Sıradüzensel Filigranlama Tekniğinin Değişim Bölgesi Belirleme Niteliğinin ve Doğruluğunun Geliştirilmesi

Metin Ertürkler[1], Yetkin Tatar[2]

[1,2] Fırat Üniversitesi, Bilgisayar Mühendisliği Bölümü, Elazığ

[1] merturkler@firat.edu.tr, [2] ytatar@firat.edu.tr

Özetçe

Kırılgan Filigranlama Teknikleri sayısal imgelerin aslıyla aynılığını doğrulamak için önerilirler. Kırılgan bir filigranlama tekniği, hem saldırılara karşı güvenilir hem de yüksek doğrulukta değişim bölgesi belirleme niteliğine sahip olmalıdır. Sıradüzensel Filigranlama Tekniği bu iki niteliği birlikte sağlamaktadır. Ancak Sıradüzensel Filigranlama Tekniğinin değişim bölgesi belirleme niteliği ve doğruluğu sayısal imgenin çözünürlüğüne bağımlıdır.

Bu bildiride, sıradüzensel ağaç yapısı önerilerek, Sıradüzensel Filigranlama Tekniğinin değişim bölgesi belirleme niteliği ve doğruluğu imge çözünürlüğünden bağımsız hale getirilmiştir.

1. Giriş

Son yıllarda sayısal cihaz ve iletişim teknolojilerindeki gelişmelere paralel olarak sayısal imgelerin kullanımında olağanüstü bir artış görülmektedir. Ancak sayısal imgeler analog imgeler gibi özgün bir negatife sahip olmadıkları için sayısal imgelerin aslıyla aynılığını doğrulamak mümkün değildir. Sayısal imgelerin özgün bir negatife sahip olmamasından kaynaklanan bu probleme çözüm olarak Kırılgan Filigranlama Tekniklerinin kullanılması önerilmiştir [1-10]. Sayısal Filigranlama, özgün imgeye ait bilgiyi (filigran) özgün imgenin algılanabilir kalitesini bozmadan doğrudan doğruya özgün imge içerisine gömen ve gerektiğinde gömülen bilgiyi özgün imge içerisinde bulabilen bir tekniktir.

Teknik yazında sıkça bahsedilen önemli bir kırılgan filigranlama tekniği Wong [1] tarafından önerilmiştir. Bu teknikte değişim bölgesini belirleyebilmek için sayısal imge üst üste gelmeyen bloklara bölünür ve her bir blok diğer bloklardan bağımsız olarak filigranlanır. Ancak imge içerisindeki her bir bloğun diğer bloklardan bağımsız olarak filigranlanmasından faydalanılarak Vektör Nicemlemeli Taklit Saldırısı (VNTS) olarak adlandırılan önemli bir saldırı gerçekleştirilmiştir [2]. VNTS'yi önlemek için blok boyutlarının büyütülmesi, blok özütünün hesaplanmasında blok indislerinin eklenmesi, daha karmaşık logoların kullanılması önerilmiştir [2]. Ancak bu öneriler saldırı yapılmasını önleyememiş, sadece saldırı yapılmasını zorlaştırmıştır. Etkili bir çözüm ise bloklar arasında bağımlılığın kurulmasıyla sağlanmıştır [2,3]. Ancak bloksal bağımlılıkta, bir bloğa ait bir pikselin bir bitinin bile bozulması her iki bloğun birden doğrulanamamasına neden olmaktadır [3]. Diğer bir çözüm ise her bir blok içerisine o bloğu kapsayan daha büyük bir bloğun özütünün gömülmesi ile elde edilmiştir [4]. Ancak bu çözüm saldırı yapılmasını bir dereceye kadar önlerken, değişim bölgesi belirleme doğruluğunu kaybetmiştir [5]. Alternatif bir çözüm olarak blok özütleri içerisine her bir imgeye ait benzersiz bir indisin gömülmesi önerilmiştir [6]. Bu öneri VNTS'nin yapılmasını tamamıyla önlemektedir. Ancak aynı imge indisinin doğrulama yordamında da kullanılması gerekmektedir. İmge veritabanlarında yapılacak doğrulamalarda imge indislerinin yönetilmesi büyük bir yük getirecektir. Bu problemi çözmek için imge indisinin imge piksellerinden hesaplanması önerilmiştir [7-9]. Ancak imge üzerinde bir değişim yapılması sonucunda yanlış imge indisinin çıkarılması, önerilen tekniğin değişim bölgesi belirleme niteliğini yok etmektedir.

