Afyon Kocatepe Üniversitesi Fen ve Mühendislik Bilimleri Dergisi

Afyon Kocatepe University Journal of Science and Engineering

AKÜ FEMÜBİD **18** (2018) **015101** (888-894) AKU J. Sci. Eng. **18** (2018) **015101** (888-894)

DOİ: 10.5578/fmbd.67746

Araştırma Makalesi / Research Article

Dalgacık Dönüşümü Tabanlı Görsel Kriptoloji

Hülya Kodal Sevindir[1], Nilhan Sayın[2]

[1] *Kocaeli Üniversitesi, Fen Edebiyat Fakültesi, Matematik Bölümü, Kocaeli.*

[2] *Kocaeli Üniversitesi, Matematik Anabilim Dalı, Doktora Programı, Kocaeli.*

e-posta: hkodal@kocaeli.edu.tr

Geliş Tarihi:03.01.2018; Kabul Tarihi:04.12.2018

Anahtar kelimeler
Dalgacık Dönüşümü; Halftone Tekniği; Kriptoloji; Stenografi.

Özet

Günlük hayatta kişi, kurum ve kuruluşlar tarafından kullanımı hızla artan bankacılık işlemleri, e-posta gönderimi ve alımı, sanal alışveriş gibi işlemler bilgi güvenliğinin önemini de giderek arttırmıştır. Bilgi güvenliğini sağlamak için bir çok yöntem vardır. Bu çalışmada, bu yöntemlerden biri olan görsel kriptografi kullanılmıştır. Bilgi aktarımı sırasında, gönderilecek olan veriler dalgacık dönüşümüne dayalı belirli bir algoritmaya bağlı olarak şifreli paylara ayırılmıştır. Daha sonra ayrılan paylar anlamlı görüntülere gömülerek, hem gönderilen verilerin güvenliği sağlanmaktadır, hem de şifrelenmiş paylara ayrılan verinin dikkat çekmesi önlenmektedir.

Visual Cryptology Based on Wavelet Transform

Keywords
Wavelet Transform; Halftone Technique; Cryptology; Stenography.

Abstract

Transmissions such as bank transactions, e-mail sending and retrieval, virtual shopping, etc. has become more and more common by people, institutions and organizations in daily life. This has also increased the importance of information security. There are many ways to ensure information security. In this study, one of these methods, visual cryptography, is used. During the data transfer, the data to be transmitted is divided into encrypted shares depending on a certain algorithm based on wavelet transfom. Then, the allocated shares are buried into meaningful images. Doing so, both the security of the transmitted data is ensured and the attention to the data which is divided into the encrypted shares is prevented.

1. Giriş

Teknolojinin gelişmesiyle birlikte kişi, kurum ve kuruluşların bilgiye ulaşma isteği artmış ve bilgiye ulaşması kolaylaşmıştır. Dünya çapında haberleşme ve veri transferinde internetin kullanılmaya başlanması ile bilgi ve veri güvenliğinin sağlanması gerekli hale gelmiştir. Tarih öncesi çağlarda daha ilkel yöntemlerle saklanan bilgiler, süper bilgisayarların gelişmesiyle dijital ortamda şifrelenmeye başlamıştır. Özellikle 2. Dünya Savaşı sırasında gelişme gösteren şifreleme bilimi, birçok yöntem ve makinenin üretilmesi ve geliştirilmesini sağlamıştır.

Görsel verilerin aktarımında kullanılan görsel kriptoloji şeması, 1994 yılında Naor ve Shamir tarafından bulunmuş ve uzun yıllar boyunca birçok şifreleme işleminde kullanılmıştır. Naor ve Shamir (1994)'e göre insanların görme sistemiyle çözülebilen bu görsel kriptoloji şeması, sır paylaşım tekniği tabanlıdır. İkili bir sır görüntüsünden elde edilen rastgele pay görüntüleri, genellikle asetat kağıtlarına basılarak katılımcılara paylaştırılmakta ve bu paylar üst üste birleştirildiğinde sır görüntüsü ortaya çıkmaktadır.

