Kırılgan Filigranların Değişim Bölgesi Belirleme Çözünürlüğünü Artırmak İçin Alt-Blok Yaklaşım Tekniği

Metin ERTÜRKLER, Yetkin TATAR
Fırat Üniversitesi, Bilgisayar Mühendisliği Bölümü
23119, ELAZIĞ

ÖZET

Bu makalede, sayısal imgelerin aslıyla aynılığını doğrulamak için hem saldırılara karşı güvenilir hem de imge çözünürlüğünden bağımsız olarak yüksek doğrulukta değişim bölgesi belirleme niteliğine sahip bir kırılgan filigranlama tekniği sunulmuştur. Önerilen teknikte alt bloklama yapısı olarak adlandırılan bir bölmeleme yapısı, bu yapı içerisinde oluşturulan bir bağımlılık düzeni ve bu bağımlılık düzenini kullanan bir doğrulama algoritması geliştirilmiştir. Ayrıca önerilen teknikte iki ayrı sayısal imza algoritmasının birlikte kullanılmasıyla, tekniğin güvenirliğinin ve değişim bölgesi belirleme doğruluğunun birlikte geliştirilebilmesi sağlanmıştır.

Anahtar Kelimeler: Sayısal filigranlama, aslıyla aynılığı doğrulama, değişim bölgesi belirleme.

Sub-Block Approach Technique for Improving the Localization Resolution of the Fragile Watermarks

ABSTRACT

In this paper, a fragile watermarking technique having both secure against attacks and high accuracy determination of tampered region independent from image resolution was presented for image authentication. In the proposed technique, a dividing structure named "sub-block structure", a dependency order constituted on this structure and an algorithm employing this dependency order were developed. Furthermore, a superior trade-off between security and tamper localization of the technique was provided by means of using two different signature algorithms together.

Key Words: Digital watermarking, authentication, localization resolution

1. GİRİŞ

Sayısal imgelerin analog imgelere göre kolaylıkla kopyalanması, dağıtılması, üzerinde değişim yapılması ve kullanımla eskimemesi gibi birçok avantaja sahip olması giderek daha çok tercih edilmelerini sağlamıştır. Ancak, sayısal imgeler analog imgeler gibi özgün bir negatife sahip değillerdir. Bu yüzden, sayısal imgelerin imge işleme programları vasıtasıyla değiştirilmesi, bütünlüğünün bozulması, telif haklarının ihlal edilmesi gibi durumlarda imgenin aslıyla aynılığının doğrulanması veya imge sahibinin telif haklarının korunması mümkün değildir.

Sayısal imgelerin aslıyla aynılığının doğrulanması veya telif haklarının korunması için, son yıllarda üzerinde oldukça yoğun çalışılan alanlardan biride Sayısal Filigranlama'dır (1). Sayısal Filigranlama, özgün veriye ilişkin bilgiyi (*filigran*), özgün verinin algılanabilir kalitesini bozmadan doğrudan doğruya özgün veri içerisine gömen ve gerektiğinde gömülen bilgiyi özgün veri içerisinden geri çıkartabilen bir teknik olarak tanımlanır. Sayısal filigranlar gürbüz, kırılgan ve yarı-kırılgan olarak sınıflandırılabilir. Gürbüz filigranlar genellikle telif haklarının korunması, sahipliğin teyit edilmesi ve DVD gibi kopya koruma uygulamalarında sıkça kullanılırlar (2,3). Kırılgan filigranlar ise imge üzerindeki en küçük değişimi bile tespit etmek için tasarlanır ve aslıyla aynılığı doğrulama uygulamalarında kullanılırlar (4-9). Gürbüz ve kırılgan filigranların yanı sıra, imge içerisindeki bir objenin silinmesi gibi içeriği değiştiren saldırılara karşı kırılgan, fakat sıkıştırma gibi içeriği değiştirmeyen saldırılara karşı dayanıklı olan filigranlar ise yarı-kırılgan filigranlar olarak tanımlanır (10,11).

Bu makalede kırılgan filigranlar üzerine odaklanılmıştır. Kırılgan bir filigranlama tekniği, imgenin aslıyla aynılığını doğrulamanın yanı sıra değişim yapılan bölgeyi belirleyebilme niteliğine de sahip olmalıdır. Bu niteliği gerçekleştirebilmek için imgenin bloklara bölünmesi ve her bir bloğun en az önemli bit (EÖB) düzlemi içerisine bloğa ait sayısal bir imzanın gömülmesi önerilmiştir (4). Ancak bu tekniğin Vektör Nicemlemeli Taklit Saldırısına (VNTS) karşı güvenilir olmadığı kanıtlanmıştır (5).

