mühendislikdergisi
Dicle Üniversitesi Mühendislik Fakültes
Cilt: 8, Sayı: 4, 781-795
Eylül 2017

G-SURF ve AKAZE tabanlı yeni bir kopyala-yapıştır sahteciliği tespit yöntemi

Güzin ULUTAŞ[*,1]

[1] *Karadeniz Teknik Üniversitesi, Bilgisayar Mühendisliği Bölümü, Trabzon*

Makale Gönderme Tarihi: 13.04.2017 Makale Kabul Tarihi: 15.05.2017

Öz

Görüntü sahteciliği yöntemlerinden sıklıkla karşılaşanı olan Kopyala-Yapıştır Sahteciliği, görüntü içerisindeki bir bölgenin başka bir bölgenin üzerine kopyalanması ile gerçekleştirilir. Bir nesnenin kapatılması yada var olan bir nesnenin tekrarlanması bu tür sahteciliğin amaçları arasında yer almaktadır. Kopyala yapıştır sahteciliğini tespit etmeye çalışan yöntemler ikiye ayrılmaktadır: Blok tabanlı ve Anahtar noktası tabanlı yöntemler. Son yıllarda ise Anahtar noktası tabanlı yöntemler daha hızlı bir şekilde sahte bölgeyi tespit edebildikleri için araştırmacılar arasında popülerlik kazanmıştır. Fakat anahtar noktası tabanlı yöntemlerin en önemli problemlerinden biri kullandıkları ölçek uzayının lineer olması ve ölçek uzayı görüntülerini oluştururken görüntünün her bölgesine eşit bulanıklaştırma uygulamasıdır. Çalışmada doğrusal olmayan ölçek uzayını ölçek görüntülerini oluşturmada kullanan AKAZE (Accelerated KAZE) anahtar noktası çıkarma yöntemini, yine tanımlayıcı elde etme aşamasında görüntünün kenar bilgisini koruyan G-SURF (Gauge-Speeded-Up Robust Features) tanımlayıcı elde etme algoritması ile beraber kullanılmıştır. Aynı zamanda hatalı eşleşmeleri ortadan kaldırabilmek amacı ile RANSAC (Random Sample Consensus) algoritmasından faydalanılmıştır. Önerilen yöntemin sonuçlarını değerlendirebilmek ve kıyaslama yapabilmek amacı ile MICC-F220 veritabanı kullanılmıştır. Deneyler yöntemin Doğru Pozitif Oranı ve Yanlış Pozitif oranı açısından benzer yöntemlerle kıyaslayınca daha iyi sonuçlar ürettiğini göstermiştir. Sonuçlar aynı zamanda yöntemin çeşitli saldırılar karşısında daha yüksek Seçicilik değerleri elde ettiğini ortaya koymaktadır. Duyarlık değerleri ise özellikle JPEG sıkıştırma ve Gauss bulanıklaştırma saldırıları değerlendirildiğinde benzer çalışmalardan daha iyi sonuçlar üretmektedir.

Anahtar Kelimeler: *Görüntü sahteciliği, AKAZE, GSurf, Kopyala yapıştır sahteciliği*

[*]Yazışmaların yapılacağı yazar: Güzin ULUTAŞ. gulutas*@ktu.edu.tr*; Tel: (462) 377 36 22

Giriş

Görüntü yakalama teknolojilerindeki hızlı ilerleme ve görüntü yakalayabilen mobil cihazların günlük hayattaki yaygın kullanımları, sık karşılaşılan çoklu ortam dosyaları olan görüntülerin orjinalliğinin sorgulanması ile sonuçlanmıştır. Görüntülerin doğrulanması, bu dosyaların yargıda delil olarak kullanıldığı günümüzde, önemli bir araştırma konusu olarak görülmektedir. Görüntü sahteciliklerinin tespit edilmesi için araştırmacılar son yıllarda, birçok yöntem önermişlerdir. Araştırmacılar tarafından en çok ilgi gören ve kopyala-yapıştır sahteciliği olarak adlandırılan görüntü sahteciliği yöntemi, görüntü içerisindeki bir bölgeyi kopyalayıp başka bir bölge üzerine kapama veya tekrarlama amaçlı yapıştırmaya dayanmaktadır. Şekil 1'de Kopyala-Yapıştır sahteciliğine örnek olarak, orjinal görüntü ve duvarın bir bölgesi ile yazının bir kısmının örtülerek oluşturulduğu sahte görüntü verilmiştir.



(a) (b)

Şekil 1. (a) Orjinal Görüntü (b) Sahte Görüntü

İlk olarak 2003 yılında Fridrich vd. tarafından ortaya konulan kopyala yapıştır sahteciliği, yazarlar tarafından Ayrık Kosinüs Dönüşümünün (AKD) kullanımı ile tespit edilmeye çalışılmıştır (Fridrich vd., 2003). Önermiş oldukları yöntem, görüntüyü birbiri ile örtüşen 8x8 büyüklüğündeki alt bloklara ayrıştırmakta ve her bloktan AKD ile beraber özellik vektörleri üretmektedir. Elde edilen özellik vektörleri üzerinde sözlük sıralaması uygulanarak, benzer olan vektörlerin yakın hale getirilmesi hedeflenmektedir. Vektörlerin kıyaslanmasında Öklid mesafesi kullanılmış ve benzer vektörlerin temsil ettiği blokların sahte olarak işaretlenmesi gerçekleştirilmiştir. Fridrich (2003)'deki yöntemde kullanılan özellik vektörü boyutunun küçültülmesini ve oluşturulan sahte görüntüye JPEG sıkıştırma uygulanması durumundaki performans kaybının giderilmesini hedefleyen Popescu ve Farid, özellik vektörlerinin elde edilmesi aşamasında Temel Bileşen Analizinden (TBA) faydalanmıştır (Popescu ve Farid, 2004). Kopyalanan bölgeye yapıştırılmadan önce döndürme veya ölçekleme uygulanması durumunda her iki yöntem de sahteciliğin tespitinde başarısız olmaktadır. 2009 yılında Bayram vd. bloklardan özellik çıkarımında Fourier Mellin kullanarak yapıştırılan bölgenin 10° 'ye kadar döndürülmesi durumunda sahteciliği tespit edebilmiştir (Bayram vd., 2009). Bu çalışmanın ardından Log Polar Dönüşümü (LPD) ve Polar Harmonik Dönüşümü'de (PHD) sahteciliğin tespitinde ilgili literatürde kullanılmıştır (Wu vd., 2010; Li vd. 2012). Özellik vektörlerinin temsilinde Fourier Dönüşümü, Dalgacık dönüşümü, Tekil değer ayrıştırma gibi frekans tabanlı yöntemler yaygın olarak kullanılmış ve sahteciliğin tespitindeki doğruluk oranı iyileştirilmeye çalışılmıştır (Ketenci ve Ulutas, 2013; Farukh vd., 2014; Zhao vd. 2013). Ayrıca araştırmacılar bloklardan özellik çıkarımı esnasında döndürme ve ölçekten bağımsız görüntü momentlerinden de faydalanmışlardır. Hu momentleri, Zernike momentleri ve Krawtchouk momentleri kopyala yapıştır sahteciliğinin tespitinde kullanılan momentlere örnek olarak verilebilir (Hu vd. 2014; Ryu vd. 2010; İmamoğlu vd., 2013).