İkili görüntüleri gizleme ile başlayan görsel kriptoloji tekniği daha sonraları renkli görüntülere de uygulanmaya başlanmıştır. Sır paylaşım şemasını renkli görüntüye uygulayabilmek için, renkli görüntüyü ikili görüntüye çeviren halftone tekniği geliştirilmiştir. Halftone tekniği ile ikili görüntüye dönüştürülen renkli sır görüntülerine, sır paylaşım

şeması uygulanarak pay görüntüleri elde edilmektedir.

Stenografi ise metin, ses, görüntü ve video dosyalarını gizlemede sıklıkla kullanılan bir veri gizleme yöntemidir. Temel mantığı gönderilmek istenen asıl veriyi, başka bir veri içerisine gömerek alıcıya ulaştırmaktır. Gizli verinin, gönderilen veri içerisine gömülü olduğunu sadece gönderici ve alıcı bilmektedir; bu sebeple, gönderim esnasında veri, üçüncü bir şahsın eline geçse bile verinin güvenliği korunacaktır.

Bu çalışmada önerilen yöntemde, üretilen kriptografik payların anlamlı görüntüler içerisine gömülmesi ile hem dikkat çekmesini önlemiş hem de sır görüntülerinin güvenliğini arttırmış olmaktayız. Gönderilen stego görüntülere veri gömüldüğü anlaşılsa bile, veri çıkarma anahtarını bilmeyen üçüncü şahıslar, paylara ulaşamayacaktır. Sır paylaşımı yöntemiyle bir kişinin sorumluluğundan çıkarılıp bir grubun sorumluluğuna giren sır görüntüsü, ancak tüm anlamlı stego görüntülerden çıkarılan payların bir araya getirilmesiyle ortaya çıkacaktır.

2. Materyal ve Metot

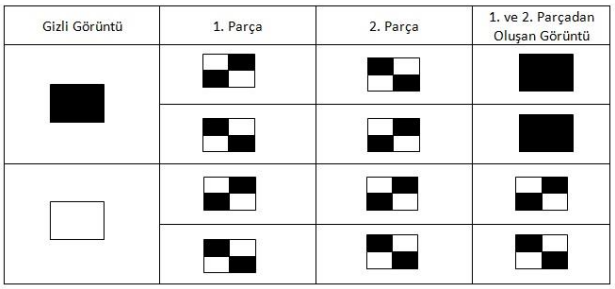
Geleneksel görsel kriptoloji şemasında, sır görüntüsü girdi olarak kullanılır ve sır görüntüsünden elde edilen anlamsız paylar elde edilen çıktılardır. Bu pay çıktılarından ilk pay rastgele üretilmektedir. Diğer pay ise ilk paya Boolean Cebri kurallarına bağlı kalarak üretilmektedir. Görsel kriptoloji şemasında paylar, sır görüntüsü hakkında hiçbir bilgi vermemektedir.

Payların oluşturulmasında ve birleştirilmesinde Boolean Cebrinin OR ve XOR işlemleri kullanılabilmektedir.

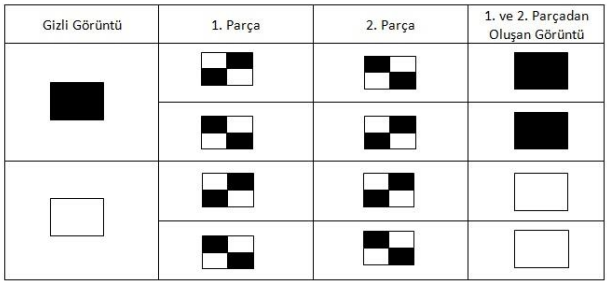
Çizelge 1. OR ve XOR tabanlı VSS

Gizli Veri	1. Pay (Rastgele)	2. Pay (1. paya OR işlemi ile bağlı)	2. Pay (1. paya XOR işlemi ile bağlı)
10111011	10101010	10011011	11101110