VNTS'yi önlemek için bloklar içerisine blok indisinin eklenmesi, blok boyutlarının büyütülmesi, filigran olarak daha karmaşık logoların kullanılması öneril-

Digital Object Identifier 10.2339/2008.11.1.57-64

miştir (5). Ancak bu öneriler saldırı yapılmasını engelleyememiş, sadece saldırı yapılmasını zorlaştırmıştır (5). Alternatif bir çözüm olarak her bir imgeye ait benzersiz bir indisin kullanılması önerilmiştir (6,7). Bu çözüm VNTS'nin yapılmasını tamamıyla önlemektedir. Ancak her bir imgeye ait indisin imgenin doğrulanmasında da kullanılacak olması, imge veritabanları için yönetim zorluğu oluşturmaktadır. Bu problemi çözmek için ise imge indisinin, imge içerisinden çıkarılması önerilmiştir (6,7). Ancak imge üzerinde bir değişim yapılması sonucunda yanlış imge indisinin çıkarılması, tüm imge bloklarının doğrulanamamasına neden olarak önerilen tekniklerin değişim bölgesi belirleme niteliğini yok etmektedir.

VNTS'ye karşı tam bir güvenlik sağlarken aynı zamanda değişim bölgesini belirleyebilmek için, bloksal bağımlılığın kullanılması önerilmiştir (5,8). Ancak bloksal bağımlılık yapısında, bir bloktaki bozulma, iki bloğun birden doğrulanamamasına neden olarak değişim bölgesi belirleme doğruluğunu azaltmaktadır.

Literatürde hem saldırılara karşı güvenilir hem de değişim bölgesi belirleyebilme niteliğine sahip diğer bir teknik Çelik ve diğ. (9) tarafından önerilmiştir. Ancak Sıradüzensel Filigranlama Tekniği (SFT) olarak adlandırılan bu tekniğin değişim bölgesi belirleme doğruluğu imge çözünürlüğüne ve kullanılan sayısal imza algoritmasının bit uzunluğuna bağımlıdır.

Bu makalede, yüksek doğrulukta değişim bölgesi belirleme niteliğine sahip bir kırılgan filigranlama tekniği önerilmiştir. Önerilen teknikte, imgenin tüm piksellerinden hesaplanılan sayısal imza ve alt-blok yapısı içerisinde geliştirilen bloksal bağımlılık düzeni saldırılara karşı tam bir güvenlik sağlarken, geliştirilen doğrulama algoritmasıyla bağımlı blok yapısının dezavantajı giderilerek değişim bölgesinin yüksek doğrulukta belirlenebilmesi sağlanmıştır.

2. SIRADÜZENSEL FİLİGRANLAMA TEKNİĞİ

Sıradüzensel Filigranlama Tekniğinde filigranın imgeler içerisine gömülmesi ve çıkarılması sıradüzensel bir yapı kullanılarak gerçekleştirilir. Sıradüzensel yapıda her bir seviye, bir önceki seviyedeki bloğun 2*2 ayrık bloğa bölünmesiyle oluşturulur. 4 seviyeli bir sıradüzen yapısı ve SFT'nin filigranlama yordamı sırasıyla şekil 1 ve 2'de gösterilmiştir. Sıradüzenin en üst seviyesindeki bloğa (imgenin kendisi) ait sayısal imza saldırılara karşı tam bir güvenlik sağlarken, en alt seviyedeki bloklara ait sayısal imzalar değişim bölgesinin belirlenmesinde kullanılırlar.

Her bir seviyedeki bloklara ait sayısal imzalar denklem 1 ve 2 kullanılarak hesaplanır.

for $l = 1:L$

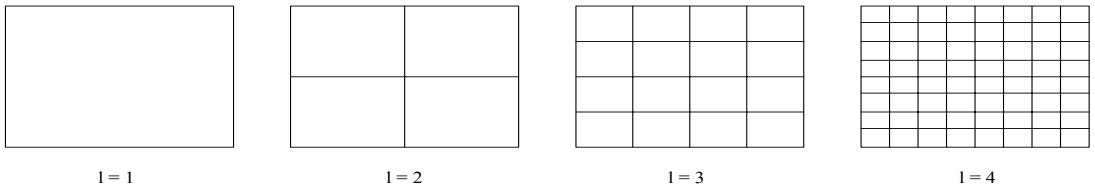
$$h_{i,j}^{l} = H\left(\tilde{I}_{i,j}^{l} \,\|\, [top]\right) \quad (1)$$