Şu ana kadar bahsi geçen yöntemlerde, görüntünün bloklara ayrıştırılması ve bu bloklardan elde edilen özellik vektörlerinin kıyaslanması~~ı~~ ile sahteciliğin tespiti gerçekleştirilmiştir. Sahteciliğin tespitinde "Blok tabanlı" bu yöntemlere alternatif olan ve anahtar noktalarından elde edilen tanımlayıcıların benzerliğini kullanan ilk yöntem Pan vd. tarafından 2010 yılında önerilmiştir (Pan ve Lyu, 2010). 2010 yılından itibaren sahteciliğin tespitinde anahtar noktası

çıkarma yöntemlerini kullanan çalışmalar, "Anahtar noktası tabanlı yöntemler" olarak adlandırılmıştır. Bu alandaki önemli çalışmalardan biri Amerini vd. tarafından ortaya konan ve Ölçekten bağımsız özellik dönüşümünden (Scale Invariant Feature Transform-SIFT) faydalanan yöntemdir (Amerini vd., 2011). Elde edilen deneysel sonuçlarda araştırmacılar, yöntemin çeşitli geometrik dönüşümlere karşı dayanıklı olduğunu göstermiştir. 2013 yılında ise yine Amerini vd. önerdikleri yöntem ile anahtar noktalarını kümeleyerek, aynı görüntüde birden fazla yerde kopyala yapıştır sahteciliğini algılayabilir hale gelmiştir (Amerini vd., 2013). Son yıllarda ise görüntüyü bölütleme yazarlar tarafından ön işlem olarak kullanılmakta ve belirli bir bölüt içerisindeki anahtar noktaları kendi bölütü dışındaki anahtar noktaları ile kıyaslanmaktadır (Li vd. 2014; Wang vd. 2016; Mishra vd. 2013). Anahtar noktası tabanlı yöntemlerin en önemli dezavantajları: (a) ~~K~~kopyalanan bölgenin küçük ve az değişimli bir bölge olması durumunda yeterli anahtar noktasının ilgili bölgede elde edilememesi (b) anahtar noktalarının kümelenmesinde kullanılacak en uygun öbekleme algoritmasının belirlenme güçlüğü olarak verilebilir. (Christlein vd., 2012) ile (Cozzolino vd., 2015)'de önerilen çalışmalarda yoğun alan teorisi~~ni~~ kullanılarak, özellikle kopyalanan bölgenin az değişim içermesi probleminin üstesinden gelinmeye çalışılmıştır.

Kopyala yapıştır sahteciliğinin tespiti alanında yapılan çalışmalar irdelendiğinde anahtar noktası tabanlı yöntemlerin ön plana çıktığı gözlemlenmektedir. Fakat bu çalışmalar ile beraber gelen en önemli problem, kopyalanıp yapıştırılan bölgenin anahtar noktası içermemesi durumunda sahteciliğin tespit edilemeyecek olmasıdır. Özellikle kötü niyetli kişilerin sahtecilik işlemi ardından, yapıştırılan bölge etrafındaki izleri kapayabilmek amacı ile sıkıştırma, bulanıklaştırma vb. son işlemleri uygulayabilecek olduğu düşünüldüğünde, yöntemin sahte bölgeler üzerinde anahtar nokta elde edebilme olasılığının da düşeceği söylenebilir. Bu alanda kullanılan anahtar noktası belirleme algoritmaları ise (SIFT-Scale Invariant Feature Transform, SURF vb), ölçekten bağımsızlık elde edebilmek amacı ile bulanıklaştırma yolu ile alt görüntüler elde etmektedir. Farklı ölçeklerdeki görüntüleri elde edebilmek amacı ile uygulanan bulanıklaştırma işlemi ise görüntü genelinde eşit olarak uygulanmamakta ve özellikle nesne kenarlarını korumamaktadır. Böylece görüntü üzerinden elde edilebilecek anahtar noktası sayısı azalabilmektedir.

Bahsi geçen problemi çözebilmek amacı ile 2012 yılında Alcantarilla vd. KAZE özelliklerini önermişlerdir (Alcantarilla vd., 2012). KAZE anahtar noktası çıkarma yöntemi doğrusal olmayan difüzyon filtreleme prosedürünü kullanmaktadır. 2013 yılında gerçekleştirdikleri bir diğer çalışmada ise, hızlandırılmış çok ölçekli özellik belirleme ve tanımlayıcı elde etme yöntemi olan AKAZE'yi (Accelerated KAZE) tanımlamışlardır (Alcantarilla vd., 2013a). AKAZE'nin en önemli özelliği nesne sınırlarını koruyacak şekilde doğrusal olmayan ölçek uzayı oluşturabilme yeteneğidir. Bu çalışmada görüntü üzerinden anahtar noktalarının elde edilmesi aşamasında, bahsi geçen (Ölçek görüntülerini oluştururken nesne sınırlarını koruyabilmesi) AKAZE yönteminden faydalanılmıştır. Alcantarilla (2013)'deki çalışmada anahtar noktalarından tanımlayıcı elde edilmesi aşamasında, değiştirilmiş yerel fark ikilileri (Modified Local Difference Binary-MLDB) kullanılmaktadır. AKAZE yönteminde var olan doğrusal olmayan difüzyon sürecinden tanımlayıcı oluşturulmasında faydalanmayan, ölçekten bağımsızlığı düşük MLDB yöntemi yerine, bu çalışmada 2013 yılında önerilmiş olan ve Gauge koordinat düzlemini kullanan Gauge-SURF (G-SURF) tanımlayıcıları kullanıldı (Alcantarilla vd., 2013b). G-SURF tanımlayıcısının en önemli özelliği aynı AKAZE gibi görüntünün kenar bilgisini korurken gürültü bilgisini göz ardı etmesidir. Bu ise G-SURF tanımlayıcılarına diğer tanımlayıcıların yanında önemli bir avantaj kazandırmaktadır.

Bu çalışmada, kopyala yapıştır sahteciliğini tespit edebilmek amacı ile görüntüden AKAZE anahtar noktaları elde edilmekte ve anahtar noktalarından tanımlayıcı üretme aşamasında ise Gauss bulanıklaştırmasına ihtiyaç duymadan görüntünün yapısal özelliklerini kullanan G-SURF tanımlayıcılarından faydalanılmaktadır. Elde edilen tanımlayıcılar arasındaki benzerlik Öklid mesafesi ile belirlenmektedir. Her bir tanımlayıcı ile kendisine en yakın iki tanımlayıcının mesafesinin oranı belirli bir değerden az ise, karşılık düşen anahtar noktalarının eşleştiği varsayılmaktadır. Elde edilen deneysel sonuçlarda, önerilen yöntemin Doğru Pozitif Oranı, Yanlış Pozitif Oranı açısından benzer çalışmalara göre daha iyi sonuçlar ürettiği gözlemlenmektedir. Aynı zamanda yöntem, Duyarlık ve Seçicilik değerleri açısından da pozitif sonuçlar ortaya koymaktadır.

Yayının geri kalan kısmı şu şekilde düzenlenmiştir. İkinci bölümde, görüntü üzerinden anahtar noktalarının elde edilmesi aşaması anlatılırken, üçüncü bölümde anahtar noktalarından tanımlayıcıların elde edilmesinden bahsedilecektir. Elde edilen tanımlayıcılar kullanılarak sahte bölgelerin tespiti yine aynı bölüm içerisinde anlatılacaktır. MICC-F220 veritabanı üzerinde elde edilen deneysel sonuçlar, görsel sonuçlar ve benzer yöntemler ile kıyaslamalar son bölümde verilecektir.

Görüntü Üzerinden Anahtar Noktalarının Elde Edilmesi

Bu bölümde giriş görüntüsü üzerindeki tanımlayıcı anahtar noktalarının elde edilmesi için uygulanacak olan AKAZE anahtar noktası çıkarma algoritmasının alt adımlarından bahsedilecektir. Günümüzde kullanılan modern anahtar noktası çıkarma yöntemleri SIFT, SURF vb. gibi, girişten gelen görüntüyü bir fonksiyon ile filtreleyerek ölçek uzayındaki alt görüntüleri oluşturmaktadır. Örneğin, SIFT görüntüye ait ölçek uzaylarındaki alt görüntüleri oluşturmak için Gauss çekirdeğinden faydalanmaktadır. Ölçek uzayını oluşturmak için her seferinde uygulanan Gauss çekirdeklerine ait sapma değeri değiştirilerek alt görüntüler üretilmektedir. SURF algoritması ise, Gauss türevlerini kutu filtreleri üzerinden yakınsayarak Gauss ölçek uzayını oluşturmaktadır. Bahsi geçen ve ölçek uzaylarını doğrusal anlamda oluşturan bu yöntemlerle ilgili en önemli dezavantaj, uyguladıkları Gauss bulanıklaştırması esnasında nesnelerin dış çeperlerini göz ardı etmeleridir. Ölçek uzayı görüntü üzerindeki gürültünün etkisinin azaltılması anlamında katkıda bulunurken, nesne sınırları üzerinde negatif etki oluşturmaktadır. AKAZE tarafından kullanılan doğrusal olmayan ölçek uzayı ise, hem gürültünün etkisini aza indirmekte hem de nesne sınırlarını koruyabilmektedir. AKAZE kendi içerisinde Hızlı Tanımlanmış Difüzyon prosedürünü (Fast Explicit Diffusion-FED) kullanarak doğrusal olmayan ölçek uzayını oluşturmaktadır.