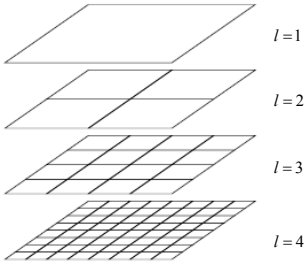
Teknik yazında hem saldırılara karşı güvenilir hem de değişim bölgesi belirleme niteliğine sahip bir teknik Çelik ve diğ. [10] tarafından önerilmiştir. Sıradüzensel Filigranlama Tekniği olarak adlandırılan bu teknikte, filigranın sayısal bir imge içerisine gömülmesi ve çıkarılması sıradüzensel bir yapı kullanılarak gerçekleştirilir. Ancak, Sıradüzensel Filigranlama Tekniğinde sıradüzenin oluşturulması imge çözünürlüğüne bağımlıdır. Eğer imge çözünürlüğü sıradüzenin en üst seviyesinde bir alt seviyeye bölünemezse, Sıradüzensel Filigranlama Tekniğinin değişim bölgesi belirleme niteliği yok olmaktadır. İmge çözünürlüğünün sıradüzenin üst seviyelerinde bir alt seviyeye bölünememesi durumunda ise Sıradüzensel Filigranlama Tekniğinin değişim bölgesi belirleme doğruluğu oldukça azalmaktadır.

Bu bildiride sıradüzensel yapı yerine, sıradüzensel ağaç yapısının kullanılması önerilmiştir. Sıradüzensel ağaç yapısı, sıradüzensel yapı ile birlikte tavan $(\lceil \cdot \rceil)$ ve taban fonksiyonlarının $(\lfloor \cdot \rfloor)$ kullanılmasıyla oluşturulmuştur. Bu yapı imge çözünürlüğünden bağımsız olarak imgenin istenilen alt seviyeye kadar bölünebilmesini sağlamaktadır. Test imgeleri üzerinde yapılan deneysel çalışmalarda önerilen sıradüzensel ağaç yapısının Sıradüzensel Filigranlama Tekniği içerisinde kullanılması 2 önemli fayda sağlamaktadır. Birincisi, sıradüzensel ağaç yapısının kullanılmasıyla Sıradüzensel Filigranlama Tekniği imge çözünürlüğünden bağımsız olarak değişim bölgesi belirleme niteliğine sahip olmaktadır. İkincisi, sıradüzensel ağaç yapısının kullanılmasıyla imgenin sıradüzen içerisinde alt seviyelere bölünmesi garanti altına alınarak, Sıradüzensel Filigranlama Tekniğinin sürekli olarak yüksek doğrulukta değişim bölgesi belirleyebilmesi sağlanmıştır.

2. Sıradüzensel Filigranlama Tekniği

Sıradüzensel Filigranlama Tekniğinde filigranın imgeler içerisine gömülmesi ve çıkarılması sıradüzensel bir yapı kullanılarak gerçekleştirilir. İmgeyi üst üste gelmeyen bloklara bölme işlemi çok seviyeli bir sıradüzenin oluşmasını sağlar. Sıradüzen içerisindeki her bir seviye bir önceki seviyedeki bloğun 2x2 ayrık bloğa bölünmesiyle oluşturulur. 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. 4 seviyeli bir sıradüzen yapısı şekil 1'de gösterilmiştir. Sıradüzensel Filigranlama Tekniği'nde filigranlanmak istenen $M * N$ boyutlu bir I imgesi ilk olarak sıradüzensel bir yapı içerisinde bloklara

bölünür. Sıradüzenin en alt seviyesinde üst üste gelmeyen her bir blok $I_{i,j}^{l}$ ile temsil edilir.



Şekil 1: Sıradüzensel 4 seviyeli blok yapısı

Burada i, j , bloğun uzaysal konumunu ve l , bloğun ait olduğu sıradüzensel seviyeyi göstermektedir. Sıradüzen içerisindeki toplam seviye ise L ile tanımlanmaktadır. Bu teknikte imgenin filigranlanması için her bir seviyedeki bloklara ait sayısal imzalar denklem 1 ve 2 kullanılarak hesaplanır.

for $l = 1 : L$

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

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

Burada $\tilde{I}_{i,j}^{l}$, EÖB düzlemi sıfır yapılmış 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 bloklara ait sayısal imzaların bir parçasını taşırlar. Her bir bloğun taşıdığı veri yükü yaklaşık olarak denklem 3'deki gibi hesaplanır.