$$S_{i,j}^{l} = E\left(h_{i,j}^{l}, K_E\right) \quad (2)$$

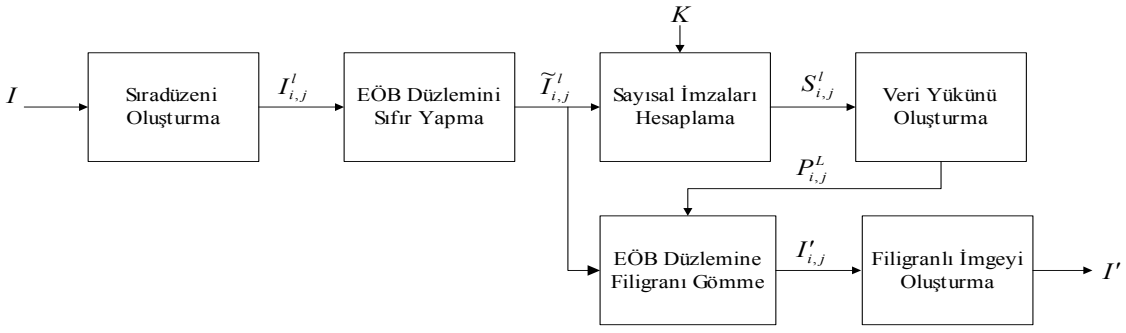
end

Burada i, j, bloğun uzaysal konumunu; l, bloğun ait olduğu sıradüzensel seviyeyi; L, toplam seviyeyi; $\tilde{I}_{i,j}^{l}$, EÖB düzlemi sıfıra eşitlenmiş bloğu; H, özüt fonksiyonunu; h, özüt değerini; E, kriptolama algoritmasını; K_E, kriptolama anahtarını ve S, sayısal imzayı tanımlamaktadır. Sıradüzenin en alt seviyesindeki bloklar, hem kendi bloklarına ait sayısal imzaları hem de üst seviyelerdeki blokların sayısal imzasını taşırlar. Her bir bloğun taşıdığı veri yükü yaklaşık olarak denklem 3'deki gibi hesaplanır.

$$P \cong \frac{4|S|}{3} \quad (3)$$



Şekil 1. Sıradüzensel 4 seviyeli blok yapısı



Şekil 2. SFT'nin filigranlama yordamı

Burada $|S|$ sayısal imzanın bit uzunluğunu göstermektedir. Sıradüzensel yapının en alt seviyesindeki blok büyüklüğü veri yüküne eşit veya daha büyük olmalıdır.

SFT'nin doğrulama yordamında her bir seviyedeki bloklara ait sayısal imzalar $\hat{S}_{i,j}^{l}$, denklem 4 kullanılarak çözülür ve elde edilen özüt değeri, bloğun yeniden hesaplanılan özüt değeri ile karşılaştırılır. Özüt değerlerinin eşleşmesi bloğun aslıyla aynılığını doğrularken, eşleşmeyen blok özüt değerleri bloğun değiştirildiğini gösterir.

for $l = 1:L$

$$\hat{h}_{i,j}^{l} = D\left(\hat{S}_{i,j}^{l}, K_D\right) \quad (4)$$

end

Burada D kripto çözme algoritmasını ve K_D kripto çözme anahtarını tanımlamaktadır.

SFT'nin önemli bir problemi imge sıradüzenin üst seviyelerinde bir alt seviyeye bölünemediğinde ortaya çıkmaktadır. Örneğin 1200*1600 piksellik uzaysal çözünürlüğe sahip bir imge sıradüzen içerisinde 5. seviyede 75*100 piksellik bloklara kadar bölünebilmektedir. Dolayısıyla bir bitlik bir bozulma 7500 pikselin doğrulanamamasına neden olarak tekniğin değişim bölgesi belirleme doğruluğunu oldukça azaltmaktadır. SFT'deki diğer bir problem ise güvenlik seviyesini artırmak için daha uzun bit çıkışına sahip daha güvenilir sayısal imza algoritmaları kullanılması durumunda ortaya çıkmaktadır. Bu kullanım tekniğin güvenirlik seviyesini artırırken, en alt seviyedeki blok büyüklüğünü de artırarak tekniğin değişim bölgesi belirleme doğruluğunu oldukça azaltmaktadır. Sayısal imza algoritmasının bit uzunluğu ile en alt seviyedeki blok büyüklüğü arasındaki ilişki tablo 1'de verilmiştir.

Tablo 1. SFT'de bit uzunluğu ile blok büyüklüğü arasındaki ilişki

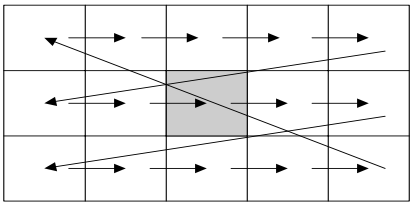
Sayısal İmza Algoritması	Bit uzunluğu	Minimum Blok Büyüklüğü (piksel)
MAC	64	≅ 86
DSA	320	≅ 427
RSA	1024	≅ 1366
RSA	2048	≅ 2731

3. HBC2 FİLİGRANLAMA TEKNİĞİ

Barreto ve diğ (8), HBC2 *(Hash Block Chaining Version 2)* olarak adlandırdıkları bloksal bağımlılığın kullanıldığı diğer bir kırılgan filigranlama tekniği önermişlerdir. Bu teknikte her bir blok kendisinden önceki blok ile şekil 3'deki gibi bağımlı hale getirilmiştir. HBC2 Filigranlama Tekniği'nde her bir blok özütü; doğrulanacak olan blok içeriği, komşu bloğun içeriği ve komşu bloğun deterministik olmayan sayısal imzası kullanılarak denklem 5'deki gibi hesaplanır.

$$h_r = H\left(M, N, \tilde{I}_r, \tilde{I}_{r-1}, r, S_{r-1}\right) \quad (5)$$

Burada S_{r-1}, $\tilde{I}_{r-1}$ bloğunun deterministik olmayan sayısal imzasıdır.



Şekil 3. HBC2 filigranlama tekniğinde kullanılan bloksal bağımlılık düzeni

Blok bağımlılığının kurulmasıyla VNTS'ye karşı güvenlik sağlanırken, bir bloktaki bozulma, hem bloğun hem de bağımlı bloğun doğrulanamamasına neden olarak değişim bölgesi belirleme doğruluğunu azaltmaktadır.