Gizli bir veri, Çizelge 1'de gösterildiği şekilde Boolean Cebri işlemleriyle paylara ayrılabilmektedir. Şekil 1'de verildiği gibi OR yöntemiyle üretilen payların birleştirilme aşamasında siyah piksellerde doğru sonuç elde edilmektedir fakat beyaz piksellerde sıkıntı çıkmaktadır. Rastgele üretilen paylarda siyah ve beyaz piksellerin birleştirilmesi sonucunda beyaz piksel oluşması beklenirken siyah piksel elde edilmektedir. Bunun sonucunda elde edilen görüntü, gürültülü bir görüntüdür. Bu sıkıntı Şekil 2'deki gibi XOR işlemiyle giderilmiştir.



Şekil 1. Siyah ve beyaz pikselli görüntülerin OR işlemiyle paylaştırılması



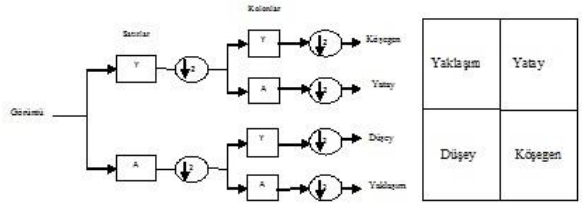
Şekil 2. Siyah ve beyaz pikselli görüntülerin XOR işlemiyle paylaştırılması

Çalışmamızda renkli görüntülerin ikili görüntüye dönüştürme aşamasında Floyd-Steinberg Halftone Tekniği kullanılmıştır. Bu teknik hata difüzyon filtresini esas almaktadır. Halftone yöntemi kullanılarak, 0-255 aralığındaki piksel değerlerine sahip olan görüntünün piksel değerleri, 0 ve 255 değerlerine dönüştürülür. 255 değerindeki beyaz piksellere de 1 değeri verilerek ikili (siyah-beyaz) görüntü elde edilmiş olur.

Üretilen paylar anlamsız görüntülerdir ve bu anlamsız pay görüntülerini, anlamlı kapak görüntülerine gömmek için LSB yöntemi esas alınmıştır. LSB yöntemi, en az anlamlı biti değiştirmeyi esas alan bir yöntemdir ve görüntünün gömüleceği kapak görüntünün her pikselinin, her baytının son biti değiştirilir. Değiştirilecek bitlerin yerine sır görüntüsünün bitleri sırayla ve teker teker yerleştirilir. Baytın en az anlamlı biti olan sekizinci

biti değiştirildiğinden ortaya çıkan stego görüntüdeki değişimler insanın görme sistemi tarafından algılanmaz.

Veri gömme aşamasında dalgacık dönüşümü kullanılmaktadır. İki boyutlu (2B) dalgacık dönüşümleri, bir boyutlu (1B) dalgacık dönüşümlerinde uygulanan yöntemin satır ve sütun olarak genişletilmiş bir uygulamasıdır. Şekil 3'te bir görüntünün bir defa dalgacık dönüşümüne tabi tutulması görülmektedir.