Artan ölçek uzayları boyunca görüntünün parlaklık değeri doğrusal olmayan difüzyon yolu ile modellenebilir ve denklem (1) ile gösterildiği gibi ifade edilebilir.

$$\frac{\partial L}{\partial t} = div(c(x,y,t).\nabla I) \quad (1)$$

Formülde verilen *div* ve ∇ sırasıyla, diverjans ve türev işlemlerini gösterirken, I ise görüntünün parlaklık değerlerini temsil etmektedir. c ile gösterilen iletkenlik fonksiyonu ise difüzyonun görüntüdeki lokal karakteristiklere göre uygulanabilirliğini garanti etmektedir. t, iletkenlik fonksiyonundaki zamanı ve aynı zamanda ölçek parametresini göstermektedir. İletkenlik fonksiyonu c ise denklem (2)'deki gibi hesaplanmaktadır.

$$c(x,y,t) = g(|\nabla I_\sigma(x,y,t)|) \quad (2)$$

(2) ile verilmiş olan denklemde I_σ ve ∇I_σ görüntünün Gauss yumuşaklaştırılmış halini ve karşılık düşen türevini temsil etmektedir. Denklem (3)'de verilmiş olan ve g_2 ile gösterilen fonksiyon iletkenlik fonksiyonu olarak kullanılmaktadır.

$$g_2 = \frac{1}{1+\frac{|\nabla I_\sigma|^2}{\lambda^2}} \quad (3)$$

λ parametresi fonksiyon tarafından kenar bilgilerinin ortadan kaldırılmasında kullanılır ve değerinin daha büyük seçilmesi kenar bilgisinin daha az tutulacağı anlamını taşır. Çalışmada yazarlar tarafından $|\nabla I_\sigma|$'in histogramındaki ilk %70'lik kısmının λ parametresinin belirlenmesi için kullanılması önerilmiştir.

Bu aşamadan sonra ölçek uzayının *O* oktav ve *S* alt seviye ile oluşturulması gerçekleştirilecektir. *I* ile gösterilen test görüntüsü kullanılarak ölçek uzayındaki $O \times S$ adet görüntü oluşturulacaktır, $I_1 \cdots I_{O \times S}$. Her oktavdaki ilk görüntü bir önceki oktavdaki son görüntünün alt örneklemesi ile elde edilmektedir, $(I_1, I_{1+S}, I_{1+2S} \cdots)$. oktavlardaki diğer görüntülerin üretimi için ise denklem (4) ile verilmiş olan ifadeden faydalanılmaktadır. $G(I, \sigma)$ ifadesi, *I* görüntüsü üzerinde verilmiş olan standart sapma değeri ile beraber bulanıklaştırma işlemini gerçekleştirmektedir.

$$\begin{aligned}
&\forall i, i \in 2 \cdots O \times S: \\
&if\ \big((mod(i,S) \equiv 1)\big)\ then \\
&\ \lambda_i = \lambda_{i-1} \times t_{cp} \\
&I_i = FED(I_{i-1}, C(G(subsample(I_{i-1}), \sigma), \lambda_i), t_i), \\
&else \\
&\ \lambda_i = \lambda_{i-1} \\
&\ I_i = FED(I_{i-1}, C(G(I_{i-1}, \sigma), \lambda_i), t_i)
\end{aligned} \quad (4)$$

İfade de verilmiş olan iletkenlik fonksiyonu *C,* alt örneklenmiş olan görüntü üzerinde (2)'de verilen fonksiyonu uygulamaktadır. *FED* ile gösterilmiş olan fonksiyon ise; *i* ile gösterilen ölçek için tanımlı zaman parametresi olan t_i'yi, bir önceki ölçek görüntüsünün yumuşaklaştırılmış halini ve iletkenlik fonksiyonunun çıkışını parametre olarak almaktadır. O anki görüntü olan I_i için zaman parametresi, denklem (5)'de verildiği gibi ölçek bilgisi *s* ve oktav bilgisi *o'*nun kullanımı ile hesaplanmaktadır.

$$\sigma_i(o,s) = \frac{1}{2}\left(2^{o+s/S}\right)^2, \quad t_i = \frac{1}{2}{\sigma_i}^2 \quad (5)$$

Yukarıdaki ifade de fonksiyon olarak tanımlanan FED işlemi, AKAZE'nin her ölçekteki görüntüleri oluşturmasını sağlamaktadır. FED, tekrarlı kutu filtrelerini kullanarak, Gauss çekirdeğine yakınsamaktadır. Farklı adım ölçülerindeki, τ, *n* adet tanımlı difüzyon adımının *M* adet döngüsü ölçek görüntülerini oluşturmaktadır. AKAZE *M*=1 döngü ve *n* adım kullanarak I_i ile gösterilen ölçek görüntüsünü oluşturur ve *n* farklı adım ölçüsünü bu adımlarla kullanılmak üzere belirler, $\tau_1 \cdots \tau_n$. Her döngü farklı bir adım ölçüsü alabilirken, τ_{max} ile gösterilen izin verilebilen en büyük adım ölçüsünü geçemez. Maksimum adım ölçüsü ise algoritma tarafından 0.25 olarak belirlenmiştir.

O anki ölçek görüntüsü I_i'nin belirlenmesinde kullanılan döngü sayısı *n* karşılık düşen zamana t_i, göre belirlenmektedir. *n* değeri ise denklem (6)'daki ifadenin kullanımı ile hesaplanır.

$$n = \left\lceil -\frac{1}{2} + \frac{1}{2}\sqrt{1 + 12(t_i - t_{i-1})/\tau_{max}} \right\rceil \quad (6)$$

Verilen ifadenin kullanımı ile, FED döngüsünün *j*'inci adımındaki adım ölçüsü ise denklem (7)'den faydalanılarak elde edilmektedir.

$$\tau_j = \frac{3(t_i - t_{i-1})}{n(n+1)\tau_{max}} \times \frac{\tau_{max}}{2cos^2\left(\pi\frac{2j+1}{4n+2}\right)} \quad (7)$$

Değişen adım ölçüleri ile *n* kere tekrarlanan *FED* döngüsü denklem (8)'de verilmektedir. I_i^j, FED'in *j*'inci döngüsünde oluşturulan geçici ölçek görüntüsünü temsil etmektedir. *A* ile gösterilen matris ifadesi ise Weickert (1998)'e göre hazırlanmıştır. *n* adımın sonunda ise I_i ile gösterilen ölçek görüntüsü oluşturulacaktır.

$$I_i^j = \left(I + \tau_j A\left(G(I_{i-1}, \sigma)\right)\right) I_i^{j-1}, \quad j = 1 \cdots n\text{-}1 \quad (8)$$

Doğrusal olmayan ölçek uzayındaki her alt görüntü I_i^j kullanılarak anahtar noktaları elde edilecektir. Görüntülerin üzerinde Hessian Matrisi hesaplanır ve normalize edilmiş ölçek faktörü ile çarpılır. Seçilen faktör değeri, ölçek

uzayındaki görüntülerin her biri için farklı olacaktır. Denklem (9)'da verilen ifade I_i^o ile gösterilen ölçek uzayındaki *o*'uncu oktavdaki görüntü için ölçek faktörünün hesaplanmasını göstermektedir.

$$sf_i = \sigma_i / 2^o \quad (9)$$

O anki görüntü, I_i^o, için oluşturulan Hessian matrisinin (9)'daki ölçek faktörü ile çarpılarak determinantı hesaplanır. Matristeki elemanlardan, değerleri önceden belirtilmiş eşik değerinden büyük olanlar, 3x3 komşuluktaki yerel ekstremum nokta olarak tanımlanır. Ölçek uzayındaki bir önceki determinant görüntüsündeki anahtar noktaları da aynı zamanda maxima'nın belirlenmesinde kullanılır. Daha önceki ölçeklerdeki anahtar noktalarına yakın olan adaylar, anahtar noktası olarak seçilir. Seçilen anahtar noktaları üzerinde yeniden bir filtreleme işlemi bu sefer bir sonraki ölçek görüntüleri de değerlendirilerek uygulanır. Eğer o anki anahtar noktası, sonraki ölçeklerde de daha yüksek bir cevaba sahip ise anahtar noktası olarak belirlenir.

