

Gerçek Zamanlı Video Kayıtlarına Veri Gizleme Uygulaması

Yıldırım Yalman, İsmail Ertürk

Kocaeli Üniversitesi Elektronik ve Bilgisayar Eğitimi Bölümü
yildiray.yalman@kocaeli.edu.tr, erturk@kocaeli.edu.tr

Özet: Günümüzde, farklı sayısal ortamların (html, imge, ses, video vb.) kullanımı yaygınlaşarak artmaktadır. Buna paralel olarak, çoklu ortam ve bilgi güvenliği uygulamaları gibi güncel gereksinimler ile gizli veri gömme (steganography) temelinde yapılan çalışmalar da yoğun ilgi görmektedir. Bu bildiride sunulan çalışmanın amacı gerçek zamanlı video kayıtlarına gizli veri gömme uygulaması gerçekleştirmektir. Gizli verilerin gömülmesi işlemi bit düzleminde gerçekleştirilmiştir. Literatürde sunulan ve klasik LSB tabanlı birçok çalışmadan farklı olarak RGB ağırlık tabanlı kodlama kullanılan bu uygulamada, veri gömme kapasitesi nispi olarak oldukça artırılmıştır.

ABSTRACT: Many different digital medium (html, image, voice, video etc.) used for information hiding (steganography) have nowadays become increasingly more sophisticated and widespread. Researches on secret information embedding, have received considerable attention for a decade due to its potential applications in multimedia communications. The main objective of this research work is to implement a steganography application for real-time video recording, where spatial domain components are used to data embedding. In this paper, not only was the LSB technique exploited for hidden data embedding but also the RGB (24 bits colored-image) weight based encoding technique was used, resulting in relatively high data embedding capacity.

Anahtar Kelimeler: Gerçek Zamanlı Video, Steganografi, Veri Gizleme.

1. Giriş

Temeli antik çağlara kadar dayanan gizli haberleşme, teknoloji değişip geliştikçe şekil ve yöntem açısından da önemli farklılıklar göstermektedir. Bununla birlikte önemini devamlı korumaktadır. Gizliliğin önemini arttığı uygulamalarda; gizli bilgilerin, üçüncü kişilerin eline geçmeden ilgili hedefe ulaştırılması amaçlanır. Bu noktadan hareketle, bildiride sunulan çalışmada Gerçek Zamanlı Video Kayıtlarına Veri Gizleme (GVVG) Uygulaması geliştirilmiştir.

Steganografi biliminin temel çıkış noktası, üçüncü kişilerde şüphe uyandırmayacak bir yaklaşımla gizli haberleşmeyi sağlamaktır. Günlük hayatta rasgele kayda alınan gerçek zamanlı video dosyaları ve steganografinin temel amaçları sunulan bu çalışmada birleşmektedir. Zira böyle bir dosya, normal koşullarda inceleyenlerin/kullanıcıların dikkatini

çekmeyecek ve oldukça büyük miktarda gizli veri ihtiva edebilme özelliğine sahip olacaktır. Literatürde yapılan değişik çalışmalarda video çerçevelerinin (frames) her birine aynı gizli verinin gömülmesi işlemi gerçekleştirilmiş [1], bazılarında grafik işlemciler kullanılmış [2], bazılarında ise özel olarak Alan Programlanabilir Kapı Dizilerinden (FPGA) faydalanılmıştır [3]. Geliştirilen GVVG uygulaması ise yazılım tabanlı olması, bahsedilen örnek uygulamalara nazaran daha esnek olması (örneğin yeni fonksiyon eklenebilmesi ve algoritma değişikliğinin kolay yapılabilmesi vb.), yükleme kolaylığı, gizli veri gömme kapasitesi ve maliyet faktörleri göz önünde bulundurulduğunda bu çalışmalardan bir adım öne çıkmaktadır.

Saniyede art arda 25—30 imgenin kamera yardımı ile alındığı ve işlendiği gerçek zamanlı video kaydı, işlem yükü ve kapasitesi açısından sistem kaynaklarının tamamını kullanmaya

ihtiyaç duyar. Kimi uygulamalarda çözünürlük ve işlem yükü göz önüne alınarak bu sayı %20 hatta %40 oranında düşürülür. Ancak bu durum video kalitesinden ödün vermek anlamına gelmektedir. Sunulan çalışma (GVVG uygulaması), saniyede 25 imgenin kamera yardımı ile alınmasını ve gizli veri gömme işlemi yapılarak video kaydedilmesini sağlamaktadır.