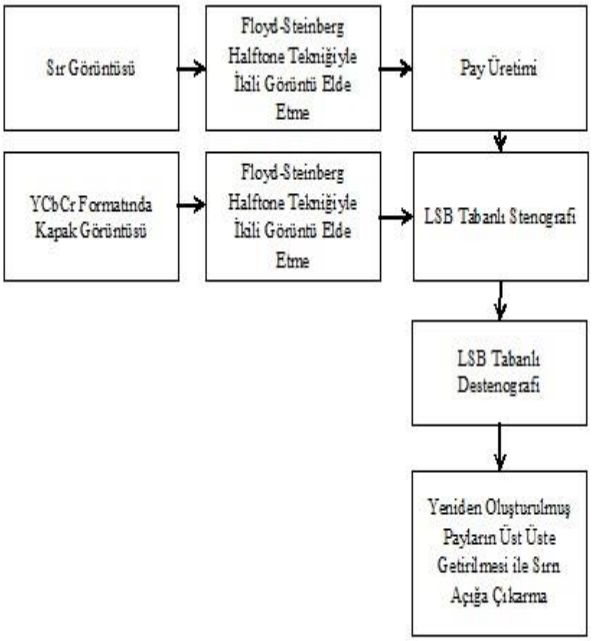
Şekil 3. Birinci seviyede İki boyutlu dalgacık dönüşümü

Ergen ve Baykara (2011)'e göre her kapak görüntünün Y katmanının satırları, alçak (L) ve yüksek (H) geçirgen filtrelerden geçirilir. Geçirildiği filtre tipine göre yaklaşım (AA), düşey (AY), yatay (YA) ve köşegen (YY) dalgacık dönüşümü sonucu katsayılar elde edilir. Görüntü, dalgacık dönüşümü kullanılacak uygulamanın gerektirdiği kadar filtreden geçirilebilir ve ayrıştırma yapılamayacak en küçük görüntü elemanı kalıncaya kadar örnek azaltımı yapılabilir. Örnek azaltımından elde edilen bu katsayılar iki boyutlu görüntülerdir.

Çalışmada RGB formatında olan kapak görüntüleri, YCbCr formatlı görüntülere dönüştürülmüştür. YCbCr formatlı görüntülerin her birinin Y katmanı, 1. seviyede Ayrık Dalgacık Dönüşümü filtresinden geçirilmiştir ve bu işlemden elde edilen düşey (AY), yatay (YA) ve köşegen (YY) katsayılarına, sır görüntüsünün payları gömülmüştür. Gömülme sonucunda her görüntüden elde edilen yeni yatay, dikey ve köşegen alt bantlar ile her görüntüden ayrı ayrı elde edilen Y katmanlarının yaklaşım (AA) katsayılarına, Ters Dalgacık Dönüşümü uygulanarak stego görüntüler elde edilir.

3. Uygulama Adımları

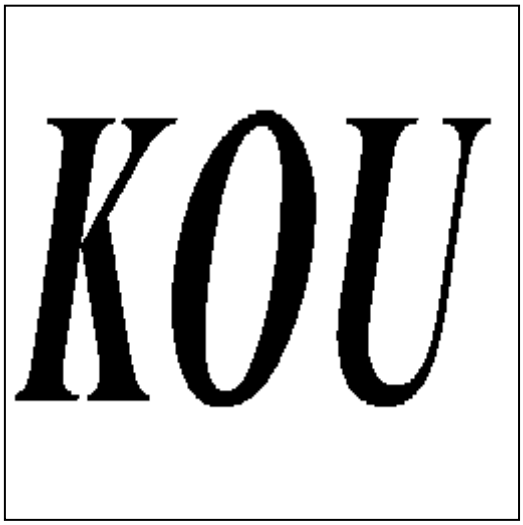
Bu çalışmada iki uygulama önerildi. Uygulamaların pay üretim aşamaları farklı olup, stenografi ve sırrı tekrar elde etme aşamaları ortaktır. Uygulamaların adımları Şekil 4'te verilmiştir.