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

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

Doğrulama yordamında ise ilk olarak doğrulanmak istenen her bir $\hat{I}_{i,j}^{l}$ alt bloğu içerisinden veri yükleri ($\hat{P}_{i,j}^{L}$) çıkartılarak her bir seviyedeki bloklara ait sayısal imzalar ($\hat{S}_{i,j}^{l}$) oluşturulur. Daha sonra her bir sayısal imza 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 $l = 1 : L$

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

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

3. Önerilen Sıradüzensel Ağaç Yapısı

Sıradüzensel yapıda imgenin sıradüzen içerisinde bir alt seviyeye bölünebilmesi imge çözünürlüğüne bağımlıdır. Örneğin 255x340 piksellik bir imge sıradüzenin en üst seviyesinde bir alt seviyeye bölünemediği için filigranlama işlemi sadece en üst seviyede yapılabilmektedir. Sadece en üst seviyede filigranlamanın yapılabilmesi ise Sıradüzensel Filigranlama Tekniğinin değişim bölgesi belirleme niteliğini yok etmektedir. Sıradüzensel yapıdaki diğer bir problem ise imge sıradüzensel seviyelerde bir alt seviyeye bölünemediğinde ortaya çıkmaktadır. Örneğin 1200x1600 piksellik bir imge sıradüzenin 5. seviyesinde 75x100 piksellik blok büyüklüğüne kadar bölünebilmektedir. Sıradüzensel Filigranlama Tekniğinde değişim bölgesi en küçük blok büyüklüğüne bağımlı olarak belirlenebilmektedir. Bu durumda bir pikselin bir bitinin bile değiştirilmesi, 7500 pikselin doğrulanamamasıyla sonuçlanmaktadır.

Yukarıdaki problemlerin çözümü için bu bildiride, sıradüzensel ağaç yapısının kullanılması önerilmektedir. Sıradüzensel ağaç yapısı, sıradüzensel yapı ile birlikte tavan ($\lceil \cdot \rceil$) ve taban fonksiyonlarının ($\lfloor \cdot \rfloor$) kullanılmasıyla oluşturulmuştur. Sıradüzensel ağaç yapısı kullanılarak $M * N$ boyutlu bir I imgesinin bölünmesi şekil 2'de gösterilmiştir. Oluşan her bir $I_{i,j}^{l}$ bloğu denklem 5 ile verilmiştir.

for $l = 1 : L$

$$I_{i,j}^{l} = \left\{ I_{i,j}^{l+1}, I_{i,j+1}^{l+1}, I_{i+1,j}^{l+1}, I_{i+1,j+1}^{l+1} \right\} \quad (5)$$

Alt seviyedeki her bir blok büyüklüğü ise denklem 6,7,8 ve 9 kullanılarak hesaplanır.

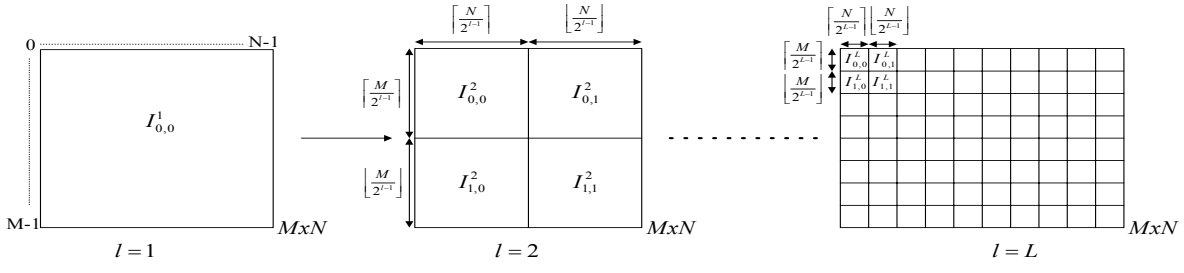
$$I_{i,j}^{l} = \left\lceil \frac{M}{2^{l-1}} \right\rceil x \left\lceil \frac{N}{2^{l-1}} \right\rceil \quad (6)$$

$$I_{i,j+1}^{l} = \left\lceil \frac{M}{2^{l-1}} \right\rceil x \left\lfloor \frac{N}{2^{l-1}} \right\rfloor \quad (7)$$