Gizli verilerin gömülmesi için RGB ağırlık tabanlı kodlamanın kullanıldığı GVVG sisteminde, genel olarak kameradan alınan gerçek zamanlı imgelere kullanıcı tarafından belirtilen bir gizli dosya/veri gömülme ve sonuç yeni bir video dosyası olarak kaydedilmektedir.

Gizli gömü verilerinin video dosyası içerisinden ayırt edilmesini sağlayan çözücü algoritma ve uygulaması da bildiride sunulmaktadır.

Bildiri bölümleri şöyle organize edilmiştir: Bölüm 2’de çalışmanın önemine ve başlatılma sebeplerine değinilmektedir. Bölüm 3’te sayısal imge ve sayısal video kavramları kısaca açıklanarak, gizli veri gömme işlemi için kullanılan algoritma ve akış şemaları verilmektedir. Ayrıca bu bölümde, gerçekleştirilen GVVG uygulamasının olumlu ve olumsuz yanları da vurgulanmaktadır. Son bölümde ise bildiri sonuçları ve genel bir değerlendirme sunulmaktadır.

2. Geliştirilen GVVG Uygulamasının Başlatılma Sebebi ve Önemi

Yaygın anlamda gizli veri gömme ile ilgili önemli çalışmalardan ilki, bir müzik şirketinin, müzik kayıtlarına sahiplik bilgisini içeren kod yerleştirmek için 1954 yılında aldığı patettir [4]. 1990’ların başında imge damgalama kavramı gelişmiş; Tanaka ve arkadaşları faks gibi ikili imgelerin korunması kavramını ortaya atmışlardır [5]. 1993 yılında Tirkel ve arkadaşları gerçekleştirdikleri veri gömme tekniğine; daha sonra “watermark” olarak birleştirilecek olan “water mark” ismini vermişlerdir [6]. Steganografi (steganography) ise iki parçadan oluşan

Yunanca bir kelimedir. “Steganos” örtülü/gizli, “grafi” ise yazım/çizim anlamına gelmektedir. Steganografi uygulaması için mutlaka ses, resim, video gibi bir taşıyıcı veri (örtü verisi) gerekmektedir (Şekil 1). Steganografide üçüncü kişilerin steganaliz işlemi yapamaması için, verinin gömülme şeklinin/yönteminin gizli tutulması ve taşıyıcı verinin ilk halinin bu kişilerin elinde bulunmaması, gömülecek verilerin güvenliği açısından büyük önem taşır.



Şekil 1. Veri gizleme yöntemlerinin sınıflandırılması

Kriptografi, haberleşen iki veya daha fazla tarafın bilgi alışverişini emniyetli olarak yapmasını sağlayan ve gizli bilgiyi istenmeyen üçüncü kişilerin anlayamayacağı bir şekilde getirerek korumayı esas alan teknik ve uygulamalar bütünüdür. Modern steganografi yöntemi ise, bir veriyi (mesaj) bir nesnenin içine gizli biçimde yerleştirmeyi esas almaktadır. Öyle ki, sadece belirlenen alıcı, kendisine iletilmek istenen mesajı nesneden seçebilmekte ve diğer gözlemcilerin (üçüncü şahısların) o nesnenin içindeki mesajın varlığından haberleri olmamaktadır. Kriptografinin bir kolu olarak da görülen steganografi, bu özelliğiyle kriptografiyi bir adım ileri taşımaktadır. Kriptografi güvenilirliği sağlasa da bir bakıma mesajın gizliliğini sağlayamamaktadır [7]. Kriptografi uygulamalarında bilgi, sadece gönderen ve alanın anlayabileceği şekilde şifrelenirken, steganografik uygulamalarda bilgi sadece gönderen ve alanın varlığını bildiği şekilde saklanmakta, bazen de şifrelenip fazladan (kriptografik) koruma sağlanabilmektedir [8].