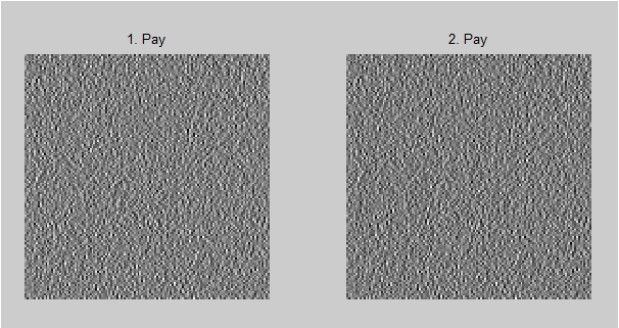
Şekil 4. Kullanılan görsel stenografi şeması

3.1. Uygulamanın Pay Üretim Aşaması

Birinci uygulamada Şekil 5'teki ikili görüntü kullanılmıştır. Sadece 0 ve 1 değerlerinden oluşan görüntü, Naor ve Shamir'in sır paylaşım yöntemi esas alınarak Şekil 6'daki gibi, XOR yöntemine göre iki paya ayrılmıştır. Üretilen paylardan birincisi rastgele üretilmiştir ve ikinci pay birinci paya XOR işlemine göre bağlıdır.



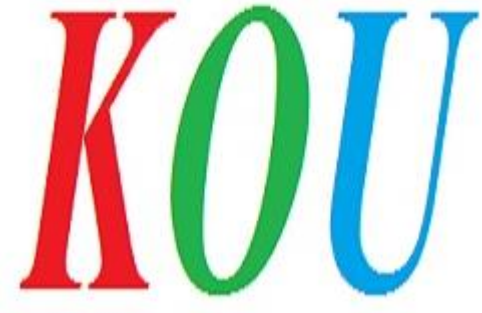
Şekil 5. İkili örnek sır görüntüsü



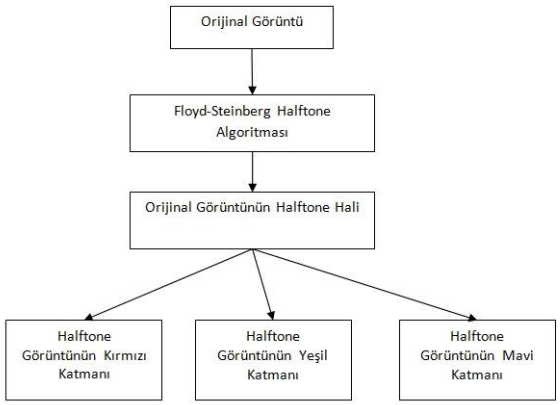
Şekil 6. Sır görüntüsünden XOR işlemiyle elde edilen paylar

İkinci uygulamada kullanılan görüntü, Şekil 7'deki gibi, 24 bit RGB görüntüdür. İkili görüntü elde etmek için alınan sır görüntüsüne Floyd-Steinberg halftone tekniği uygulanır. Bu uygulama iki şekilde denenmiştir. Renkli görüntüler için ilk uygulamanın algoritması Şekil 8'de verilmiştir. Öncelikle görüntü, Şekil 9'daki gibi halftone görüntüye dönüştürülmüştür. Daha sonra Şekil 10'daki gibi R-G-B katmanlarına ayrılarak, Şekil 11'deki paylar elde edilmiştir.

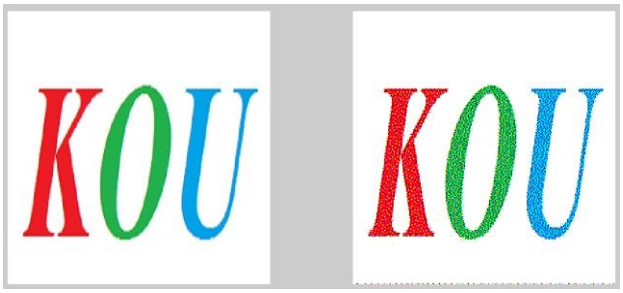
Renkli görüntüler için ikinci uygulamada, Şekil 7'de verilen sır görüntüsü ve Şekil 12'de verilen algoritma kullanılmıştır. Sır görüntüsü, önce Şekil 13'deki gibi R-G-B katmanlarına ayrılmış ve her katman halftone görüntüye dönüştürülerek, Şekil 14'teki gibi paylar elde edilmiştir. Bu iki durumda da elde edilen sır görüntülerinin PSNR değerleri verilmiştir.



