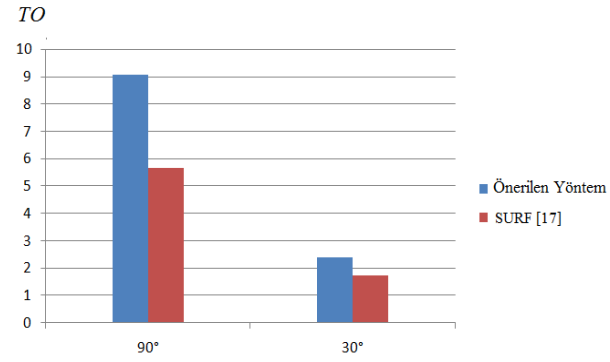
$$TO = \left(\frac{K_F}{|F|}\right)\frac{NM}{100} \tag{4}$$

İlk olarak önerilen yöntemin kopyalanan bölgenin döndürülüp daha sonra yapıştırılması durumunda performansı test edilmiştir. Buna göre veri tabanındaki 30 ve 90 derece döndürme atağına maruz kalmış 40'ar adet görüntü üzerinde test işlemi gerçekleştirilmiştir. Şekil 8'de önerilen yöntemin 90 derece dönme atağı uygulanmış bir sahte görüntü üzerinde örnek görsel sonucu verilmiştir. [17]'deki çalışma ve önerilen yöntem sonuçları Şekil 6c ve Şekil 6d'de gösterilmiştir. Bu örnek için [17]'deki yöntem ile 26 adet eşleşme bulunurken önerilen yöntem ile bu sayı 63'e çıkarak daha fazla eşleşme gerçekleştirilmiş olur.

Önerilen yöntemin dönme atağı durumundaki performansına ilişkin ortalama bir sonuç elde etmek için 30 derece ve 90 derece dönme atağına maruz kalmış bütün bu görüntülere [17]'deki yöntem ve önerilen yöntem uygulanarak ortalama TO değerleri elde edilmiş ve sonuçlara ait bir grafik Şekil 7'de verilmiştir. Şekilde de görüldüğü gibi belirtilen döndürme derecelerinde [17]'ye göre daha başarılı sonuçlar elde edilmiştir.

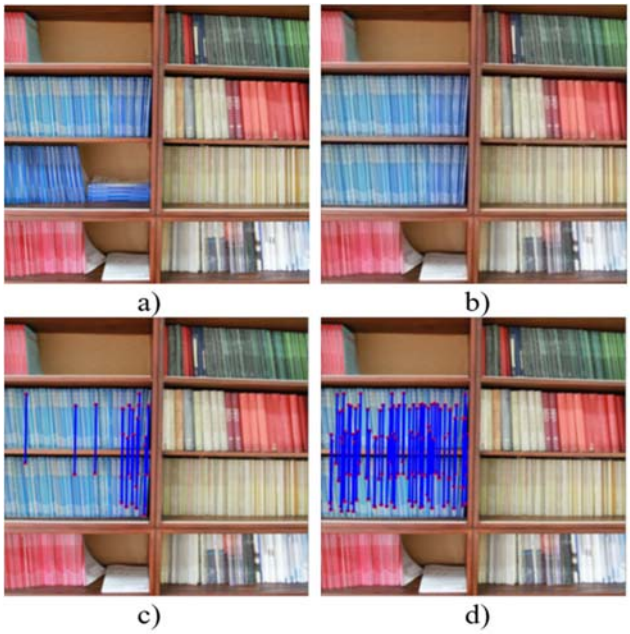


Şekil 6. a) Orijinal görüntü b) Sahte görüntü c) [17]'de önerilen yöntem sonucu (Eşleşme sayısı: 26) d) Önerilen yöntem sonucu (Eşleşme sayısı: 63) ((a) Original image (b)Forged image (c) Result of proposed method in [17] (Matching result: 26) (d) Result of proposed method (Matching result: 63))



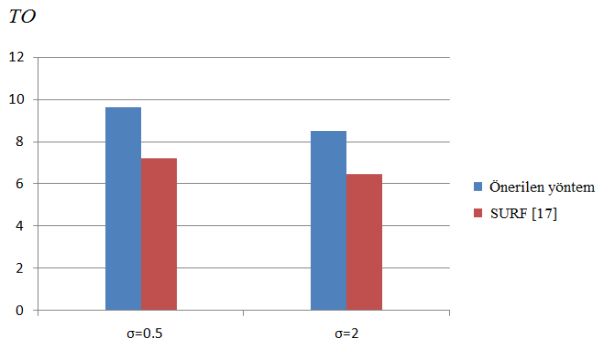
Şekil 7. Dönme atağı durumunda karşılaştırmalı test sonucu (Comparative test results under rotation attack)