4. ÖNERİLEN TEKNİK

Önerilen teknikte alt bloklama yapısı olarak adlandırılan bir bölmeleme yapısı, bu yapı içerisinde geliştirilen bir bağımlılık düzeni ve bu bağımlılık düzenini kullanan yüksek doğrulukta değişim bölgesi belirleme niteliğine sahip bir doğrulama algoritması geliştirilmiştir. Ayrıca önerilen teknikte iki ayrı sayısal imza algoritması birlikte kullanılarak tekniğin değişim bölgesi belirleme doğruluğu ile güvenirliğinin birlikte geliştirilebilmesine imkân sağlanmıştır. Önerilen teknikte güvenlik tüm imgeye ait sayısal imza ve bloklar ile alt bloklar arasında kurulan bağımlılık ile sağlanmaktadır.

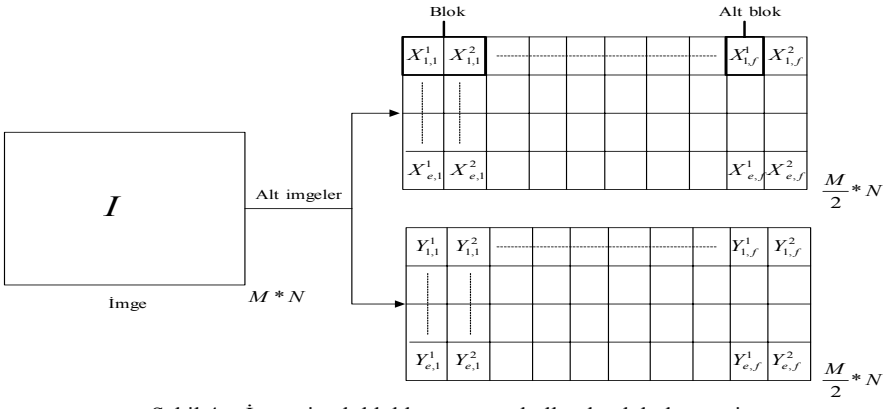
4.1. Filigranlama Yordamı

Önerilen teknik ile sayısal bir imgenin filigranlanması dört aşamada gerçekleştirilmiştir. İlk aşamada, imgenin EÖB düzlemindeki değerler sıfır yapılarak imgeye ait sayısal imza denklem 6 ve 7 kullanılarak hesaplanmıştır. Tüm imgeye ait sayısal imza saldırılara karşı tam bir güvenlik sağlamak amacıyla kullanıldığı için daha uzun bit çıkışına ve daha güvenilir bir yapıya sahip sayısal imza algoritması kullanılmıştır.

$$h = H\left(\tilde{I}\right) \quad (6)$$

$$S = E\left(h, K_E\right) \quad (7)$$

İkinci aşamada $M * N$ piksellik $\tilde{I}$ imgesi $(M/2) * N$ piksellik X ve Y alt imgelerine, her bir alt imge üst üste gelmeyen $r * s$ piksellik $X_{i,j}$ ve $Y_{i,j}$ bloklarına ve her bir blok $r * (s/2)$ piksellik $\left(X_{i,j}^{1}, X_{i,j}^{2}\right)$ ve $\left(Y_{i,j}^{1}, Y_{i,j}^{2}\right)$ gibi iki eşit alt bloğa şekil 4'deki gibi bölünmüştür. Burada $i = \{1,2,...,e\}$ ve $j = \{1,2,...,f\}$, bloğun imge içerisindeki konumunu göstermektedir. Ayrıca $e = M/(2*r)$ ve $f = (N/s)$'dir.



Şekil 4. İmgenin alt bloklama yapısı kullanılarak bölünmesi

Üçüncü aşama bloksal bağımlılıkların kurulmasından ve blok ile bağımlılıklara ait sayısal imzaların hesaplanmasından oluşmaktadır. Buradaki sayısal imzaların hesaplanmasında daha kısa bit çıkışına sahip sayısal imza algoritması kullanılmaktadır. Önerilen teknikte bloksal bağımlılık, X alt imgesindeki her bir $X_{i,j}$ bloğunun Y alt imgesindeki $Y^2_{i,\mathrm{mod}(j-1,f)}$ ve $Y^1_{i,\mathrm{mod}(j+1,f)}$ alt blokları ile; Y alt imgesindeki her bir $Y_{i,j}$ bloğunun da X alt imgesindeki $X^2_{i,\mathrm{mod}(j-1,f)}$ ve $X^1_{i,\mathrm{mod}(j+1,f)}$ alt blokları ile bağımlı hale getirilmesiyle oluşturulmuştur. X alt imgesine ait bloklara ve bağımlılıklara ait sayısal imzalar denklem 8,9 ve 10; Y alt imgesine ait bloklara ve bağımlılıklara ait sayısal imzalar ise denklem 11,12 ve 13 kullanılarak hesaplanır.