Literatürde sunulan veri gömme uygulamalarının büyük çoğunluğu, boyutu belirli olan taşıyıcı

cı veriler (ortamlar) esas alınarak gerçekleştirilmiştir. Örneğin Adlı ve Nakao, “.midi” uzantılı dosyalar için üç farklı steganografi algoritması geliştirmiştir [9]. Xu ve arkadaşları da sıkıştırılmış video görüntülerine başka bir steganografi uygulama algoritması önermişlerdir [10]. Yapılan kimi çalışmalarda ise aynı gizli verinin video dosyalarındaki her imgeye gömülmesi ya da video dosyası içerisindeki her imgenin belirlenmiş bloklarına gömülmesi önerilmektedir [1, 11]. Bu veri gömme algoritmalarının iki önemli sakıncası bulunmaktadır. Birincisi, gömülecek gizli verinin boyutunun büyük olması durumunda ilgili taşıyıcı veri (imge, ses vb.) yetersiz kalacak ya da veri gömme uygulaması parçalı halde işlem yapmak zorunda kalacaktır. İkincisi ise, taşıyıcı verinin gizli veri gömme uygulaması gerçekleştirilmeden önceki halinin üçüncü kişilerin eline geçmesi durumunda, aradaki farkın kolayca tespit edilerek gizli verinin elde edilebilmesidir.

Bu bildiride sunulan GVVG uygulama çalışmalarının temel başlatılma sebebi, yukarıda anılan sakıncaların ortadan kaldırılması için sıralı imgelerin kameradan gerçek zamanlı alınarak, üçüncü kişilerin bu imgelere sahip olmasının engellenmesi ve bu imgeler dizisinin oluşturduğu video dosyası kullanılarak yüksek gizli veri gömme kapasitesi elde etmektir.

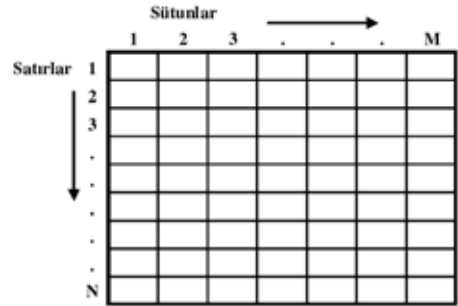
3. Gerçek Zamanlı Video Veri Yapısı ve GVVG Uygulaması

Bu bölümde uygulamaya temel oluşturan sayısal imge ve sayısal video kavramı ile ilgili temel bilgiler verilerek, esinlenen veri gizleme tekniğinin algoritması açıklanmaktadır. Ayrıca GVVG sistemi için geliştirilen yöntemin akış şemaları sunularak, örnek bir uygulamaya da yer verilmektedir.

3.1. Sayısal İmge ve Sayısal Video

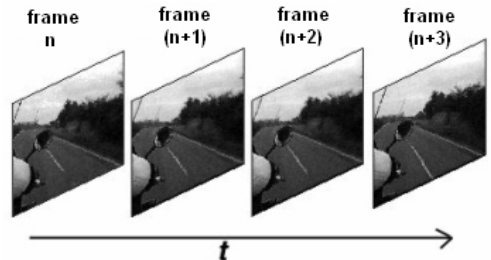
Sayısal (dijital) imge, N satır ve M sütunluk bir dizi ile temsil edilir (Şekil 2). Bir imge dizisinin elemanlarına “piksel” denir. En basit durumda

pikseller 0 veya 1 değerini alır ve bu piksellerden oluşan resimlere ikili (binary) imge denir. 1 ve 0 değerleri sırasıyla aydınlık ve karanlık bölgeleri veya nesne ve zemini (nesnenin önünde veya üzerinde bulunduğu çevre zemini) temsil ederler [12]. Sayısal görüntü dosyaları renkli olarak genellikle 24 bit (R, G, B değerlerinin her biri için 8'er bit olmak üzere), gri-seviye görüntüler ise 1, 2, 4, 6 ya da 8 bit olabilirler. İmgeler bilgiyi görsel bir biçimde saklar ve gösterilmesini sağlarlar. Bu açıdan resimler ve fotoğraflar imge kapsamında ele alınabileceği gibi, geniş bir bakış açısı ile her türlü iki boyutlu veri imge olarak değerlendirilebilmektedir. Video ise ardışık imge çerçeveleridir. Bir diğer ifade ile video, birim zamanda art arda oynatılan imgeler dizisidir (Şekil 3).