İkinci test işleminde önerilen yöntemin Gauss bulanıklaştırma atağı durumunda performans analizi yapılmıştır. Şekil 8'de, pencere boyutu [3x3] ve σ değeri 2 olacak şekilde bulanıklaştırma atağına maruz kalmış bir örnek sahte görüntüye [17] ve önerilen yöntemin uygulanması ile elde edilen eşleşme sonuçları verilmiştir. Şekil 8c ve Şekil 8d'de sırasıyla görsel eşleşme sonuçları görülmektedir. [17]'deki önerilen yöntem ile 16 adet eşleşme elde edilirken önerilen yöntem ile 40 adet eşleşme sonucu elde edilmiştir. Böylece kopyalanan bölgeler daha net ortaya konulmuştur.



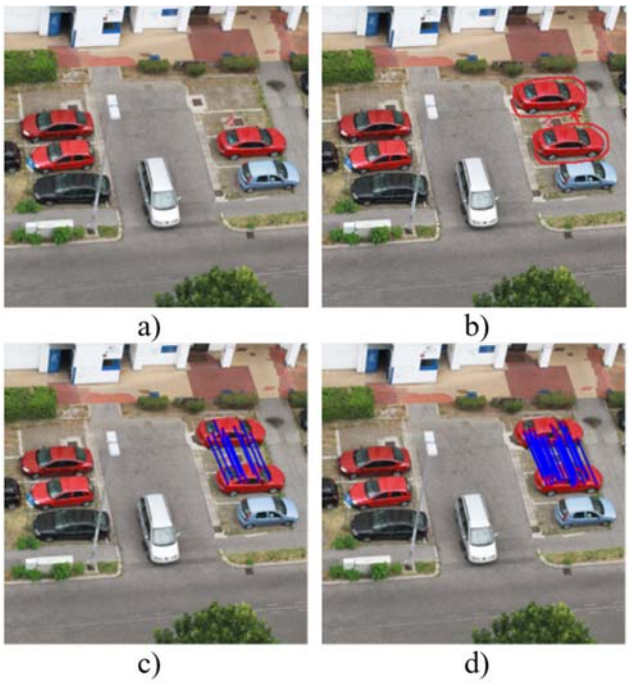
Şekil 8. a) Orijinal görüntü b) Sahte görüntü c) [17]'deki yöntem sonucu (Eşleşme sayısı: 16) d) Önerilen yöntem sonucu (Eşleşme sayısı: 40) ((a) Original image (b)Forged image (c) Result of proposed method in [17] (Matching result: 16) (d) Result of proposed method (Matching result: 40))

Bulanıklaştırma atağındaki performans analizine dair ortalama bir sonuç elde etmek için veri setindeki σ=0. 5 ve σ=2 değerleri ile bulanıklaştırılmış 40'ar tane sahte test görüntüsüne [17]'deki yöntem ve önerilen yöntem uygulanmış olup sonuçlar elde edilmiştir. Elde edilen bu sonuçların ortalama TO değerlerine ait karşılaştırmalı grafik Şekil 9'de verilmiştir.



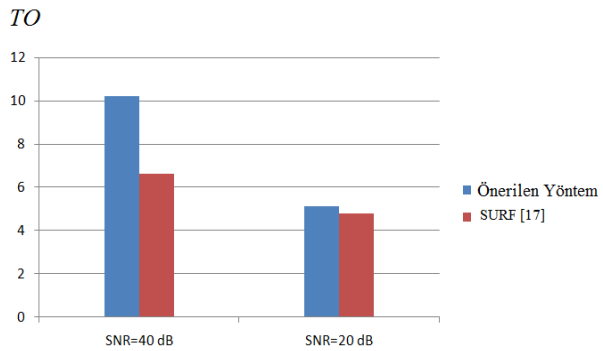
Şekil 9. Gauss bulanıklaştırma atağı durumunda karşılaştırmalı test sonucu
(Comparative test results under Gaussian blurring attack)