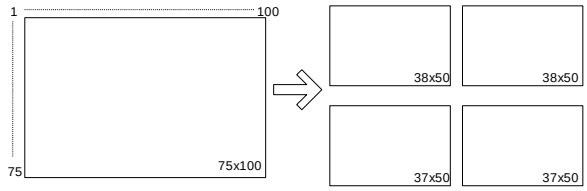
$$I_{i+1,j}^{l} = \left\lfloor \frac{M}{2^{l-1}} \right\rfloor x \left\lceil \frac{N}{2^{l-1}} \right\rceil \quad (8)$$

$$I_{i+1,j+1}^{l} = \left\lfloor \frac{M}{2^{l-1}} \right\rfloor x \left\lfloor \frac{N}{2^{l-1}} \right\rfloor \quad (9)$$

Örneğin 75x100 piksellik bir bloğun sıradüzensel ağaç yapısı kullanılarak bir alt seviyeye bölünmesi şekil 3 ile gösterilmiştir.



Şekil 2: Sıradüzensel ağaç yapısı kullanılarak imgenin bloklara bölünmesi



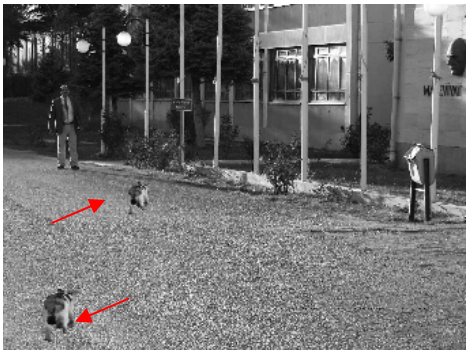
Şekil 3: 75x100 piksellik bir bloğun bir alt seviyeye bölünmesi

4. Deneysel Sonuçlar

Önerilen sıradüzensel ağaç yapısının etkinliğini değerlendirebilmek için 255x340 ve 1200x1600 piksel çözünürlüğündeki test imgeleri üzerinde çalışılmıştır. Yapılan deneysel çalışmalarda, SHA-1 (Secure Hash Algorithm) algoritmasına dayanan 320 bitlik DSA (Digital Signature Algorithm) sayısal imza algoritması kullanılmıştır. 320 bitlik DSA sayısal imza algoritması kullanılması durumunda oluşan veri yükü yaklaşık olarak 427 bittir.

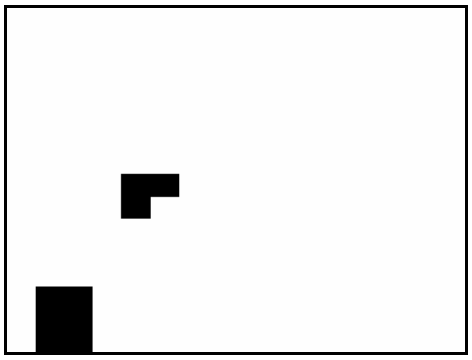
İlk deneysel çalışma önerilen sıradüzensel ağaç yapısının imge çözünürlüğünden bağımsız olarak çalıştığını göstermek için yapılmıştır. Sıradüzensel Filigranlama Tekniğinin en önemli dezavantajı imge en üst seviyede bir alt seviyeye bölünemediğinde ortaya çıkmaktadır. Örneğin şekil 4'de verilen 255*340 piksellik imge sıradüzensel yapıda sıradüzenin en üst seviyesinde bir alt seviyeye bölünemediğinden dolayı, filigranlama sadece en üst seviyede tüm imge pikselleri kullanılarak yapılmaktadır. Ancak bu durumda imgenin bir pikselinin bile bozulması tüm imgenin doğrulanamamasına neden olmaktadır. Sıradüzensel Filigranlama Tekniği ile filigranlanmış 255*340 piksellik imge şekil 4'de verilmiştir. Şekil 4'deki filigranlı imge üzerinde değişimler yapılarak şekil 5'deki imge oluşturulmuştur. Değiştirilen bölgeler şekil 5'de oklarla gösterilmiştir.