Şekil 2. Sayısal imgenin temel yapısı.

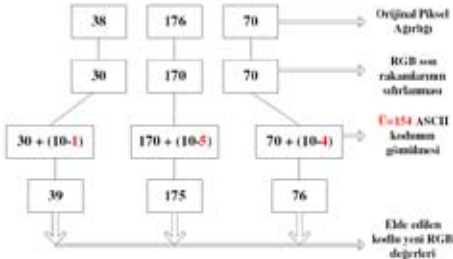
Bu bildiride sunulan GVVG uygulamasında 24 bit renkli imgeler kamera yardımı ile alınarak, bu temelde veri gizleme işlemleri gerçekleştirilmektedir.



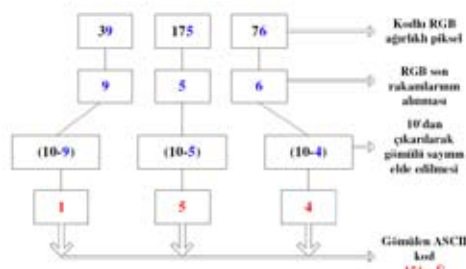
Şekil 3. Bir videonun temel yapısı.

3.2. GVVG Uygulamasının Algoritma Akış Şemaları

GVVG uygulaması, steganografi işlemini gerçekleştirerek için her bir piksel içerisine bir ASCII kodunun gömülmesi yaklaşımını kullanmaktadır [13]. İlk olarak Akar (2005)'in önerdiği bu yöntemde örneğin, RGB ağırlıkları (38, 176, 70) olan bir pikselin içerisine “Ü” harfinin ASCII karşılığı olan “(10011010)_{ascii} = 154” verisinin gömülmesi işlemi ve gömülü bilginin yeniden elde edilmesi işlem süreci sırasıyla Şekil 4 ve Şekil 5'te görülmektedir.



Şekil 4. Bir piksel içerisine bir ASCII kodunun gömülmesi.



Şekil 5. Bir pikselden gömülü ASCII kodun çıkarılması

GVVG algoritmasından geçen bir pikselin ilk RGB değeri ile gizli veri gömülü yeni RGB değeri arasında oluşan fark gözle algılanamayacak seviyededir ve bu sonuç renkli ve karşılaştırmalı olarak örnek bir piksel için Şekil 6'da sunulmaktadır. İnsanların görme duyusunun duyma gibi diğer duyularına kıyasla daha az hassas olması imgeler üzerindeki farklılıkların sezilememesinin ana sebepleri arasındadır [14].



(a) RGB:(38, 176, 70) (b) RGB:(39, 175, 76)

Şekil 6. Şekil 4'te işlenen pikselin büyültülmüş ilk (a) ve son (b) görüntüsü.

Sonuç olarak, taşıyıcı veri ve gömülecek gizli veriye bağlı olarak, piksel RGB değerlerinin en az LSB'si değişmekte ya da daha büyük değişiklikler meydana gelebilmektedir. Bu değişim imgenin RGB değerlerine ve gizli verinin ASCII değerine bağlı olarak farklılık gösterir. Şekiller 7 ve 8'de geliştirilen GVVG sisteminin, sırasıyla gizli veriyi gömme ve gömülü/gizli veriyi elde etme akış şemaları verilmektedir.

Resim içerisinde yer alan RGB piksel ağırlıklarının 250-255 arasında olması ve 1, 2, 3, 4 rakamlarından herhangi birisinin gömülecek ASCII kodunun bir rakamını oluşturması durumunda 255'in üzerinde, karşılığı olmayan bir kodlama sonucu elde edilecektir. Bu durumda hatalı sonuç oluşmaması için, orijinal pikselde düzenleme yapılarak 240-245 değerlerini almaları sağlanmaktadır. [13]'te önerilen algoritma, RGB imgeler için taşıyıcı dosya boyutunun yaklaşık 1/3'ü kadar gizli veri taşınmasını sağlamaktadır. Geliştirilen GVVG uygulaması ise bu algoritmanın gizli veri gömme kapasitesini, video oluşturarak kullanıcının istediği doğrultuda arttırmaktadır. Akış şemasında da görüldüğü gibi (Şekil 7), video içerisinde gizli veri olup olmadığı konusundaki bilgi “gizli veri var” örüntüsü ile verilmektedir ve bu özel kodlu bilgi uygulama içerisinde 64 bit olarak belirlenmiştir.

