SAYISAL İMGELER İÇİN YENİ BİR HIZLI LOJİSTİK KİMLİK DOĞRULAMA YÖNTEMİ

Turker Tuncer[1]

Original scientific paper

İmgelerde kimlik doğrulamak için sıklıkla kullanılan yöntemlerden birisiside kırılgan damgalama yöntemleridir. Bu makalede lojistik harita fonksiyonunu kullanan yeni bir imge kimlik doğrulama (LİK) yöntemi önerilmiştir. Önerilen yöntem damga üretme, damga gizleme, damga çıkarma ve saldırı tespit aşamalarından oluşmaktadır. LİK yönteminde pikseller 3 gruba ayrılır. En anlamlı 2 grup damga üretmek için kullanılır. En anlamsız grup ise damga gömme işleminde kullanılmaktadır. Bu çalışmada, damga gömmek için LSB (Least Significant Bit, En anlamsız bit) ve 2LSBs kullanılmıştır. LİK yönteminin performansını test edebilmek için çalışma zamanı, görsel kalite ve saldırı tespiti yetenekleri kullanılmıştır. Saldırı tespiti yeteneğini ölçmek için, medyan filtre, JPEG sıkıştırma, ortalama filtre, döndürme atakları, gürültü ekleme, kolaj saldırıları kullanılmıştır. Elde edilen sonuçlar, deneysel sonuçlarda sunulmuştur. Deneysel sonuçlar, önerilen yöntemin hızlı ve başarılı bir yöntem olduğunu göstermektedir.

Anahtar Kelimeler: *Veri Gizleme; Damgalama; Görsel Sır Paylaşımı; Adli Bilişim; Kriptolojik Özet Fonksiyonları; Bilgi Güvenliği; Görüntü İşleme.*

1 Giriş

Günümüzde, IOT (Internet of things, nesnelerin interneti), sosyal medya, internet bağlantılı cihazlar vb. teknolojik aygıtlar yaygın olarak kullanılmaktadır. Bu cihazlar kullanılarak ses, imge, video gibi çoklu ortam verilerinin transferi ve erişimi de kolaylaşmıştır. Sayısallaşan dünyadaki en önemli problem siber saldırılar olarak karşımıza çıkmaktadır [1-3]. İmge düzenleme araçlarının çok fazla gelişmesi, imgeler için bilgi güvenliği ve kimlik doğrulama önemli bir konu haline gelmiştir. İmgelerde kimlik doğrulama için genel olarak 2 ayrı yöntem kullanılmaktadır. Bunlar;

- Sayısal imza tabanlı imge kimlik doğrulama
- Kırılgan damgalama yöntemleridir.

İmza tabanlı kimlik doğrulama yöntemlerinde genellikle kriptolojik özet fonksiyonları ve açık anahtar alt yapılı sayısal imza şemaları kullanılmaktadır. Bu tür yöntemlerde öncelikle imgenin kriptolojik özet değeri elde edilir. Ardından bu özet değeri RSA, Eliptik Eğri Şifreleme gibi açık anahtar alt yapısını kullanan bir imza şemasıyla imzalanır. Kimlik doğrulamayı gerçekleştirmek için özet değerleri karşılaştırılır. Eğer bu değerler birbirinden farklı ise kimlik doğrulama gerçekleştirilemez. İmza şemasında elde edilen değerler aynı ise imgenin kimlik doğrulaması başarılıdır. Kırılgan damgalama yöntemlerinde ise üretilen veya dışarıdan girilen damga veri gizleme fonksiyonları kullanılarak imgeye gömülür. İmgenin kimlik doğrulamasını gerçekleştirmek için dışarıdan girilen veya üretilen damga ile çıkarılan damga karşılaştırılır. Kırılgan damgalama tabanlı imge kimlik doğrulama yöntemlerini oluşturan bileşenler aşağıdaki gibi verilmiştir [4-6].

- Damga üretme
- Damga gömme
- Damga çıkarma
- Saldırı tespiti

Bir kırılgan damgalama yöntemi, yüksek görsel kaliteye ve yüksek imge kimlik doğrulama sahip olmalıdır [7-9].