Şekil 4: Sıradüzensel Filigranlama Tekniği ile filigranlanmış imge



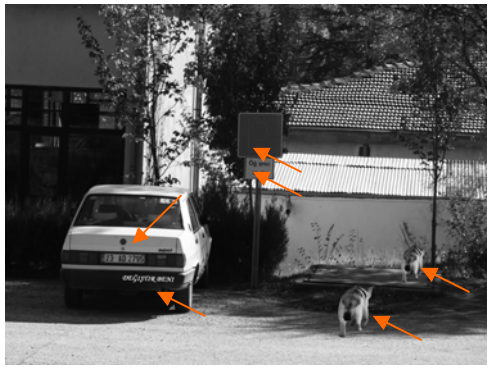
Şekil 5: Değiştirilmiş filigranlı imge

Şekil 6: Sıradüzensel Filigranlama Tekniğinin doğrulama sonucu



Şekil 7: Sıradüzensel ağaç yapısının kullanılmasıyla elde edilen doğrulama sonucu

Şekil 8: Sıradüzensel Filigranlama Tekniği ile filigranlanmış 1200x1600 piksellik imge



Şekil 9: Değiştirilmiş filigranlı imge

Sıradüzensel Filigranlama Tekniğinin doğrulama algoritması çalıştırılarak elde edilen sonuç ise şekil 6'da

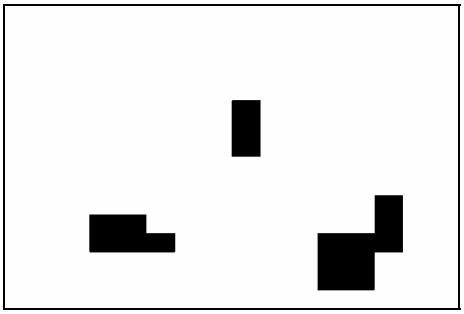
gösterilmiştir. Şekil 6'da görüldüğü gibi piksel değerlerindeki bir bozulma tüm imgenin doğrulanamamasına neden olmuştur. Sıradüzensel Filigranlama Tekniği imgeyi en üst seviyede bir alt seviyeye bölemediği takdirde, imge üzerinde bir değişimin olup olmadığını belirleyebilirken, değişim yapılan bölgeyi belirleyememektedir.

Önerilen sıradüzensel ağaç yapısının Sıradüzensel Filigranlama Tekniği içerisinde kullanılmasıyla bu problem tamamen çözülmüştür. Şekil 4'de verilen test imgesi önerilen sıradüzensel ağaç yapısı kullanılarak 4. seviyede 31x42 piksellik bloklara kadar bölünerek filigranlanmış ve şekil 5'deki aynı değişimler uygulandıktan sonra doğrulama algoritması çalıştırılarak şekil 7'deki imge elde edilmiştir. Şekil 7'de doğrulanan bölgeler beyaz, doğrulanamayan bölgeler ise siyah ile gösterilmiştir. Şekil 7'de de görüldüğü gibi değiştirilen bölgeler sıradüzensel ağaç yapısının kullanılmasıyla belirlenebilmektedir.

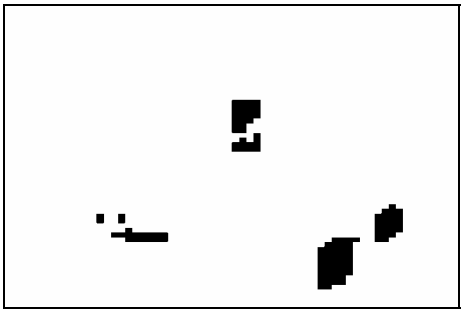
İkinci deneysel çalışma şekil 8'de gösterilen 1200x1600 piksellik test imgesi üzerinde yapılmıştır. Sıradüzensel yapı 1200x1600 piksellik test imgesini 5. seviyede 75x100 piksellik bloklara kadar bölebilmektedir. Sıradüzensel Filigranlama Tekniği ile filigranlanmış imge şekil 8'de gösterilmiştir. Sıradüzensel Filigranlama Tekniğinin değişim bölgesi belirleme doğruluğunu değerlendirebilmek için, şekil 8'de verilen filigranlı imge üzerinde değişimler yapılarak şekil 9'da gösterilen imge elde edilmiştir.