Şekil 9'da da görüldüğü gibi önerilen yöntem ile iki durumda da daha yüksek TO değerleri elde edilmiştir, önerilen yöntem ile daha etkin sahtecilik tespiti gerçekleştirilmiştir. Son deneyde ise önerilen yöntemin AWGN atağına karşı dayanıklılığı gözlemlenmiştir. Şekil 10a'daki örnekte orijinal görüntünün kopyala yapıştır işleminden sonra SNR değeri 20 dB olacak şekilde AWGN atağına maruz kalması sonucu Şekil 10b görüntüsü elde edilmiştir. Bu görüntüde, [17]'de önerilen yöntem ile 17 adet eşleşme tespiti yapılırken önerilen yöntem ile bu sayı 32 olmaktadır. 20 dB sinyal durumunda bile önerilen yöntem [17]'e göre daha etkin bir sahtecilik tespiti yapabilmektedir. Şekil 10c ve Şekil 10d'de de [17] ve önerilen yöntem için görsel eşleşme sonuçları da verilmiştir.



Şekil 10. a) Orijinal görüntü b) Sahte görüntü c) [17]'deki yöntem sonucu (Eşleşme sayısı:17) d) Önerilen yöntem sonucu (Eşleşme sayısı: 32) ((a) Original image (b)Forged image (c) Result of proposed method in [17] (Matching result: 17) (d) Result of proposed method (Matching result: 32))

Veri setinde oluşturulan 40 sahte görüntüye ayrı ayrı 20 dB ve 40 dB sinyalleri ile AWGN atağı uygulanması ile bu atak durumunda [17]'deki yöntemin ve önerilen yöntemin ortalama TO değerleri elde edilmiştir. Şekil 11'de de görüldüğü gibi bu atak durumunda bile önerilen yöntem [17]'e göre daha yüksek performans sergilemiştir.



Şekil 11. AWGN atağı durumunda karşılaştırmalı test sonucu
(Comparative test results under AWGN attack)

Önerilen yöntem R,G,B renk kanallarının her birinden SURF anahtar noktaları ve özellik tanımlayıcıları çıkardığı için çalışma zamanı açısından [17]'deki yönteme göre daha yavaş çalışmaktadır. Ancak SURF algoritması hızlı çalışması ile popüler olduğu ve diğer anahtar noktası çıkarma yöntemlerine göre daha hızlı çalıştığı için önerilen yöntemde üç kanaldan da anahtar noktası çıkarılmasına rağmen fazla hız kaybı gözlemlenmemektedir. Tablo 1.'de önerilen yöntemin [17]'deki yöntem ile ortalama çalışma zamanı karşılaştırması verilmiştir. Sonuçtan da gözlemleneceği gibi önerilen yöntemde gözlemlenen süre kaybı birçok durum için ihmal edilebilirdir.

Tablo 1. Ortalama çalışma zamanı değerlendirmesi (sn.)
(Evaluation of average running time (sec.))

Ataklar	Parametreler	Çalışma Zamanı (sn.)	
		[17]	Önerilen Yöntem
Dönme	30°	2,10	4,28
	90°	2,22	4,40
Gauss Bulanıklaştırma	σ=0,5	2,25	4,48
	σ=2	2,17	3,98
AWGN	40 dB	2,20	4,65
	20 dB	2,14	4,302

3.2. Sınıflandırma Performansı Değerlendirmesi
(Evaluation of Classification Performance)

Bu bölümde önerilen yöntemin sınıflandırma performansı (bir test görüntüsünün sahte veya orijinal olduğunu ortaya koyma kapasitesi) kesinlik (precision) ve hassasiyet (recall) metrikleri açısından literatürdeki benzer çalışmalarla karşılaştırılmıştır [17, 18]. "p" ile ifade edilen kesinlik (precision) metriği, sahte olarak belirlenen bir görüntünün gerçekten de sahte olması olasılığı anlamına gelmektedir. "r" gösterimi de hassasiyet(recall) metriğini ifade etmektedir ve sahte bir görüntüyü tespit edebilme olasılığı anlamına gelmektedir. Eş 5'de verilen "p" ve "r" metriklerinin hesaplanmasında kullanılan T_p, sahte görüntülerin sahte olarak tespit edildiği toplam görüntü sayısını ifade eder. F_p, orijinal görüntülerin sahte olarak ortaya konduğu toplam görüntü sayısını temsil ederken, F_n de sahte görüntülerin orijinal olarak belirlendiği toplam görüntü sayısını gösterir. Bir görüntünün sahte olarak etiketlendirilmesi için, görüntü üzerinde elde edilen eşleşme sayısının ∂ ile gösterilen eşik değerinden fazla olması gerekmektedir. Yapılan çalışmada ilgili eşik değeri deneysel olarak 4 seçilmiştir ($\partial = 4$).