Tablo 1'de uygulamanın gerçekleştirildiği sistemin ve oluşturulan videonun temel özellikleri verilmektedir. Şekil 9'da ise, uygulama örneklerinden elde edilen bir videoya ait orijinal ve gizli veri gömülmüş video imgelerine yer verilmektedir.



Şekil 7. Gizli veri gömme akış şeması.



Şekil 8. Gömülü/gizli veriyi elde etme akış şeması.

Bilgisayar İşlemci Hızı ve Bellek Boyutu	Intel® Pentium® IV 3,2 GHz. 384 MB RAM
Kamera	Akita 100K Web-Cam
Çerçeve Oranı	25 fps
Çözünürlük	352 x 288 piksel
Dosya Tipi	.avi

Tablo 1. GVVG sistem özellikleri

En Büyük PSNR Değeri	En Küçük PSNR Değeri	Ortalama PSNR Değeri
46,2265	39,6939	42,3452

Tablo 2. GVVG sistem özellikleri

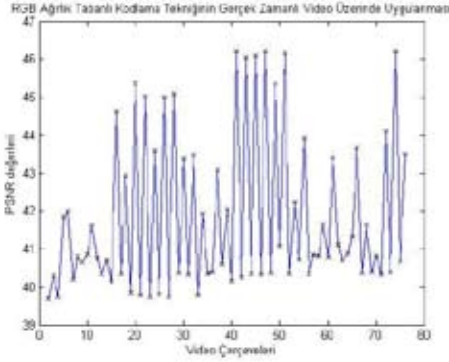


(a)

(b)

Şekil 9. GVVG uygulama örneği: orijinal (a) ve gizli veri içeren (b) video imgeleri

Tablo 2 video imgelerinin en büyük, en küçük ve ortalama Tepe Sinyal Gürültü Oranı (Peak Signal to Noise Ratio: PSNR) değerlerini göstermektedir. Video dosyasına ait her bir çerçevenin PSNR değerleri ise Ş ekil 10'da gösterilmektedir.



Şekil 10. Örnek uygulamada elde edilen video çerçevelerine ait PSNR değerleri

Yapılan çalışmaların başarımı hakkındaki en iyi fikri, benzer çalışmalardan elde edilen sonuçlarla yapılan karşılaştırmalar verir. Tablo 3'te, gerçekleştirilen çalışmanın literatürdeki eşlenikleri ile PSNR değerleri açısından karşılaştırılmasını sağlayacak değerler sunulmaktadır. PSNR değerleri açısından uygulama, literatürde kabul görmüş birçok yöntemle yaklaşık aynı sonuçları sağlarken, yüksek veri gömme kapasitesiyle ön plana çıkmaktadır. Ancak veri gömme algoritmalarının uygulanması sonucunda elde edilecek olan sonuçların örtü verisi ve gömü verisi arasındaki benzerlikler ile doğru orantılı olarak olumlu yönde artacağı unutulmamalıdır.

3.3. GVVG Uygulamasının Olumlu ve Olumsuz Yanları

Yapılan çalışmalar ve uygulamalarda belirlenen GVVG sistemine ait önemli özellikler özetle şöyle sıralanabilir:

- Veri gömme uygulamalarında, gizli veriyi içerecek olan taşıyıcı boyutunun önemi vurgulanır. Geliştirilen bu uygulama ile gömülmek istenen gizli veri/dosya boyutu göz önünde bulundurularak, ihtiyaç duyulduğu kadar taşıyıcı veri elde edilmekte ve gizli veri gömme işlemi yapılmaktadır.,
- Geliştirilen uygulama RGB ağırlık tabanlı kodlama tekniği ile taşıyıcı dosyanın yakla-

şık 1/3'ü kadar gizli veri gömme kapasitesi sağlamaktadır. Yüksek veri gömme kapasitesine rağmen PSNR değeri oldukça iyi seviyededir (Tablo 3).