Yukarıda verilen adımların uygulanması ile girişten gelen test görüntüsü olan *I* üzerindeki anahtar noktaları belirlenmektedir. Anahtar noktalarının belirlenmesi aşamasında doğrusal olmayan ölçek uzayı kullanan ve kenar görüntülerini gürültüye oranla daha az yumuşatma yeteneğine sahip AKAZE yöntemi kullanılmıştır. Bir sonraki bölümde ise elde edilmiş anahtar noktaları kullanılarak tanımlayıcıların oluşturulmasından bahsedilecektir.

Tanımlayıcıların Elde Edilmesi ve Sahte Bölgenin İşaretlenmesi

Bu bölümde, görüntü üzerinden elde edilen anahtar noktaları için tanımlayıcı üretimi ve üretilen tanımlayıcılar kullanılarak sahte bölgenin işaretlenmesinden bahsedilecektir.

a) Anahtar noktalarından G-SURF yöntemi ile tanımlayıcıların elde edilmesi

Bir önceki bölümde elde edilmiş anahtar noktaları üzerinde G-SURF tanımlayıcı elde etme algoritması kullanılarak, anahtar noktalarına karşılık düşen tanımlayıcılar elde edilecektir (Alcantarilla vd., 2013b). Gauge koordinatları görüntü işleme ve bilgisayarla görü alanında birçok kullanım alanına sahiptir. Koordinat düzleminin sahip olduğu rotasyon bağımsızlığı, ilgili alandaki kullanım yaygınlığının en önemli sebebidir. G-SURF tanımlayıcıları kenar bilgisini korurken, anahtar noktalarının eşleşme oranını iyileştirme özelliğine sahiptir.

Gauge koordinatları ile görüntüdeki her bir piksel, denklem (10)'da verilen eğim vektörü $\overleftarrow{w}$ ve dikey yönü $\overleftarrow{v}$ ile temsil edilerek, rotasyon bağımsız olarak ifade edilebilir.

$$\overleftarrow{w} = \left(\frac{\partial L}{\partial x}, \frac{\partial L}{\partial y}\right) = \frac{1}{\sqrt{L_x^2 + L_y^2}}\left(L_x, L_y\right) \quad (10)$$

$$\overleftarrow{v} = \left(\frac{\partial L}{\partial y}, -\frac{\partial L}{\partial x}\right) = \frac{1}{\sqrt{L_x^2 + L_y^2}}\left(L_y, -L_x\right)$$

(10) ile verilen ifade de, *L*, *I* ile gösterilen görüntünün 2 boyutlu Gauss çekirdeği $g(x, y, \sigma)$ ile katlanmasıdır. σ değeri ise ölçek parametresidir.

Türevler, farklı büyüklükteki özellikleri yakalayabilmek amacı ile birçok seviyede ve istenilen dereceye kadar alınabilmektedir. Ham görüntü türevleri yalnız Kartezyen koordinat sistemi kullanılarak hesaplanabildiğinden, Gauge türevlerini elde edebilmek için sabit bir eğim yönüne bağlı $\left(L_x, L_y\right)$ yönlü türevleri kullanmaya ihtiyaç vardır. İkinci dereceden gauge türevleri ise denklem (11)'deki ifade yardımı ile hesaplanmaktadır.

$$L_{ww} = \frac{L_x^2 L_{xx} + 2L_x L_{xy} L_y + L_y^2 L_{yy}}{L_x^2 + L_y^2} \quad (11)$$

$$L_{vv} = \frac{L_y^2 L_{xx} - 2L_x L_{xy} L_y + L_x^2 L_{yy}}{L_x^2 + L_y^2}$$

G-SURF tanımlayıcıları, SURF algoritmasındaki birinci türevler yerine (L_x, L_y), ikinci dereceden Gauge türevlerini (L_{ww}, L_{vv}) kullanmaktadır. AKAZE tarafından *s*'inci ölçekte belirlenen anahtar noktası için birinci ve ikinci dereceden Haar Dalgacık cevabı 20*s*x20*s*'lik bir komşuluk bölgesinde hesaplanır, $L_x, L_y, L_{xx}, L_{xy}, L_{yy}$. L_x ve L_y sırası ile, yatay ve dikey yöndeki Haar cevabını temsil etmektedir. 20*s*×20*s* büyüklüğündeki tanımlayıcı çerçevesi, 4x4 adet birbiri ile örtüşmeyen alt bölgeye ayrıştırılır. Her alt bölgede 25 düzgün dağıtılmış örnek nokta için *2s* Haar dalgacığı hesaplanır. Bütün pikseller için Gauge koordinat çerçevesi sabitlenince ((L_x, L_y) hesaplandıktan sonra), $(|L_{ww}|, |L_{vv}|)$ ile gösterilen Gauge değişmezleri elde edilecektir. Sonuç olarak, her bir alt bölge dört elemanlı $d_v = (\sum L_{ww}, \sum L_{vv}, \sum|L_{ww}|, \sum|L_{vv}|)$ ile gösterilen özellik vektörü üretir ve her bir AKAZE anahtar noktası etrafındaki 20s×20s'lik bölgenin kullanımı ile 1x64 büyüklüğündeki G-SURF tanımlayıcısı elde edilir.

Yukarıda detayları verilmiş olan G-SURF tanımlayıcı belirleme algoritmasının kullanımı ile görüntü üzerindeki AKAZE anahtar noktaları için tanımlayıcı vektörler üretilir.

b) Tanımlayıcılar Kullanılarak Sahte Bölgenin Belirlenmesi

Bir önceki bölümde görüntüdeki *m* adet anahtar noktasından G-SURF yöntemi ile 1×64 büyüklüğünde elde edilen tanımlayıcılar *D* ile gösterilen $m \times 64$ boyutlarındaki matrise yerleştirilir, $D = \{d_1, \cdots, d_m\}$. Önerilen yöntem her bir anahtar noktasını kendinden t_d uzaklıktaki diğer anahtar noktaları ile kıyaslamaktadır. Böyle bir kriter koymadaki amaç, yakın bölgelerdeki dokusal benzerlikten kaynaklı hatalı eşleştirmelere engel olmaktır. *i* ile gösterilen anahtar noktasına ait koordinatlar (i_x, i_y) olsun. *j* ile gösterilen anahtar noktası ile *i*'nin kıyaslanabilir olması için denklem (12) ile verilen koşulu sağlaması gerekmektedir.

$$\sqrt{(i_x - j_x)^2 + \left(i_y - j_y\right)^2} \geq t_d \qquad (12)$$

Verilen koşul doğrultusunda her bir nokta kendisinden belirli bir mesafedeki (t_d'den uzak olması koşulu ile) diğer noktalar ile kıyaslanacaktır. Kıyaslamada kullanılan eşik değeri, test görüntüsünün büyüklüğüne bağlı olarak dinamik seçilmektedir. *N* x *M* büyüklüğündeki bir görüntü için, kopyalanıp yapıştırılan bölgelerin birbirlerine olan Öklid mesafesinin en az $t_d = \sqrt{\left(\frac{N}{10}\right)^2 + \left(\frac{M}{10}\right)^2}$ olması beklenmektedir. Görüntünün onda birlik kısmının Öklid uzaklık değeri, kopyalama yapıştırma işleminin anlamlı olabilmesi açısından yeterli olmaktadır.

Tanımlayıcıların kıyaslamasında ise Lowe (2004)'de tanımlı yaklaşımdan faydalanılmıştır. Her bir tanımlayıcının, d_i, kendisine en yakın komşulukları Öklid uzaklığı kullanılarak belirlenir. En yakın iki komşu tanımlayıcı d_k ve d_j ile gösterilsin. Bu iki tanımlayıcı ile d_i arasındaki Öklid mesafelerinin oranı belirli bir eşik değeri *T'den* küçükse, d_i'nin gösterdiği anahtar noktasının d_k'nın tanımladığı anahtar noktası ile eşleştiği varsayılacaktır. Kıyaslamaya ilişkin ifade denklem (13)'de verilmiştir.

$$\frac{|d_k - d_i|}{|d_j - d_i|} < T \qquad (13)$$

Formülde iki tanımlayıcı arasındaki Öklid mesafesi, $|d_k - d_i|$ ile gösterilmektedir. Kullanılan eşik değeri 0.6 olarak belirlenmiştir. Diğer bir kriter olarak ise Öklid mesafesi t_{match}'den büyük olan tanımlayıcılar değerlendirmeye alınmamıştır. (12) ve (13)'deki ifadelerin kullanımı ile her anahtar noktası eğer varsa kendisi ile en benzer diğer bir anahtar noktası ile eşleştirilecektir.