Bu makalede lojistik harita tabanlı yeni bir imge kimlik doğrulama önerilmiştir. Önerilen yöntem güvenilir, hızlı, yüksek görsel kaliteye ve yüksek imge kimlik doğrulama yeteneğine sahip bir yöntemdir.

2 Önerilen Yöntem

Bu çalışmada, lojistik harita tabanlı yeni ve hızlı bir imge kimlik doğrulama yöntemi önerilmiştir. Önerilen yöntem karmaşıklığı O(1)' dir. LIK yöntemi, basit matematiksel işlemler yaparak imge kimlik doğrulamasını gerçekleştirmeyi planlanmaktadır. LIK yöntemi, damga oluşturma, damga gömme, damga çıkarma ve saldırı tepit aşamalarından oluşan kör ve kırılgan bir damgalama yöntemidir. LIK' in güvenilirliğini sağlamak için sözde rastgele sayı üreteçleri kullanılarak damgalar üretilmekte ve üretilen damgaların imgeyle ilişkilendirilmesi için, damga ve imge özelliği XOR işlemine tabi tutulmaktadır. Elde edilen damga LSB veya 2LSBs yöntemi kullanılarak imgeye gizlenmektedir. Bu çalışmada, LSB ve 2LSBs veri gizleme fonksiyonları optimum hale getirilmiştir. Önerilen veri gizleme yapısı xLSBs veri gizleme yöntemlerinin yanı sıra, modulo tabanlı veri gizleme yöntemlerini de içerisinde barındırmaktadır. LSB ve 2LSBs veri gizleme yöntemlerinde genellikle piksel değeri ikili forma çevrilir ve damga en anlamsız bitlere gömülür. Geleneksel bu yöntemde pikselleri ikili forma çevirmek maliyetli bir işlemdir ve karmaşıklığı O(n)'dir. Bu yöntemde optimum veri gizleme önerilerek karmaşıklık O(1)'e düşürülmüştür. Veri çıkarma aşamasında ise sadece modulo fonksiyon kullanılmaktadır. Saldırı tespiti aşamasında, gömülen damga ile çıkarılan damga karşılaştırılmaktadır. LIK'in damga üretme algoritmasının adımları aşağıdaki gibidir.

Adım 1: Lojistik harita kullanılarak rastgele damga üretilir. Lojistik haritanın formülü Eşitlik 1 ve 2' de verilmiştir.

$$x_{i+1} = hx_i(1-x_i), h \in [3.57, 4], \quad x \in (0,1), x \neq \{0.25, 0.5, 0.75\} \tag{1}$$

$$x = \left\lfloor 2^b x \right\rfloor \tag{2}$$

Adım 2: Eşitlik 3 ve 4 kullanılarak a ve b değerleri elde edilir.

$$a = \left\lfloor \frac{OI}{64} \right\rfloor \tag{3}$$

$$b = \left\lfloor \frac{OI(\mathrm{mod}\,64)}{8} \right\rfloor \tag{4}$$

Yukarıdaki denklemde a orijinal imge piksellerinin en anlamlı 2 bitini, b ise 3,4 ve 5. bitlerini, OI orijinal imgeyi temsil etmektedir. Bu iki parça imgeden özellik çıkarmak için kullanılmaktadır.

Adım 3: Doğrulama bitlerini elde etmek için lojistik haritaya benzer bir yöntem kullanılmaktadır. Doğrulama bitlerinin elde edilişi Eşitlik 5'te gösterilmektedir.

$$d = axbx(8-b)(mod\,2^b) \oplus x \qquad (5)$$

Bu çalışmada veri gizlemek için basit ama efektif bir yöntem kullanılmıştır. Kullanılan yöntemin matematiksel açıklaması Eşitlik 6'te verilmiştir.

$$SI = \left\lfloor \frac{CI}{2^b} \right\rfloor 2^b + d \qquad (6)$$

Yukarıdaki denklemde SI Stego imge ve d doğrulama bitlerini temsil etmektedir.