$$S^1_{i,j} = E\left(H\left(X_{i,j}\right), K_E\right) \quad (8)$$

$$S^2_{i,j} = E\left(H\left(X_{i,j} + Y^2_{i,\mathrm{mod}(j-1,f)}\right), K_E\right) \quad (9)$$

$$S^3_{i,j} = E\left(H\left(X_{i,j} + Y^1_{i,\mathrm{mod}(j+1,f)}\right), K_E\right) \quad (10)$$

$$S^1_{i,j} = E\left(H\left(Y_{i,j}\right), K_E\right) \quad (11)$$

$$S^2_{i,j} = E\left(H\left(Y_{i,j} + X^2_{i,\mathrm{mod}(j-1,f)}\right), K_E\right) \quad (12)$$

$$S^3_{i,j} = E\left(H\left(Y_{i,j} + X^1_{i,\mathrm{mod}(j+1,f)}\right), K_E\right) \quad (13)$$

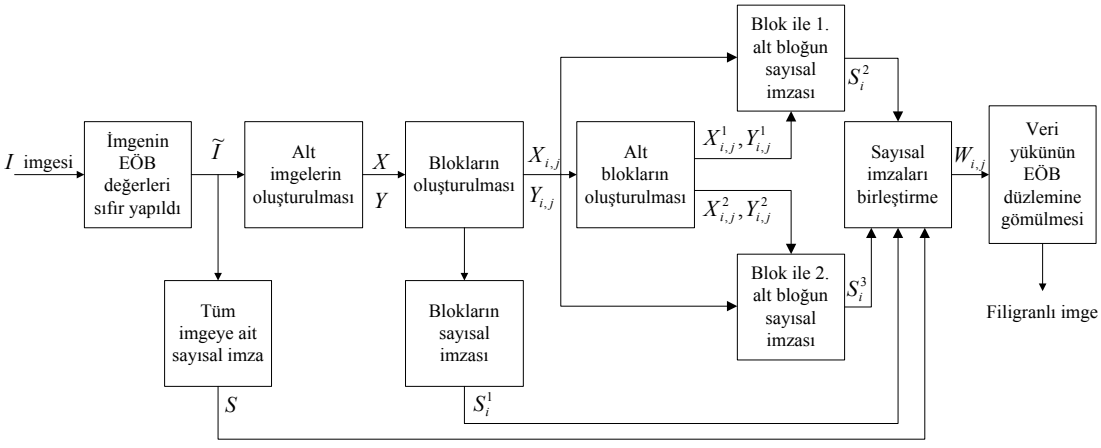
Dördüncü aşamada ise her bir sayısal imzanın bir bölümü denklem 14 kullanılarak birleştirilir ve $W_{i,j}$ filigranı elde edilir. Sayısal imza S'in her blok içerisine sırayla bir biti yerleştirilirken, bloklar ile alt bloklara ait sayısal imzaların kaç bitinin gömüleceği seçilen blok büyüklüğüne bağımlı olarak denklem 15 ve 16 ile belirlenmiştir.

$$W_{i,j} = S\left\|S^1_{i,j}\right\|S^2_{i,j}\left\|S^3_{i,j}\right. \quad (14)$$

$$S_{S^1_{i,j}} = fix\left(\frac{SBB-1}{2}\right) \quad (15)$$

$$S_{S^2_{i,j}} = S_{S^3_{i,j}} = \frac{SBB - 1 - fix\left(\frac{SBB-1}{2}\right)}{2} \quad (16)$$

Burada $\|$, birleştirme işlemini; SBB, seçilen blok büyüklüğünü; $S_{S^1_{i,j}}$, $S_{S^2_{i,j}}$, ve $S_{S^3_{i,j}}$, her bir sayısal imza için seçilen bit sayısını ; fix , sıfıra doğru en yakın tam sayıya yuvarlama işlemini tanımlamaktadır. Son olarak filigranlı imge bloklarını oluşturmak için, her bir bloğun EÖB düzlemi içerisine denklem 14 kullanılarak elde edilen filigran gömülerek filigranlı imge $\tilde{I}$ oluşturulur. Önerilen tekniğin filigranlama yordamı şekil 5'de gösterilmiştir.



Şekil 5. Önerilen tekniğin filigranlama yordamı

4.2. Doğrulama Yordamı

Sayısal imge filigranlandıktan sonra, üzerinde bir değişim yapılıp yapılmadığını belirleyebilmek için ilk olarak tüm imgeye ait sayısal imzanın doğrulanması gerekir. Filigranlama yordamında tüm imgeye ait sayısal imzanın her bir biti her bir bloğun ilk pikselinin EÖB düzlemine gömüldüğü için, ilk olarak her bir blok içerisinden S sayısal imzasına ait bitler okunup birleştirilerek $\acute{S}$ sayısal imzası elde edilir. Daha sonra $\acute{S}$ sayısal imzası denklem 17 kullanılarak çözülür ve $\acute{h}$ özütü bulunur.

$$\acute{h} = D(\acute{S}, K_D) \tag{17}$$

Filigranlı imge üzerinde bir değişim yapılıp yapılmadığını belirleyebilmek için denklem 17 kullanılarak elde edilen özüt ile yeniden hesaplanan imge özütünün eşleşmesi gerekir. Özütlerin eşleşmesi imgede herhangi bir değişimin yapılmadığını, eşleşmemeleri ise bir değişim yapıldığını belirtir. Özütlerin eşleşmemesi durumunda blok büyüklüğünde değişim bölgesini belirleyebilmek için bloklara ait sayısal imzaların doğrulanması gerekir. Bunun için imge alt bloklama yapısı kullanılarak bölmelenir. Daha sonra her bir bloğa ait sayısal imza $S^1_{i,j}$ denklem 18 kullanılarak çözülür ve $\acute{h}^1_{i,j}$ blok özütü elde edilir.