Son olarak ise hatalı eşleşmeleri ortadan kaldırabilmek amacı ile RANSAC (Random

Sample Consensus) algoritmasından faydalanılacaktır (Fischler ve Bolles, 1981). Yöntem, eşleşen anahtar noktaları çiftlerinden rasgele bir küme belirlemekte (en az beş adet eşleşmiş anahtar noktası çiftinin olması beklenmektedir) ve H ile gösterilen ifadesi denklem (14)'te verilen transformasyon matrisine yakınsamaktadır.

$$H\begin{bmatrix}x_i\\y_i\end{bmatrix}=\begin{bmatrix}x_j\\y_j\end{bmatrix} \quad (14)$$

Diğer eşleşen anahtar noktaları, belirlenmiş olan H matrisine göre değerlendirilmektedir. Eşleşen anahtar noktalarının her biri H ile transform edilir ve kendisi ile eşleşen noktaya olan uzaklığı hesaplanır. Eğer aradaki mesafe belirli bir değerden küçükse bu iki noktanın, H matrisine uyum gösterdiğine ve doğru eşleşmeyi temsil ettiğine karar verilir. Aksi takdirde hatalı eşleşme olarak, eşleşme veri kümesinden çıkarılır. Önerilen yöntem tarafından kullanılan uzaklık eşiği 3 olarak seçilmiştir. Başlangıç noktası transform edildiğinde eşleşen anahtar noktası ile arasındaki Öklid mesafesinin 3'ü geçmesi durumunda ilgili noktalar hatalı eşleşme olarak adlandırılmaktadır. Şekil 2'de hatalı eşleştirmelerin ortadan kaldırılması aşamasında, RANSAC yönteminin pozitif etkisi gözükmektedir. Şekil 2(a)'da verilmiş olan orjinal görüntünün değiştirilmiş hali olan Şekil 2(b)'deki sahte görüntü (Ön taraftaki bardağın üzerine etiket yapıştırılmıştır) için elde edilen eşleştirme sonuçları Şekil 2(c)'de gözükmektedir. RANSAC algoritmasının eşleşen noktalar üzerinde uygulanması sonucu üretilen Şekil 2(d)'deki sonuç görüntüsü ise, yöntemin yeterli hata eliminasyonu gerçekleştirdiğini göstermektedir. Arka tarafta yer alan kasenin üzerindeki hatalı eşleşmeler ortadan kaldırılmıştır.



(a)



(b)



(c)



(d)

Şekil 2. (a) Orjinal Görüntü (b)Sahte görüntü (c) RANSAC öncesi (d) RANSAC sonrası

Bu bölümde önerilen yöntemin detaylarından bahsedilmiştir. Girişten alınan I görüntüsü üzerinde öncelikle AKAZE anahtar noktaları belirlenmiş ardından her bir anahtar noktası için tanımlayıcı vektörleri G-SURF algoritmasının kullanımı ile üretilmiştir. Anahtar noktaları kendinden belirli bir mesafe uzaklıktaki anahtar noktaları ile (12) ve (13)'deki ifadelerin yardımı ile eşleştirilmiştir. Eşleştirme sonucundaki hatalı durumlar ise RANSAC algoritmasının kullanımı ile filtrelenmiştir. Bir sonraki bölümde yöntemin kullanımı ile üretilen deneysel sonuçlar verilecektir.

Deneysel Sonuçlar

Bu bölümde elde edilen deneysel sonuçlar MICC-F220 veritabanı üzerinde üretilmiştir (Amerini vd., 2011). Veritabanı 220 adet görüntüden oluşmaktadır. Görüntülerin yarısı orjinal görüntü iken diğer yarısı çeşitli saldırıların uygulanması ile elde edilen sahte görüntülerdir. Veritabanındaki görüntü çözünürlükleri 722×480 ile 800×600 arasında değişmektedir. Sahteciliği oluşturmakta kullanılan bölgeler görüntü genelinin %1.2'si büyüklüğündedir. Veritabanındaki sahte görüntülerin oluşturulmasında kullanılan saldırılar Tablo 1'de verilmiştir. A ile gösterilen saldırı türü, kopyalanan bölgeyi yapıştırmadan önce herhangi bir ekstra işlem uygulamamaktadır. B, C, D ve E ile gösterilen saldırılarda sahte bölge yapıştırılmadan önce sırası ile 10, 20, 30 ve 40°'lik döndürmelere tabi tutulmaktadır. Kopyalanan bölgenin x ve y yönünde farklı ölçeklerde (1.2-1.2, 1.3-1.3, 1.4-1.2) genişletilmesi ile üretilen saldırılar F, G ve H olarak isimlendirilmektedir. I ve J

saldırılarında ise rotasyon ve ölçeklendirme beraber uygulanır.

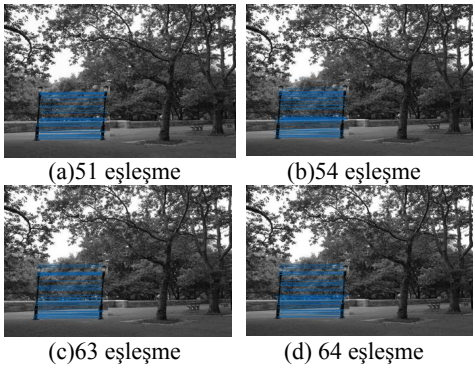
Tablo 1. MICC-F220 veritabanındaki sahte görüntülerin oluşumunda kullanılan yöntemler

Saldırı	θ°	s_x	s_y	Saldırı	θ°	s_x	s_y
A	0	1	1	F	0	1.2	1.2
B	10	1	1	G	0	1.3	1.3
C	20	1	1	H	0	1.4	1.2
D	30	1	1	I	10	1.2	1.2
E	40	1	1	J	20	1.4	1.2

Bölümün geri kalanında verilecek olan sonuçlar üç alt sınıfta toplanmıştır. İlk olarak yöntemin gürültü, sıkıştırma ve bulanıklaştırma saldırılarına karşı dayanıklılık sonuçları verilirken, bir sonraki bölümde rotasyon, ölçeklendirme ve kombine saldırılar durumundaki görsel sonuçlar verilecektir. Son bölümde ise önerilen çalışmanın benzer çalışmalar ile olan kıyaslaması üzerinde durulacaktır.

a) Gürültü Ekleme, Sıkıştırma ve Bulanıklaştırma Saldırılarına Karşı Dayanıklılık Testi

MICC-F220 veritabanından seçilen bazı görüntüler üzerinde gürültü ekleme, sıkıştırma ve bulanıklaştırma saldırıları uygulanması sonucu elde edilen görsel sonuçlar bu bölüm kapsamında verilecektir. Gerçekleştirilen ilk deneyde MICC-F220 veritabanındaki A sınıfında yer alan görüntülerden seçilen bir tanesi üzerinde farklı kalite faktörleri ile JPEG sıkıştırma atağı uygulanmıştır. Sıkıştırma esnasında kalite faktörü (KF) 20, 40, 60 ve 80 seçilerek sahte görüntüler elde edilmiştir. Kalite faktörü 20 iken eşleştirilen anahtar noktası çifti sayısı 51 iken, bu değerin kalite faktörü 80'e yükseldiğinde 64 olduğu Şekil 3'de gözlemlenmektedir. Kalite faktöründeki azalma ile beraber, görüntüdeki kayıpların artması eşleştirme sayısını düşürmektedir. Fakat yüksek sıkıştırma oranlarına (KF=20) rağmen elde edilen eşleştirme sayısı miktarları oldukça yeterli gözükmektedir. Aynı zamanda görsel sonuçlarda hatalı eşleşme ile karşılaşılmamıştır.