Önerilen yöntemin damga çıkarma yöntemi de damga gömme yöntemi kadar basittir. Damga çıkarma için sadece mod ve XOR operatörünün kullanılması yeterlidir. Eşitlik 7'de damga çıkarma yönteminin denklemi verilmektedir.

$$d = CI(mod\,2^b) \oplus x \qquad (7)$$

Yukarıdaki denklemde ed çıkarılan damgayı temsil etmektedir. Saldırı tespit aşamasında ed ve $ed = axbx(8-b)(mod\,2^b)$ değerlerinin birbirine eşit olması beklenmektedir. Eğer bu değerler birbirlerine eşit değilse saldırı tespiti yapılır. Saldırı tespitinin matematiksel açıklaması Eşitlik 8' de verilmiştir.

$$tp = \begin{Bmatrix} (0, ed = axbx(8-b)(mod\,2^b)) \\ 1, ed \neq axbx(8-b)(mod\,2^b) \end{Bmatrix} \qquad (8)$$

Yukarıdaki denklemde tp saldırı tespit değeridir. Bu değer her piksel için hesaplanır ve böylece W x H boyutunda saldırı tespiti matrisi oluşturulur.

3 Deneysel Sonuçlar

LIK yönteminin performansını test edebilmek için görsel kalite ve imge kimlik doğrulama yeteneği (saldırı tespiti) kullanılmıştır. Deneysel sonuçları elde edebilmek için literatürde sıklıkla kullanılan ve Şekil 1' de gösterilen imgeler kullanılmaktadır.

Görsel kaliteyi ölçmek için genellikle PSNR (Peak signal noise-to-ratio, Tepe sinyal gürültü oranı) kullanılmaktadır. PSNR' nin formülü Eşitlik 9' de verilmiştir.

$$SNR = \frac{10log_{10}(255^2\, xWxH)}{\sum_{I=1}^{W}\sum_{J=1}^{H}\left(OI_{I,J} - WI_{I,J}\right)^2} \qquad (9)$$

OI orijinal imge, WI damgalı imgeyi ifade etmektedir. LSBs ve 2LSBs' e göre yani b=1 ve b=2 değerlerine göre elde edilen PSNR değerleri Tablo 1'de verilmiştir.

Şekil 1. 20 standart test imgesi [10].

Tablo 1. Test imgelerine LİK yönteminin uygulanması sonucu elde edilen PSNR değerleri.

İmge	b=1	b=2	İmge	b=1	b=2
Parot	51.15	44.14	Man	51.14	44.14
Baboon	51.14	44.16	Goldhill	51.14	44.17
Couple	51.12	44.14	Bridge	51.13	44.16
SailBoat	51.15	44.16	Cameraman	51.13	44.14
F16	51.13	44.15	House	51.14	43.78
Lena	51.13	44.16	Tiffany	51.15	44.15
Peppers	51.13	44.15	Crowd	51.13	44.16
Boat	51.14	44.12	Girl1	51.14	44.15
Barbara	51.14	44.15	Girl2	51.13	44.14
Pentagon	51.14	44.15	Girl3	51.12	44.09

Tablo 2. 20 resimden else edilen ortalama BER değerleri.

Damga gömme fonksiyonu	Medyan		JPEG	Ortalama		Döndürme		Gürültü ekleme		Kolaj
	3 x 3	5 x 5	%50	3 x 3	5 x 5	45º	90º	SP (1)	Speckle (1)	%25
b=1 (LSB)	0.33	0.44	0.50	0.50	0.51	0.50	0.50	0.50	0.50	0.48
b=2 (2LSBs)	0.53	0.68	0.75	0.74	0.75	0.75	0.75	0.72	0.75	0.76

Önerilen LİK yönteminin imgel kimlik doğrulama yeteneğini test edebilmek için medyan filtre, JPEG sıkıştırma, ortalama filtre, döndürme atakları, gürültü ekleme ve kolaj saldırıları uygulanmıştır. Önerilen LİK yönteminin imge kimlik doğrulama yeteneğini ölçmek için saldırı tespiti yeteneğine bağlı BER (Bit Error Rate, Bit Hata Oranı) ölçüm metriği kullanılmıştır. BER' in denklemi Eşitlik 10' de verilmiştir.