$$\acute{h}^1_{i,j} = D(S^1_{i,j}, K_D) \tag{18}$$

Blok üzerinde bir değişim yapılıp yapılmadığını belirleyebilmek için denklem 18 kullanılarak elde edilen özüt ile yeniden hesaplanan blok özütünün eşleşmesi gerekir. Blok özütlerin eşleşmesi blok üzerinde bir değişimin yapılmadığını, eşleşmemeleri ise blokta bir değişim yapıldığını belirtir.

Blok üzerinde bir değişim belirlenmesi durumunda, değişim bölgesinin daha hassas olarak belirlenebilmesi için bozulmuş bloğun alt bloklarının doğrulanması yapılır. Alt blokların doğrulanması için iki aşamadan oluşan bir algoritma geliştirilmiştir. İlk aşamada muhtemelen bozulmuş alt blokları kendisine komşu seçen blokların aslıyla aynılığının doğrulanması yapılır. İkinci aşamada ise bir önceki aşamada doğrulanan blokların doğrulanması istenen alt bloklar ile oluşturdukları bağımlılıkların doğrulanması yapılır. Geliştirilen doğrulama algoritması herhangi bir $X_{i,j}$ bloğu için aşağıda verilmiştir. $Y_{i,j}$ bloklarının doğrulanması için aşağıda verilen algoritmada X değişkeni yerine Y, Y değişkeni yerine de X yazılmaktadır.

5. DENEYSEL SONUÇLAR

Önerilen tekniğin etkinliğini değerlendirebilmek için deneysel çalışmalarda 1200*1600, 768*1024 ve 480*640 piksellik test imgeleri kullanılmıştır. Deneysel çalışmalarda önerilen tekniğin blok büyüklüğü 8*8 ve alt blok büyüklüğü 8*4 piksel olarak seçilmiştir. Önerilen teknikte tüm imgeye ait sayısal imzanın hesaplanmasında SHA-1 (Secure Hash Algorithm) algoritmasına dayanan 320 bitlik DSA (Digital Signature Algorithm); blok ve blokların alt bloklar ile oluşturdukları bağımlı-

If $E(H(X_{i,j}), K_D)$ % bloğun doğrulanması
  "*Bloğun aslıyla aynılığı doğrulandı*"
Else
  If $E\left(H(Y_{i,mod(j-1,f)}, K_D)\right)$ % $X^1_{i,j}$ alt bloğunu kendisine bağımlı blok seçen bloğun doğrulanması
    If $E(H(Y_{i,mod(j-1,f)} + X^1_{i,j}), K_D)$ % bağımlılığın doğrulanması
      "$X^1_{i,j}$ *alt bloğu doğrulandı*"
    Else
      "$X^1_{i,j}$ *alt bloğu doğrulanmadı*"
    End
  Else
  "$Y_{i,mod(j-1,f)}$ *bloğu doğrulanamadığından* $X^1_{i,j}$ *alt bloğu doğrulanmadı*"
  End
  If $E(H(Y_{i,mod(j+1,f)}), K_D)$ % $X^2_{i,j}$ alt bloğunu kendisine bağımlı blok seçen bloğun doğrulanması
  If $E(H(Y_{i,mod(j+1,f)} + X^2_{i,j}), K_D)$ % bağımlılığın doğrulanması
      "$X^2_{i,j}$ *alt bloğu doğrulandı*"
    Else
      "$X^2_{i,j}$ *alt bloğu doğrulanmadı*"
    End
  Else
  "$Y_{i,mod(j-1,f)}$ *bloğu doğrulanamadığından* $X^2_{i,j}$ *alt bloğu doğrulanmadı*"
  End
End

lıklara ait sayısal imzaların hesaplanmasında MD-5 (Message Digest 5) algoritmasına dayanan 64 bitlik MAC (Message Authentication Code) kullanılmıştır. Aynı kriptografik güvenlik seviyesini sağlamak için SFT'de 320 bitlik DSA, HBC2 filigranlama tekniğinde ise SHA-1 algoritmasına dayanan 288 bitlik deterministik olmayan Schnorr sayısal imza algoritması kullanılmıştır.