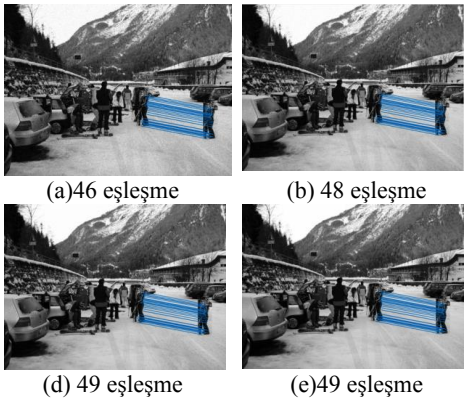


(a)51 eşleşme (b)54 eşleşme

(c)63 eşleşme (d) 64 eşleşme

Şekil 3. JPEG sıkıştırma karşısında dayanıklılık testi (a) KF=20 (b) KF=40 (c) KF=60 (d) KF = 80

Bu bölüm kapsamında gerçekleştirilen bir diğer deneyde ise A sınıfından seçilen sahte görüntü üzerinde gürültü ekleme atağı uygulanmıştır. Farklı Sinyal Gürültü Oranlarında (SGO) uygulanan gürültü miktarlarında (15, 20, 25, 30 ve 35 dB) elde edilen görsel sonuçlar Şekil 4'te verilmiştir. SGO değeri 15 dB iken sahte bölge içerisindeki eşleştirme sayısı 46, eklenen gürültü düştüğünde (35 dB) ise eşleştirme sayısı 51 olmaktadır. Görsel sonuçtan yola çıkarak, yöntemin gürültü ekleme saldırılarına karşı dayanıklı olduğu söylenebilir. Aynı zamanda görsellerde hatalı eşleştirme olmadığı da gözlemlenmektedir.



(a)46 eşleşme (b) 48 eşleşme

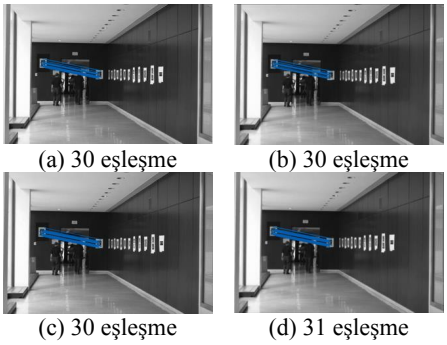
(d) 49 eşleşme (e)49 eşleşme



(e)51 eşleşme

Şekil 4. Gürültü ekleme atağına karşı dayanıklılık testi (a) SGO = 15 dB (b) SGO = 20 dB (c) SGO = 25 dB (d) SGO = 30 dB (e) SGO = 35 dB

Son olarak gerçekleştirilen testte ise yöntemin bulanıklaştırma saldırıları karşısında dayanıklılığı test edilecektir. Seçilen sahte görüntü üzerinde 3×3 ve 5×5 çerçeve büyüklüğünde standart sapma değerleri 0.5 ve 1 olan Gauss bulanıklaştırmaları uygulanmıştır. Şekil 5'de bulanıklaştırma atağı karşısındaki eşleştirme miktarları verilmiştir. Deneysel sonuçlardan da gözlemlenebileceği gibi, yöntem bulanıklaştırma saldırılarındaki çerçeve ve sapma değerlerinden bağımsız olarak yaklaşık eşit sayıda eşleştirme elde etmektedir.



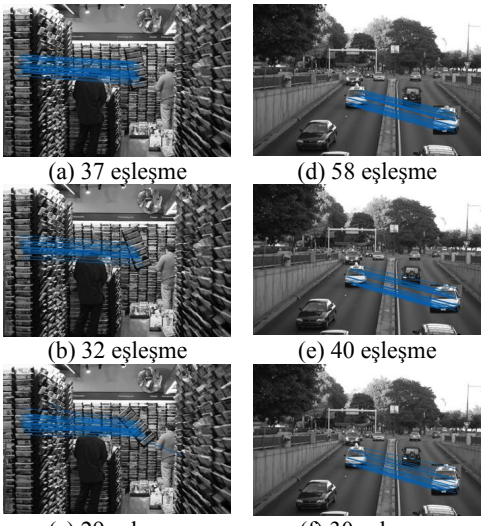
(a) 30 eşleşme (b) 30 eşleşme

(c) 30 eşleşme (d) 31 eşleşme

Şekil 5. Bulanıklaştırma atağı karşısında yöntemin dayanıklılık testi (a) $3 \times 3, \sigma = 0.5$ *(b)* $3 \times 3, \sigma = 1$ *(c)* $5 \times 5, \sigma = 0.5$ *(d)* $5 \times 5, \sigma = 1$

b) Rotasyon, Ölçekleme ve Öteleme Saldırıları Karşısında Dayanıklılık Testi

Yöntemin, transformasyon saldırılarına karşı dayanıklılığını gösterebilmek amacı ile veritabanındaki çeşitli test görüntüleri kullanılmıştır. Kötü niyetli bir kişinin kopyalanan bölgeyi yapıştırmadan önce herhangi bir transformasyona tabi tutması durumunda, yöntemin yine de sahte bölgeyi tespit edebilmesi önemlidir. Rotasyona karşılık dayanıklılık testi için 10, 20 ve 40° döndürme açıları kullanan test görüntülerinden faydalanılmıştır. Şekil 6(a)-6(c) arasında rotasyon saldırıları karşısında eşleştirme sonuçları verilmiştir. Eşleştirme sayıları değerlendirildiğinde, rotasyon açısı arttıkça eşleştirme sayısının azaldığı gözlemlenmektedir.



(a) 37 eşleşme (d) 58 eşleşme

(b) 32 eşleşme (e) 40 eşleşme

(c) 29 eşleşme (f) 30 eşleşme

Şekil 6. Rotasyon ve Ölçekleme saldırılarına karşı dayanıklılık testi (a) 10° (b) 20° (c) 40° (d) x=1.2, y=1.2 (e) x=1.3, y=1.3 (f) x=1.4, y=1.2

Döndürme açısı 40 iken eşleştirme sayısı 29 iken, döndürme açısı 10 derece olduğunda eşleştirme sayısı 37'ye yükselmektedir. Döndürme açısı artsa bile görsel sonuçlarda sahte bölgenin tespit edilebildiği gözlemlenmektedir. Ölçekleme saldırılarına karşı dayanıklılık sonuçlarını gösterebilmek amacı ile farklı ölçekleme seviyeleri kullanılmıştır. Bu bölüm kapsamında gerçekleştirilen bir diğer deneysel sonuçta, ölçekleme saldırılarına karşı dayanıklılık test

edilmiştir. Ölçekleme için kullanılan değerler ilk iki saldırı *x* ve *y* yönünde 1.2 ve 1.3 iken son saldırıda *x* ve *y* yönünde sırası ile 1.4 ve 1.2 şeklindedir. Şekil 6(d)-(f) de verilmiş olan görsel sonuçlardan da gözlemlenebileceği gibi önerilen yöntem ölçekleme saldırılarında sahte bölgeyi tespit edebilmekte ve hatalı eşleştirme yapmamaktadır.

Rotasyon ve ölçekleme dönüşümlerinin beraber kullanıldığı hibrit bir senaryo için elde edilen sonuçlar ise Şekil 7'de verilmiştir. Görsel sonuçtan da gözlemlenebileceği gibi önerilen yöntem hibrit saldırı durumunda dahi sahte bölgede eşleştirme yapabilme yeteneğine sahiptir. Görüntüde yumuşak geçişli bölgeler olmasına rağmen, sonuçlarda yanlış eşleştirme olmamaktadır.



(a) 30 eşleşme (b) 17 eşleşme

Şekil 7. Rotasyon ve Ölçekleme saldırılarına karşı dayanıklılık testi (a) 10°, x=1.2, y=1.2 (b) 20°, x=1.4, y=1.2

Bölüm kapsamında elde edilen sonuçlar, yöntemin çeşitli transformasyon saldırılarında dahi pozitif sonuçlar ürettiğini göstermektedir.

c) Başarım Analizi

Önerilen yöntemin doğrulama performansı ve literatürdeki benzer çalışmalar ile kıyaslaması bu bölüm kapsamında gerçekleştirilecektir. Performansın testi için kullanılacak metrikler aşağıdaki şekilde verilebilir.

- Doğru Pozitif (DP): Orjinal görüntülerin doğru olarak orjinal diye sınıflandırılması.
- Yanlış Pozitif (YP): Orjinal görüntülerin yanlış olarak sahte diye sınıflandırılması.
- Yanlış Negatif (YN): Sahte görüntülerin yanlış olarak orjinal diye sınıflandırılması.