- Video içerisinde gizli veri gömme işlemine bağlı olarak değişiklikler meydana gelmektedir. Bu durum, videoyu izleyenler tarafından fark edilemeyecek seviyededir.

Steganografi Çalışması	PSNR Değeri
Önerilen Çalışma	42,34 db
Chia-Chen Lin ve ark. [15]	42,69 db
Zhicheng Ni ve ark. [16]	40,20 db
Zhicheng Ni ve ark. [17]	40,00 db
Gwenael Doerr ve ark. [1]	39,00 db
Yuanjun Dai ve ark. [18]	33,47 db
Bijan G. Mobasser [19]	17,00 db
M.D. Swanson ve ark. [20]	24,60 db

Tablo 3. GVVG sisteminin başarımı

- Gizli veriyi taşıyan gerçek zamanlı videonun, veri gizleme işleminin gerçekleşmesinden önce var olmaması, gömülü/gizli veriyi taşıyan video dosyasına steganaliz işleminin yapılması durumunda, videonun orijinal hali ile karşılaştırma yapılamamasını sağlamakta ve gizli veri taşıdığına dair şüphe uyandırmamaktadır.
- Gerçekleştirilen çalışmanın yazılım tabanlı olması sayesinde, algoritmada isteğe bağlı olarak değişiklikler (örneğin yeni fonksiyon eklenmesi) yapılabilmektedir. Düşük maliyetli olması ve yükleme kolaylığı da uygulamanın olumlu yanları arasında yer almaktadır.

Geliştirilen GVVG sisteminin çeşitli olumsuzlukları da bulunmaktadır:

- Gizli veri gömme işlemi sonucunda oluşan videonun bir takım ataklara maruz kalması (kayıplı sıkıştırma, kırılma, satır/sütun silinmesi vb.) durumunda, gizli veride bozulmalar meydana gelmektedir. Zira işlemler bit düzleminde yapılmakta ve nispi olarak

küçük değerlikli bitlere veri gömülmektedir. Dolayısıyla ataklarda ilk etkilenen bit değerlerinin, içerisinde gizli verileri de barındıran düşük değerlikli bitler olacağı anlamına gelmektedir. Ancak böyle bir durumun gerçekleşmesi için, üçüncü kişilerin video içerisinde gizli veri olduğunu bilmeleri ya da tahmin etmeleri gerekmektedir.

- Son derece düşük bir olasılık olsa da, kimi video dosyalarının gizli veriyi taşımadığı halde, “gizli veri var” örneğine sahip olma ihtimali (2^{-64}) söz konusudur. Ancak, bu durumun gerçekleşme olasılığı, yazılımın esnekliği sayesinde “gizli veri var” örneğinin uzunluğu değiştirilerek, çok daha küçük değerlere indirgenebilmektedir.

4. Sonuç ve Değerlendirmeler

Bu bildiride bir veri ya da dosyanın gerçek zamanlı olarak elde edilen video çerçevelerine (imgelerine) RGB ağırlık tabanlı kodlama tekniği ile gömülmesi uygulaması gerçekleştirilmiştir. Geliştirilen GVVG sisteminin ilgili akış şemaları, algoritmalar ve uygulama örneğinden elde edilen sonuç imgeler sunulmuştur. Bu çalışmada önerilen yaklaşım, klasik veri gömme uygulamalarından farklı olarak, bir video dosyasının yaklaşık 1/3'ü kadar gizli veri gömme yeteneğine sahiptir ve yazılım tabanlı olması nedeniyle birçok eşleniğine nazaran daha yüksek başarımlı, esnek ve maliyeti düşüktür. Geliştirilen uygulamanın bahsi geçen özelliklerinin ilerleyen zamanlarda yapılacak olan başkaca çalışmalara önemli bir dayanak olabileceği değerlendirilmektedir.

5. Kaynaklar

- [1] Doerr, G., Dugelay, J., ‘Security Pitfalls of Frame-by-Frame Approaches to Video Watermarking’, IEEE Transactions on Signal Processing, October, 2004, Vol. 52, pp 2955-2964.
- [2] Koichi, T., Yoshifumi, F., ‘Development of Real-time Video Watermarking System Using

Media Processor’, Journal of the Institute of Image Information and Television Eng., 2004, Vol. 58, No. 12, pp 1820-1827.