Şekil 9'da 27.759 piksel değiştirilmiş ve bu bölgeler oklarla gösterilmiştir. Daha sonra Sıradüzensel Filigranlama Tekniğinin doğrulama algoritması çalıştırılarak elde edilen sonuç şekil 10'da gösterilmiştir. Şekil 10'da doğrulanan bölgeler beyaz ile doğrulanamayan bölgeler ise siyah ile gösterilmiştir. Sıradüzensel Filigranlama Tekniği tarafından doğrulanamayan piksel sayısı 127.500 olarak bulunmuştur.

Sıradüzensel Filigranlama Tekniği içerisinde sıradüzensel ağaç yapısı kullanılarak şekil 8'de verilen test imgesi 7. seviyede 18x25 piksellik bloklara kadar bölmelenerek filigranlanmıştır. Daha sonra şekil 9'daki aynı değişimler uygulandıktan sonra doğrulama algoritması çalıştırılarak şekil 11'deki imge elde edilmiştir.



Şekil 10: Sıradüzensel Filigranlama Tekniğinin doğrulama sonucu



Şekil 11: Sıradüzensel ağaç yapısının kullanılmasıyla elde edilen doğrulama sonucu

Sıradüzensel Filigranlama Tekniği içerisinde sıradüzensel ağaç yapısının kullanımıyla doğrulanamayan piksel sayısı ise 59.225 olarak bulunmuştur. Bu sonuç, Sıradüzensel Filigranlama Tekniğinin doğrulama algoritmasının bulduğu sonuçtan (127.500) çok daha doğrudur.

5. Sonuçlar

Bu bildiride sıradüzensel ağaç yapısı önerilerek, Sıradüzensel Filigranlama Tekniğinin değişim bölgesi belirleme niteliği ve doğruluğu imge çözünürlüğünden bağımsız hale getirilmiştir. 255x340 piksellik test imgesiyle yapılan deneysel çalışmalarda Sıradüzensel Filigranlama Tekniği değişim bölgesini belirleyemezken, önerilen sıradüzensel ağaç yapısı değişim bölgesini iyi bir çözünürlükte belirleyebilmektedir. Ayrıca 1200x1600 piksellik test imgesi ile yapılan deneysel çalışmada Sıradüzensel Filigranlama Tekniği 127.500 pikselin aslıyla aynılığını doğrulayamazken, önerilen sıradüzensel ağaç yapısı 59.225 pikselin aslıyla aynılığını doğrulamayarak değişim bölgesini çok daha hassas bir çözünürlükte belirleyebilmektedir.

6. Kaynakça

[1] Wong, P. W., A Public Key Watermark for Image Verification and Authentication, Proc. IEEE Int. Conf. Image Processing, 1, 455-459, 1998.

[2] Holliman M., and Memon, N., Counterfeiting Attacks on Oblivious Blockwise Independent Invisible Watermarking Schemes, IEEE Trans. Image Processing, 9, No. 3, 432-441, 2000.

[3] 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, 149, No. 2, 57-62, 2002.

[4] Coppersmith, D., Mintzer, F., Tresser, C., Wu, C. W. and Yeung, M. M., Fragile Imperceptible Digital Watermark with Privacy Control, Proc. SPIE/IS&T Int. Symp. Electronic Imaging: Science and Technology, 3657, 79-84, 1999.

[5] Fridrich, J., Security of Fragile Authentication Watermarks with Localization, Proc. SPIE Photonic West, Vol. 4675, Electronic Imaging 2002, Security and Watermarking of Multimedia Contents, San Jose, California, January, 691-700, 2002.

[6] Wong, P. W. and Memon, N., Secret and Public Key Image Watermarking Schemes for Image Authentication and Ownership Verification, IEEE. Trans. Image Processing, 10, No. 10, 1593-1601, 2001.

[7] Wong, P. W., Memon, N., Secret and Public Key Authentication Watermarking Schemes that Resist Vector Quantization Attack, Proc. SPIE, 3971, No. 40, 417-427, 2000.

[8] Holliman, M., Memon, N. and Yeung, M. M., On the Need for Image Dependent Keys for Watermarking, Proc. Content Security and Data Hiding in Digital Media, Newark, NJ, May 14, 1999.

[9] Fridrich, J., Robust Bit Extraction from Images, Proc. IEEE Int. Conf. Multimedia Computing & Systems, 2, 536-540, 1999.

[10] Çelik, M. U., Sharma, G., Saber, E. and Tekalp, A. M., Hierarchical Watermarking for Secure Image Authentication with Localization, IEEE Transactions on Image Processing, 11, No. 6, 585-595, 2002.