Verilen metriklerin kullanımı ile sınıflama performansını ölçen dört kritere (Duyarlık (D), Seçicilik (S), Doğru Pozitif Oranı (DPO), Yanlış Pozitif Oranı (YPO)) ilişkin ifadeler denklem (15)'te verilmiştir.

$$D = \frac{DP}{DT+YP}\ , S = \frac{DP}{DP+YN} \tag{15}$$

$$DPO = \frac{Sahte\ olarak\ sınıflanan\ sahte\ görüntü\ sayısı}{Toplam\ sahte\ görüntü\ sayısı}$$

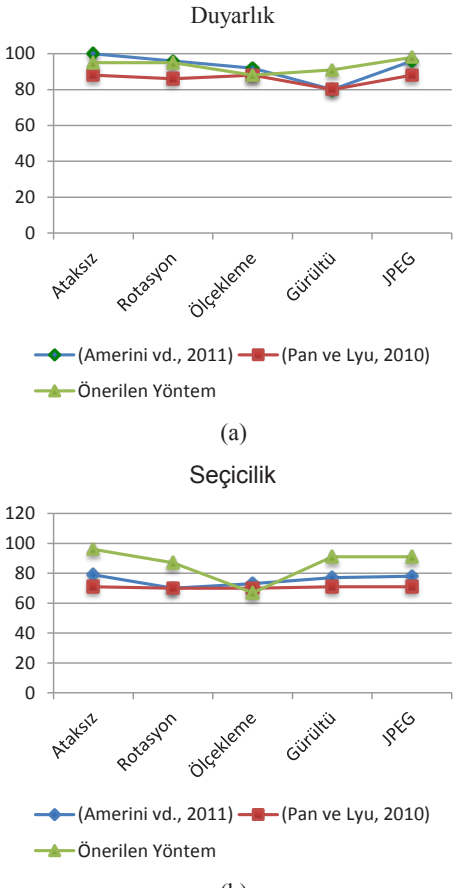
$$YPO = \frac{Orjinal\ olup\ sahte\ sınıflanan\ görüntü\ sayısı}{Orjinal\ görüntü\ sayısı}$$

Duyarlık, sahte olarak belirlenen görüntünün gerçekten sahte olma olasılığını verirken, Seçicilik sahte görüntünün fark edilme olasılığını göstermektedir. *DPO* yöntemin sahte görüntüleri yakalayabilme performansı, *YPO* ise yanlış algılanan orjinal görüntü oranı hakkında bilgi vermektedir. *DPO* oranı en iyi durumda 1'e yakınsarken, *YPO* oranı ise 0'a yakınsamalıdır.

Performans analizi için gerçekleştirilen ilk testte, veritabanındaki çeşitli saldırılara maruz kalmış sahte görüntüler ve yine veritabanında yer alan 110 adet orjinal görüntü kullanılmıştır. Fakat veritabanında yer alan saldırılar içerisinde JPEG sıkıştırma, bulanıklaştırma ve gürültü ekleme saldırıları olmadığı için, veritabanındaki sahte görüntüler üzerinde bu saldırılar tarafımızca uygulanmıştır. Gürültü ekleme için 25 dB SGO'ya sahip Beyaz Gauss gürültüsü, bulanıklaştırma için 5×5 çerçeve ile standart sapması 0.5 olan Gauss çerçevesi, JPEG sıkıştırma için ise KF=70 sahte görüntülerin üretiminde kullanılmıştır. Şekil 8'de literatürde var olan önemli iki çalışma ile Duyarlık ve Seçicilik açısından kıyaslama sonuçları verilmiştir.

Şekil 8(a)'daki Duyarlık kıyaslamasında, yöntemin Gürültü ekleme ve JPEG sıkıştırma saldırılarında diğer yöntemleri geride bıraktığı

gözlemlenmektedir. Pan ve Lyu(2010)'daki çalışma ile kıyaslayınca tüm durumlarda daha yüksek duyarlık oranı elde edilirken, Amerini (2011)'deki çalışma ile JPEG sıkıştırma ve Gürültü ekleme saldırıları dışındaki durumlarda denk gözükmektedir. Yöntem, Ölçekleme atağında Amerini (2011)'deki çalışmaya kıyasla biraz daha düşük sonuçlar üretmektedir. Böyle bir performans kaybındaki en önemli sebep, anahtar noktası çıkarma esnasında kullanılan AKAZE yöntemidir. AKAZE, SIFT anahtar noktası elde etme yöntemi ile kıyaslanınca, ölçekleme durumunda daha düşük performans gösteren bir algoritmadır. Bu nedenle de çalışmanın ölçekleme atakları karşısındaki başarısı, Amerini (2011)'e göre daha düşük çıkmıştır. Şekil 8(b) değerlendirildiğinde ise yöntemin diğer yöntemlere kıyasla daha üstün sonuçlar verdiği gözlemlenmektedir. Rotasyon, Gürültü ekleme ve JPEG sıkıştırma atakları için yöntemin Seçicilik değerleri daha yüksek iken Ölçekleme atağında Amerini (2011)'e göre daha düşük sonuçlar elde edilmiştir. Ölçekleme atağındaki problem, duyarlık parametresinde olduğu gibi burada da gözlemlenmektedir. AKAZE anahtar çıkarma yöntemi, özellikle yeniden ölçekleme durumlarında SIFT yöntemine göre, kopyalanıp yapıştırılan bölge de daha az anahtar noktası tespit edebilmektedir. Anahtar noktasının daha az sayıda tespit edilmesinden dolayı ise, tanımlayıcı üretme algoritmasının (Gauge-SURF tanımlayıcıları) etkinliği ölçekleme ataklarında önemini yitirmektedir.



Şekil 8. Yöntemlerin Duyarlık ve Seçicilik açısından kıyaslaması

Performans kıyaslaması için gerçekleştirilen son deneyde, yöntem benzer çalışmalar ile *DPO* ve *YPO* açısından değerlendirilmiştir. Tablo 2'de yöntemin benzer çalışmalar ile iki metrik açısından kıyaslama sonuçları verilmiştir. Sonuçlar değerlendirildiğinde, önerilen çalışmanın her iki metrik açısından da diğer yöntemlere göre daha üstün sonuçlar verdiği gözlemlenmektedir. Amerini (2011)'deki çalışmanın DPO oranı daha yüksek olmasına rağmen, YPO oranının da yüksek olması önerilen yöntemi daha üstün kılmaktadır.

Tablo 2. Yöntemlerin tespit doğruluğu açısından kıyaslaması

Yöntem	DPO (%)	YPO(%)
(Fridrich vd., 2003)	89	84
(Popescu ve Farid, 2004)	87	86
(Pan ve Lyu, 2010)	89.96	1.25
(Amerini vd., 2011)	100	8
(Li vd., 2014)	70.91	17.27
(Cozzolino vd., 2015)	84.55	17.27
(Mishra vd., 2013)	73.64	3.64
Yöntem	95.2	2.8

Değerlendirme

Görüntülerde kopyala yapıştır sahteciliğinin tespiti alanında son yıllarda önemli çalışmalar gerçekleştirilmektedir. Var olan çalışmalar, tanımlı veritabanları üzerinde doğrulama performansını iyileştirebilme amacı ile farklı teknikler kullanmaktadır. Çalışma kapsamında doğrusal olmayan ölçek uzayından faydalanan AKAZE görüntülerden anahtar çıkarımında kullanılırken, anahtar noktalarından tanımlayıcı vektörlerin elde edilmesi aşamasında G-SURF yönteminden faydalanılmıştır. G-SURF tanımlayıcı elde etme algoritması da, AKAZE'ye benzer şekilde kenar bilgisini korurken gürültü bilgisini tanımlayıcı üretimi esnasında baskılamaktadır. Yanlış eşleştirmelerin eliminasyonu aşamasında ise RANSAC algoritmasından faydalanılmıştır. MICC-F220 veritabanı üzerinde gerçekleştirilen deneysel sonuçlarda yöntemin DPO ve YPO açısından literatürdeki benzer çalışmalara kıyasla daha iyi sonuçlar ürettiği gözlemlenmiştir. Seçicilik ve Duyarlık metrikleri üzerinde yapılan testlerde ise bu alandaki önemli çalışmalar olan Pan ve Lyu (2010) ve Amerini vd. (2011)'e göre özellikle JPEG sıkıştırma ve bulanıklaştırma saldırılarında, yöntem daha pozitif sonuçlar vermektedir.

İleride yapılması planlanan çalışmalarda, yöntemin Seçicilik ve Duyarlık değerlerini iyileştirebilecek şekilde, bölütleme tabanlı yöntemlerden faydalanılması ve doku analizine bağlı anahtar noktası çıkarma algoritmasının dinamik olarak belirlenmesi düşünülmektedir. Ayrıca, AKAZE anahtar noktası elde etme algoritmasının yeniden ölçeklendirme durumlarındaki performansını iyileştirebilmek amacı ile, doğrusal olmayan ölçek uzaylarında kullanılan bulanıklaştırma parametresinin adaptif olarak belirlenmesi düşünülmektedir.