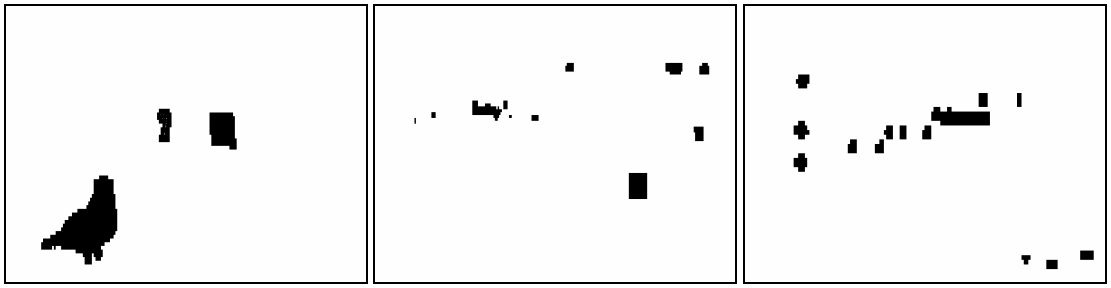
Önerilen teknik ile filigranlanmış test imgeleri şekil 6'da gösterilmiştir. Önerilen tekniğin etkinliğini değerlendirebilmek için şekil 6'da verilen filigranlı imgeler üzerinde değişimler yapılarak önerilen tekniğin doğrulama algoritması çalıştırılmıştır. 1200*1600 piksel çözünürlüğündeki imge üzerinde 18.000, 768*1024 piksel çözünürlüğündeki imge üzerinde 7.879, 480*640 piksel çözünürlüğündeki imge üzerinde ise 3.689 piksel değiştirilerek şekil 7'deki imgeler oluşturulmuştur.

1200*1600 768*1024 480*640

Şekil 6. Önerilen teknik ile filigranlanmış imgeler

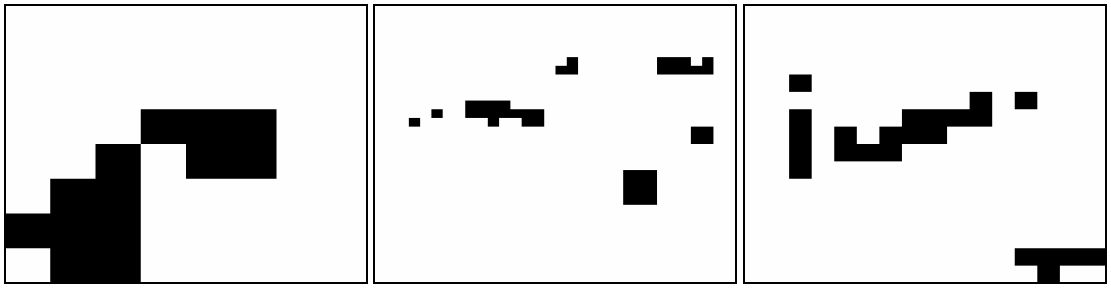
1200*1600 768*1024 480*640

Şekil 7. Değiştirilmiş filigranlı imgeler



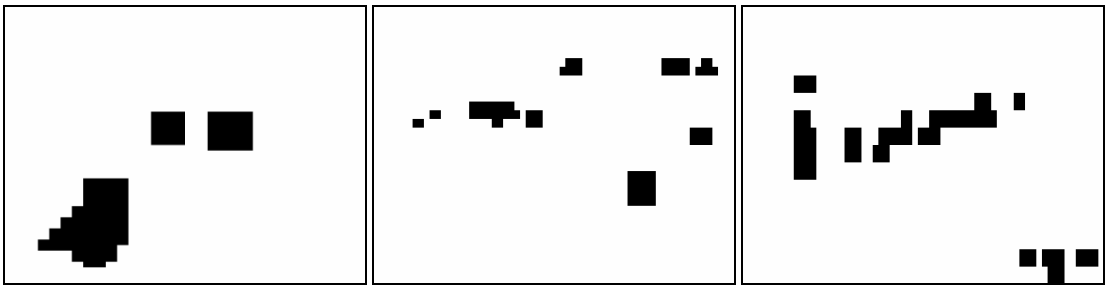
1200*1600 768*1024 480*640

Şekil 8. Önerilen tekniğin doğrulama sonucu



1200*1600 768*1024 480*640

Şekil 9. SFT'nin doğrulama sonucu



1200*1600 768*1024 480*640

Şekil 10. HBC2'nin doğrulama sonucu

Önerilen tekniğin doğrulama algoritması çalıştırılarak elde edilen sonuç ise şekil 8'de gösterilmiştir. Şekil 8'de doğrulanan bölgeler beyaz, doğrulanamayan bölgeler ise siyah ile gösterilmiştir. Doğrulanamayan piksel sayısı ise 1200*1600, 768*1024 ve 480*640 piksellik imgeler için sırasıyla 21.120, 10.912 ve 7.296 piksel olarak bulunmuştur.

Önerilen teknik ile Sıradüzensel Filigranlama Tekniğini karşılaştırabilmek için aynı test imgeleri SFT'nin filigranlama yordamı kullanılarak filigranlanmıştır. SFT'de 320 bitlik DSA sayısal imza algoritması kullanılması durumunda 427 bitlik veri yükü oluşmaktadır. Sıradüzensel yapı kullanılarak 1200*1600 piksellik test imgesi 5. seviyede 75*100 piksellik bloklara, 768*1024 piksellik test imgesi 6.seviyede 24*32 piksellik bloklara, 480*640 piksellik test imgesi ise 5. seviyede 30*40 piksellik bloklara kadar bölmelenmiştir. İmgeler sıradüzensel yapı içerisinde 427 bitlik veri yükünü taşıyabilecek minimum blok büyüklüğüne kadar bölmelenmiştir. SFT ile filigranlanmış imgelere şekil 6'ya uygulanan aynı değişimler uygulandıktan sonra, SFT'nin doğrulama algoritmasının sonucu şekil 9'da gösterilmiştir. Doğrulanamayan piksel sayısı ise 1200*1600, 768*1024 ve 480*640 piksel çözünürlüğündeki imgeler için sırasıyla 97.500, 33.792 ve 27.600 piksel olarak bulunmuştur.