[3] Owada, S., vd., ‘Development of Hardware Based Watermarking System’, Symposium on Cryptography and Information Security (SCIS'04), 2004, 3D5-2.

[4] Cox, I. J., Miller, M.L., ‘The First 50 Years of Electronic Watermarking’, Journal of Applied Signal Processing, 2002, Vol. 16, No. 4, pp 126-132.

[5] Tanaka, K., Nakamura, Y., Matsui, K., ‘Embedding a Secret Information into a Dithered Multi-level Image’, Proceedings of IEEE Military Communications Conference, 1990, pp 216-220.

[6] Hartung, F., Kutter, M., ‘Multimedia Watermarking Techniques’, Proceedings of the IEEE, 1999, Vol. 87, No. 7, pp 1079-1107.

[7] Yalman, Y., ‘Sayısal Ses İçerisinde Gizli Veri Transferinin Kablosuz Ortamda Gerçekleştirilmesi’, Yüksek Lisans Tezi, 2007, Kocaeli Üniversitesi F.B.E.

[8] Yalman, Y., Ertürk, İ., ‘Sayısal Ses İçerisinde Gizli Metin Transferinin Kablosuz Ortamda Gerçekleştirilmesi’, UMES'07, 20-22 Haziran 2007, Kocaeli, pp 41-45. [9] Adlı, A., Nakao, Z., ‘Three Steganography Algorithms for MIDI Files’, IEEE Proceedings of the Fourth International Conference on Machine Learning and Cybernetics, 2005. [10] Xu, C., Ping, X., Zhang, T., ‘Steganography in Compressed Video Stream’, Proceedings of the First International Conference on Innovative Computing, IEEE, 2006.

[11] Lee, C., Oh, H., Lee, H., ‘Adaptive Video Watermarking Using Motion Information’, Proceedings of SPIE, 2000, Vol. 3971, pp 209-214.

[12] Şahin, A., Buluş, E., Sakallı, M.T., ‘24-bit Renkli Resimler Üzerinde En Önemli Bite Ekleme Yöntemi Kullanarak Bilgi Gizleme’, *Trakya Üniversitesi J. Sci.*, 2006, pp 17-22.

[13] Akar, F., ‘Veri Gizleme ve Şifreleme Tabanlı Bilgi Güvenliği Uygulaması’, *Doktora Tezi, Marmara Üniversitesi Fen Bilimleri Enstitüsü*, 2005.

[14] Erçelebi, E., Subaşı, A., ‘Robust Multi Bit and High Quality Audio Watermarking Using Pseudo-Random Sequences’, *Computers and Electrical Engineering*, 2006, pp 525-536.

[15] Lin, C., Tai, W., Chang, C., ‘Multilevel Reversible Data Hiding Based on Histogram Modification of Difference Images’, *Pattern Recognition*, 2008, vol 41., pp 35823591.

[16] Ni, Z., Shi, Y., Ansari, N., Su, W., Sun, Q., Lin, X., ‘Robust Lossless Image Data Hiding Designed for Semi-Fragile Image Authentication’, *IEEE Transactions on Circuits and Systems for video Technology*, 2008, vol. 18, No. 4, pp 497-509.

[17] Ni, Z., Shi, Y. Q., Ansari, N., Su, W., Sun, Q., Lin, X., ‘Robust Lossless Image Data Hiding’, *IEEE International Conference on Multimedia And Expo (ICME)*, 2004, pp 2199-2202.

[18] Dai, Y., Zhang, L., Yang, Y., ‘A New Method of MPEG Video Watermarking Technology’, *Proceedings of ICCT*, 2003, pp 1845-1847.

[19] Mobasseri, B.G., ‘Direct Sequence Watermarking of Digital Video Using m-frames’, *IEEE*, 1998, pp 399403.

[20] Swanson, M.D., Zhu, B., Chau, B., Tewfik, A.H., ‘Object-Based Transparent Video Watermarking’, *IEEE*, 1997, pp 369-374.