Kaynaklar

Alcantarilla, P. F., Bartoli, A., Davison, A. J. , (2012). KAZE Features, European Conference on Computer Vision (ECCV), Fiorenze, Italya.

Alcantarilla, P. F., Nuevo, J., Bartoli, A., (2013a). Fast Explicit Diffusion for Accelerated Features in Nonlinear Scale Spaces, British Machine Vision Conference (BMVC), Bristol, İngiltere.

Alcantarilla, P. F., Bergasa, L. M., Davison, A. J., (2013b). Gauge-SURF descriptors, Image and Vision Computing, 31, 103-116.

Amerini, I., Ballan, L., Caldelli, R., Bimbo, A. Del., Serra, G., (2011). A sift-based forensic method for copy–move attack detection and transformation recovery", IEEE Ttans. Inf. Forensics Secur., 6, 1099–1110.

Amerini, I., Ballan, L., Caldelli, R., Bimbo, A. Del. , Tongo, L. Del, Serra, G., (2013). Copy- move forgery detection and localization by means of robust clustering with J-linkage, Signal Process. Image Commun., 28, 659–669.

Bayram, S., Sencar, H. T., Memon, N., (2009). An efficient and robust method for detecting copy-move forgery, Proceedings of IEEE International Conference on Acoustics, Speech and Signal Processing, 1053–1056.

Christlein, V., Riess, C., Jordan, J., Riess, C., Angelopoulou, E., (2012). An evaluation of popular copy-move forgery detection approaches, *IEEE TIFS*, 7(6), 2012.

Cozzolino, D., Poggi, G., Verdoliva, L., (2015). Efficient dense-field copy- move forgery detection, *IEEE TIFS*, 10(11), 2015.

Farukh, M., Anand, V., Keskar, A. G., (2014). Copy-move Image Forgery Detection Using an Efficient and Robust Method Combining Un-decimated Wavelet Transform and Scale Invariant Feature Transform", AASRI Procedia, 9, 84–91.

Fischler, M.A., Bolles, R.C., (1981). Random sample consensus: a paradigm for model fitting with applications to image analysis and automated cartography, Commun ACM, 24, 381-395.

Fridrich, J., Soukal, D., Luka´s, J., (2003). Detection of copy-move forgery in digital images, Proceedings of DFRWS 2003, Cleveland, OH, USA.

Hu, H., Zhang, Y., Shao, C., Ju, Q., (2014). Orthogonal moments based on exponent functions: exponent-Fourier moments, Pattern Recognit, 47, 2596–2606.

İmamoğlu, M. B., Ulutas, G., Ulutas, M., (2013). Detection of Copy-Move Forgery Using Krawtchouk Moment, in: 8th International Conference on Electrical and Electronics Engineering (ELECO), 311–314.

Ketenci, S., Ulutas, G., (2013). Copy-move forgery detection in images via 2D-Fourier Transform, 36th Int. Conf. Telecommun. Signal Process, 813-816.

Li, L., Li, S., Wang, J., (2012). Copy-move forgery detection based on PHT, Proceeding World Congr. Inf. Commun. Technol, WICT, 1061–1065.

Li, J., Li, X., Yang, B., Sun, X., (2014). Segmentation-based Image Copy-move Forgery Detection Scheme. IEEE Trans. Inf. Forensics Secur. 6013, 1–12.

Lowe, D. G., (2004). Distinctive image features from scale-invariant key- points, Int. J. Comput. Vision, 60(2), 91–110.

Mishra, P., Mishra, N., Sharma, S., Patel, R., (2013). Region duplication forgery detection technique based on SURF and HAC, Sci. World J., Article ID 267691, 1-8.

Pan, X., Lyu, S., (2010). Region duplication detection using image feature matching, IEEE Trans. Inf. Forensics Secur, 5, 857-867.

Popescu, A.C., Farid, H., (2004). Exposing digital forgeries by detecting duplicated image regions,TR2004–515, 1–11, 2004.

Ryu, S.-J., Lee, M.-J., Lee, H.-K., (2010). Detection of copy-rotate-move forgery using Zernike moments, Proceedings of the 12th international conference on information hiding, 51-65, Canada.

Wang, X.-Y., Li, S., Liu, Y.-N., Niu, Y., Yang, H.-Y., Zhou, Z., (2016). A new keypoint-based copy-move forgery detection for small smooth regions, Multimed Tools Appl, 1-16.

Weickert, J., Romeny, B.H., Viergever, M. A., (1998). Efficient and reliable schemes for nonlinear diffusion filtering, IEEE Trans. Image Processing, 7(3), 398–410.

Wu, Q., Wang, S., Zhang, X., (2010). Detection of image region-duplication with rotation and scaling tolerance, Second International Conference ICCCI., 100–108.

Zhao, J., Guo, J., (2013). Passive forensics for copy-move image forgery using a method based on DCT and SVD, Forensic Sci. Int., 233, 158–166.

A new copy-move forgery detection method based on AKAZE and G-SURF

Extended abstract

Copy move forgery, one of the most common type of image forgeries, copies a portion on the image and pastes it onto another region on the same image. Main purposes of this forgery type are either replicate or conceal an object in the image. Copy move forgery detection methods can be classified into two groups: Block based and Keypoint based methods. Keypoint based methods have gained popularity lately because they can detect forged regions faster. Two of the most important problems of these techniques are, linear scale space used in creating scale images and blurring whole image without preserving edges, which feature extraction methods rely on. In this work, we used both AKAZE keypoint extraction method, utilizing non-linear scale space to construct scale images and G-SURF descriptor extraction algorithm, relying edge information during the descriptor construction. The method also uses RANSAC algorithm to eliminate false matches.

AKAZE is a keypoint extraction and descriptor construction algorithm using non-linear scale space. Keypoint extraction methods in the literature construct scale space of an image by using approximation of Gaussian. Main disadvantage of these methods is they do not respect the natural boundaries of objects in the image. These algorithms apply smoothing operation on image diminishing both noise and edge information at the same time. Thus keypoint information on the edge regions of the image cannot be preserved by these methods. However, AKAZE constructs non-linear scale space of the image and applies adaptive blurring operation on image.

G-SURF descriptor extraction algorithm use second order multi-scale gauge derivatives to construct descriptors and it also utilizes per pixel information to make blurring adaptive according to the content of the image. In this work we used Gauge-SURF descriptor with 20s×20s square grid.

RANSAC is also used by the method to eliminate false matches. This algorithm determines a randomly created set from matched keypoints and it constructs a transformation matrix by using this set. This transformation matrix evaluates other matched keypoints and some of them are indicated as outlier. This procedure can be applied number of times to approximate real solution.

Proposed method extracts keypoints from the test image using AKAZE keypoint extraction algorithm and it then constructs descriptors for each keypoint using G-SURF descriptor extraction algorithm. Matching keypoints are determined after descriptors are extracted. The method uses k-nn to determine the best match for each keypoint. RANSAC algorithm is applied on the matched keypoints to eliminate false matches as the last step.

MICC-F220 database is used to evaluate and to compare the results of the method. The database consists of 110 forged and 110 original images. Experiments indicate that the method has improved True Positive Rate (TPR) with reduced False Positive Rate (FPR) compared to similar works reported in the literature. The method gives better results when both TPR and FPR are considered together.

The results also indicate that the method has higher recall rates under various attacks. Precision values are also better than the similar works when JPEG compression and Gaussian blurring attacks are considered. However, the method gives worse results when scaling attack is considered. AKAZE detects less keypoints on the pasted regions compared to SIFT method when rescaling attack is applied before pasting operation. Thus, the method cannot detect some keypoints on the forged regions when compared to the method in (Amerini et al., 2011). Usage of Gauge-SURF descriptor becomes meaningless due to the artefacts of keypoint extraction method.

We plan to improve the method with segmentation algorithms in the future. Test image can be segmented into regions depending on colour or pattern information and similarity can be tested among regions to improve the precision of the method. We also aim to improve AKAZE keypoint extraction method to make it more robust against scaling attacks. Blurring parameter, which is used during scale space construction, can be adaptively chosen according to the characteristics of the current test image.

Keywords: *— Image forgery, AKAZE, GSurf, Copy Move Forgery, RANSAC.*

mühendislikdergi