$$BER = \frac{\sum_{I=1}^{W}\sum_{J=1}^{H} WM \oplus WM^{1}}{WxH} \qquad (10)$$

4 Sonuç ve Öneriler

Bu makalede lojistik tabanlı yeni bir imge kimlik doğrulama yöntemi önerilmiştir. Yöntemi kırılgan hale dönüştürmek için lojistik harita kullanılmıştır. Önerilen yöntem damga üretme, damga gömme, damga çıkarma ve saldırı tespiti aşamalarından oluşmaktadır. LİK yöntemi aktif imge kimlik doğrulama yöntemlerinden biri olup saldırı zamansal karmaşıklığı O(1)' dir. MATLAB programının paralel işlem yeteneği kullanılarak yazılan LİK efektif çalışan hızlı bir yöntemdir. LİK yönteminde damga üretmek için lojistik harita kullanılarak rastgele sayı dizisi üretilmiştir ve lojistik harita modifiye edilerek imgenin özellikleri elde edilmiştir. Rastgele üretilen değerlerle imgenin değerleri XOR işlemine tabi tutularak damga üretilmiştir. LİK yönteminin güvenliğini lojistik harita tabanlı rastgele sayı üreteci sağlamaktadır. Önerilen LİK yönteminde LSB ve 2LSBs veri gizleme fonksiyonları kullanılmıştır. LSB veri gizleme fonksiyonunda görsel kalite yüksek çıkarkan, 2LSBs veri gizleme fonksiyonunda saldırı tespit yeteneği yüksek çıkmaktadır. Deneysel sonuçlar önerilen yöntemin başarılı sonuçlar elde ettiğini göstermektedir.

Bu çalışma, gelecekteki çalışmalarda lojistik harita gibi doğrusal olmayan denklemler kullanılarak farklı imge kimlik doğrulama yöntemlerinin önerilebileceğini göstermektedir.

7 Kaynaklar

[1] Y. Xiang, S. Guo, W. Zhou, S. Nahavandi, Patchwork-based audio watermarking method robust to de-synchronization attacks, IEEE/ACM Trans. Audio Speech Lang. Process. 22 (9) (2014) 1413–1423.

[2] A. Akter, N. E-Tajnina, M.A. Ullah, Digital image watermarking based on DWT-DCT: evaluate for a new embedding algorithm, in: Third Int. Conf. On Informatics, Electronics & Vision, May, Dhaka,Bangladesh, 2014, pp. 1–6.

[3] Q. Su, Y. Niu, Q. Wang, G. Sheng, A blind color image watermarking based on DC component in thespatial domain, Optik 124 (23) (2013) 6255–6260.

[4] C.Y. Lin, S.F. Chang A robust image authentication method distinguish JPEG compression from malicious manipulation, IEEE Trans. Circuits Syst. Video Technol. 11 (2), (2001),153-168.

[5] X. Qi, X. Xin, A quantization-based semi-fragile watermarking scheme for image content authentication, J. Vis. Commun. Image Represent. 22 (2) (2011), 187-200.

[6] Y.-C. Hu, C.-C. Lo, W.-L. Chen, Probability-based reversible image authentication scheme for image

demosaicking, Future Generation Computer Systems 62 (2016), 92-103.
[7] T. Tuncer, D. Avci, E. Avci, A new data hiding algorithm based on minesweeper game for binary images, Journal of The Faculty of Engineering and Architecture of Gazi University 31.4 (2016): 951-959.
[8] L. Yuan, Q. Ran, T. Zhao, Image authentication based on double-image encryption and partial phase decryption in nonseparable fractional Fourier domain, Optics & Laser Technology 88 (2017) 111–120.
[9] X. Li, X. Meng, Y. Yin, X. Yang, Y. Wang, X. Peng, W. He, X. Pan, G. Dong, H. Chen, Hierarchical multilevel authentication system for multiple-image based on phase retrieval and basic vector operations, Optics and Lasers in Engineering 89 (2017) 59–71.
[10] C. Qin, X. Chen, D. Ye, J. Wang, X. Sun, A novel image hashing scheme with perceptual robustness using block truncation coding, Information Sciences, 361-362, pp. 84-99, 2016.

Authors' addresses

Dr. Türker Tuncer[1], Asistant Research
Fırat University
Technology Faculty, Forensic Engineering
ttuncer@firat.edu.tr

.