$$p = \frac{T_p}{T_p + F_p} \quad r = \frac{T_p}{T_p + F_n} \tag{5}$$

Tablo 2.'de önerilen yöntemin literatürde yer alan [17, 18]'deki çalışmalarla sınıflandırma performansı açısından karşılaştırmalı sonuçları verilmiştir. 30° dönme atağı uygulanan sahte görüntüler üzerinde yapılan test sonuçlarına göre [17]'deki ve [18]'deki yöntemler ile elde edilen keskinlik değeri sırasıyla 0,80 ve 0,85 olduğu görülürken, bu değer önerilen yöntem için 0,92 olarak elde edilmiştir. Hassasiyet değeri ise [17]'deki yöntemde 0,80 olarak elde edilirken [18]'deki yöntem ve önerilen yöntemde 0,87 olarak elde edilmiştir. 20 dB AWGN atağı durumdaki deneysel sonuçlara göre ise [17]'deki ve [18]'deki yöntemler ile elde edilen keskinlik değeri sırasıyla 0,81 ve 0,90 olduğu görülürken bu değer önerilen yöntem ile 0,92 olarak elde edilmiştir. Hassasiyet değeri ise [17]'deki yöntemde 0,90 iken [18]'deki yöntem ile önerilen yöntemde 0,95 olarak elde edilmiştir. Tablo 2.'den de görüleceği gibi veri setindeki çeşitli ataklara maruz kalmış görüntüler üzerinde yapılan testlerde keskinlik ve hassasiyet değerleri, literatürdeki diğer yöntemlere göre nispeten daha yüksek olarak elde edilmiştir [17, 18].

Tablo 2. Sınıflama performansı değerlendirmesi (Evaluation of classification performance)

	Parametreler		[17]	[18]	Önerilen Yöntem
Dönme	30°	p	0,80	0,85	0,92
		r	0,80	0,87	0,87
	90°	p	0,83	0,86	0,92
		r	0,95	0,95	0,97
Gauss Bulanıklaştırma	σ=0,5	p	0,82	0,86	0,92
		r	0,92	0,95	0,97
	σ=2	p	0,81	0,86	0,92
		r	0,90	0,92	0,97
AWGN	40 dB	p	0,82	0,86	0,93
		r	0,95	0,95	0,97
	20 dB	p	0,81	0,90	0,92
		r	0,90	0,95	0,95

4. SONUÇLAR (CONCLUSIONS)

Bu çalışmada renkli görüntülerde daha etkin olan yeni bir kopyala yapıştır sahteciliği tespiti yöntemi önerilmiştir. Önerilen yöntemde sahte test görüntüsünün R, G, B renk kanallarının her birinden SURF anahtar noktalarının çıkarılması yöntemin üstünlüğünü sağlamıştır. Bu üç kanaldan elde edilen anahtar noktaları ve özellik tanımlayıcıları birleştirilmiştir. Bir sonraki aşamada ise özellik tanımlayıcıların eşleştirilmesi yapılmıştır. Eşleşme aşamasından sonra hatalı eşleşmeler RANSAC algoritması ile giderilmiştir. Önerilen bu yöntem literatürdeki SURF tabanlı ve ORB tabanlı çalışmalarla karşılaştırılmış ve daha üstün performansa sahip olduğu deneysel sonuçlarla ispatlanmıştır [17, 18]. Ayrıca yöntemin dönme, bulanıklaştırma ve AWGN gürültü ekleme atakları durumunda da etkin sonuçlar ürettiği deneysel sonuçlarda gösterilmiştir.

KAYNAKLAR (REFERENCES)