Önerilen teknik ile HBC2 Filigranlama Tekniğini karşılaştırabilmek için aynı test imgeleri HBC2'nin filigranlama yordamı kullanılarak filigranlanmıştır. HBC2'de 288 bitlik Schnorr sayısal imza algoritması kullanılması durumunda minimum blok büyüklüğü 288 piksel büyüklüğünde olmalıdır. Bu yüzden HBC2'de 1200*1600 piksel çözünürlüğündeki test imgesi 15*20 piksellik bloklara, 768*1024 piksellik test imgesi 6 24*16 piksellik bloklara, 480*640 piksellik test imgesi ise 5. seviyede 30*10 piksellik üst üste gelmeyen bloklara bölünmüştür. HBC2 ile filigranlanmış imgelere şekil 6'ya uygulanan aynı değişimler uygulandıktan sonra, HBC2'nin doğrulama algoritmasının sonucu şekil 10'da gösterilmiştir. Doğrulanamayan piksel sayısı ise 1200*1600, 768*1024 ve 480*640 piksellik imgeler için sırasıyla 38.100, 30.720 ve 21.300 piksel olarak bulunmuştur. Tablo 2'de doğrulama sonuçları birlikte verilmiştir.

Tablo 2. Önerilen Teknik, SFT ve HBC2'nin doğrulama sonuçları

Çözünürlük	Değiştirilen Piksel Sayısı	Önerilen Teknik	SFT	HBC2
1200*1600	18.000	21.120	97.500	38.100
768*1024	7.879	10.912	33.792	30.720
480*640	3.689	7.296	27.600	21.300

6. SONUÇLAR

Bağımlı blok yapısını kullanan filigranlama tekniklerinde bir bloktaki bozulma bu bloğa bağımlı diğer bloklarında bozulmasına neden olarak değişim bölgesi belirleme doğruluğunu oldukça azaltmaktadır. Bu makalede alt bloklama yapısı, bu yapı içerisinde oluşturulan bir bağımlılık düzeni ve bu bağımlılık düzenini kullanan bir doğrulama algoritması geliştirilerek, imge çözünürlüğünden bağımsız olarak yüksek doğrulukta değişim bölgesi belirleme niteliğine sahip bir teknik önerilmiştir. Önerilen teknikte tüm imgeye ait sayısal bir imzanın kullanılması ve oluşturulan bağımlı blok yapısı ise saldırılara karşı tam bir güvenlik sağlamaktadır.

7. KAYNAKLAR

1. Cox, I. J., Miller, M. L., Bloom, J. A., "Digital Watermarking", Morgan Kaufmann Publishers, USA, 2002.

2. Cox, I. J., Kilian, J., Leighton, T., Shamoon, T. , "Secure Spread Spectrum Watermarking for multimedia", IEEE Trans. Image Processing, vol.6, pp. 283-301, 1997.

3. Shih, F. Y., Wu, Y. T., "Combinational Image Watermarking in the Spatial and Frequency Domain", Pattern Recognition, vol.36, no.4, pp.969-975, 2003.

4. Wong, P. W., "A Public Key Watermark for Image Verification and Authentication", Proc. IEEE Int. Conf. Image Processing, pp.425-429, 1998.

5. Holliman, M. Memon, N., "Counterfeiting Attack on Oblivious Blockwise Independent Invisible

Watermarking Schemes", IEEE Trans. On Image Processing, vol.9, pp. 432- 441, 2000.

6. Wong, P. W., Memon, N., "Secret and Public Key Authentication Watermarking Schemes that Resist Vector Quantization Attack", Proc. SPIE, 3971(40), 2000.
7. Fridrich, J., Goljan, M., Baldoza, A. C., "New Fragile Authentication Waternark for Images", IEEE Int. Conf. Image Processing, 10-13, 2000.
8. Barreto, P. S. L. M., Kim, H. Y., Rijmen, V., "Toward Secure Public Key Blockwise Fragile Authentication Watermarking ", IEE Proceedings Vision, Image and Signal Processing, vol. 149(2), 57-62, 2002.
9. Celik, M. U., Sharma, G.,Saber, E.,Tekalp, A.M., "Hierarchical Watermarking for Secure Image Authentication With Localization",IEEE Trans. On Image Processing, vol.11 no.6, 585-595,2002.
10. Kundur, D., Hatzinakos, D., "Digital Watermarking for Telltale Tamper Proofing and Authentication", Proceedings of the IEEE Special Issue on Identification and Protection of Multimedia Information, vol. 87, no. 7, pp. 1167-1180, 1999.
11. Eggers, J. J., Girod, B. "Blind Watermarking Applied to Image Authentication," ICASSP 2001, Salt Lake City, Utah, USA, 2001.
12. Menezes, A., Oorchot, P., Vanstone, S., "Handbook of Applied Cryptography", Boca Raton, FL:CRC, 1997.