1. Qureshi, M.A. ve Deriche, M., A bibliography of Pixel-Based Blind Image Forgery Detection Techniques, Signal Processing: Image Communication, 39, 46–74, 2015.
2. Lian, S. ve Kanellopoulos D., Recent Advances in Multimedia Information System Security, Informatica, 33, 3–24, 2009.
3. Om, A. ve Be, K., Passive detection of Copy-Move Forgery in Digital Images: State-of-the-Art, Forensic Science International, 231, 284–295, 2013.
4. Zhang, Z., Zhou, Y., Kang, J., ve Ren, Y., Study of Image Splicing Detection, Advanced Intelligent Computing Theories and Applications. With Aspects of Theoretical and Methodological Issues, 5226, 1103-1110, 2008.
5. Redi, J.A., Taktak, W. ve Dugelay, J. L., Digital Image Forensics: A Booklet for Beginners, Multimedia Tools Appl., 51 (1), 133–162, 2011.
6. Fridrich, A.J., Soukal, B.D. ve Lukáš, A.J., Detection of Copy-Move Forgery in Digital Images, Digital Forensic Research Workshop (DFRWS), 2003.
7. Popescu, A. ve Farid, H., Exposing Digital Forgeries by Detecting Duplicated Image Regions, Tech. Rep., TR2004-515, Dartmount Collage, 2004.
8. Luo, W., Huang, J. ve Qiu, G., Robust Detection of Region-Duplication Forgery in Digital Images, International Conference on Pattern Recognition, Hong Kong, Bildiriler Kitabı 4, 746–749, Kasım 2009.
9. Mahdian, B. ve Saic, S., Detection of Copy-Move Forgery Using a Method Based on Blur Moment Invariants, Forensic Sci. Int., 171, 180–189, 2007.
10. Kang, X. ve Wei, S., Identifying Tampered Regions Using Singular Value Decomposition in Digital Image Forensics, International Conference on Computer Science and Software Engineering, Wuhan, Hubei, Bildiriler Kitabı: 926–930, Aralık 2008.
11. Huang, Y., Lu, W., Sun, W. ve Long, D., Improved DCT Based Detection of Copy-Move Forgery in Images, Forensic Science International, 206, 178–184, 2011.
12. Bravo-Solorio, S. ve Nandi, A.K., Exposing Duplicated Regions Affected by Reflection, Rotation and Scaling, International Conference on Acoustics, Speech and Signal Processing, Prague, Bildiriler Kitabı: 1880–1883, Mayıs 2011.
13. Li, L., Li, S. ve Zhu, H., An Efficient Scheme for Detecting Copy-Move Forged Images by Local Binary Patterns", Journal of Information Hiding and Multimedia Signal Processing, 4, 1, 46–56, 2013.
14. Lee, J., Chang, C. ve Chen, W., Detection of Copy–Move Image Forgery Using Histogram of Oriented Gradients, Information Sciences, 321, 250–262, 2015.
15. Huang, H., Guo, W. ve Zhang, Y., Detection of Copy-Move Forgery in Digital Images using SIFT Algorithm, Computational Intelligence and Industrial Application, Computer Society, Wuhan, Bildiriler Kitabı: 272–276, Aralık 2008.
16. Amerini, I., Ballan, L., Caldelli, R., Bimbo, A.D. ve Serra, G., A SIFT-Based Forensic Method For Copy-Move Attack Detection and Transformation Recovery, IEEE Transactions on Information Forensics and Security, 6 (3), 1099–1110, 2011.
17. Xu, B., Wang, J., Liu, G., Li, H. ve Dai, Y., Image Copy-Move Forgery Detection Based on SURF, International Conference on Multimedia Information Networking and Security, Nanjing, Jiangsu, Bildiriler Kitabı: 889–892, Kasım 2010.
18. Zhu, Y., Shen, X. ve Chen, H., Copy-Move Forgery Detection Based on Scaled ORB, Multimedia Tools and Applications, 75 (6), 1-15, 2015.
19. Bay, H., Ess, A., Tuytelaars, T. ve Van Gool, L., SURF: Speeded Up Robust Features, Computer Vision and Image Understanding, 110 (3), 346-359, 2008.
20. Fischler, M.A. ve Bolles, R.C., Random Sample Consensus: A Paradigm for Model Fitting with Applications to Image Analysis and Automated Cartography, Communications of the ACM, 24 (6), 381–395, 1981.
21. Muzaffer, G., Anahtar Noktası Tabanlı Kopyala Yapıştır Sahtecilikleri Tespiti, Yüksek Lisans Tezi, KTÜ Fen Bilimleri Enstitüsü, Trabzon, 2016.
22. http://www.vcl.fer.hr/comofod, 15 Ocak 2016.
23. Ustübioglu, B., Muzaffer, G., Ulutas, G., Nabiyev, V., Ulutas, M., A Novel Keypoint Based Forgery Detection Method Based On LPQ and SIFT, International Conference on Electrical and Electronics Engineering (ELECO'15), Bursa, Bildiriler Kitabı: 185 – 189, Ekim 2015.