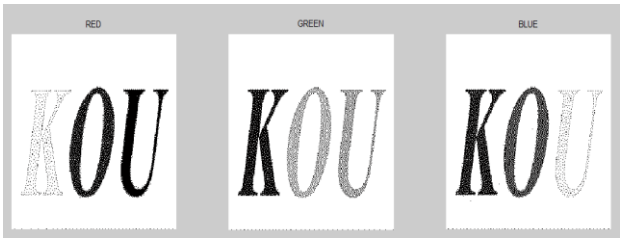
Şekil 7. 2. durumda kullanılacak renkli sır görüntüsü



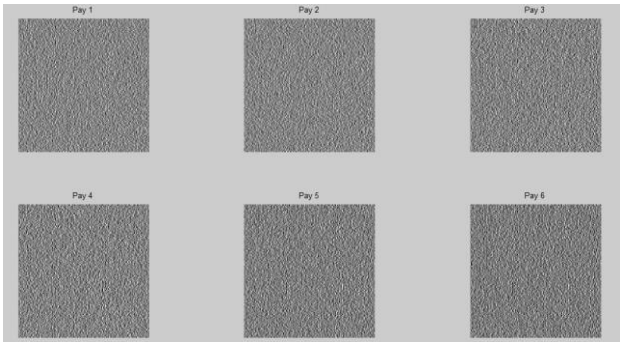
Şekil 8. 1. durumda renkli görüntünün halftone görüntüye dönüşüm şeması



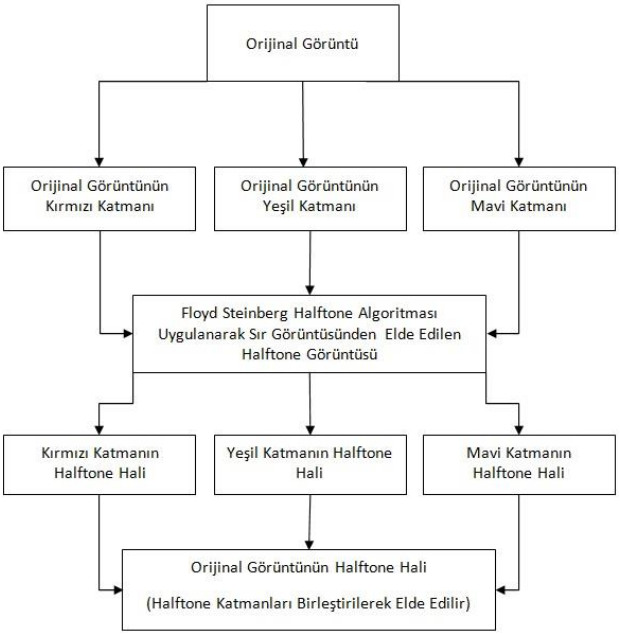
Şekil 9. 1. durumda renkli görüntünün halftone görüntüye dönüşümü



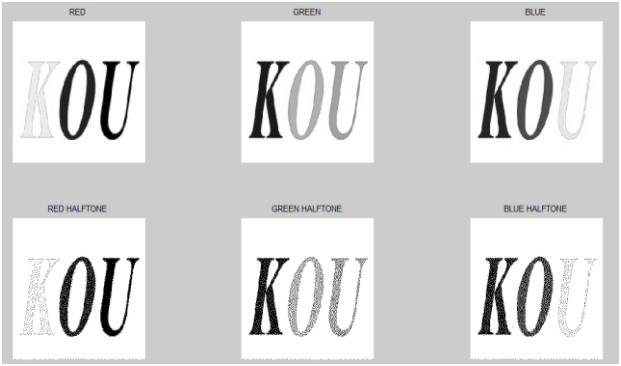
Şekil 10. 1. durumda halftone görüntünün R-G-B katmanları



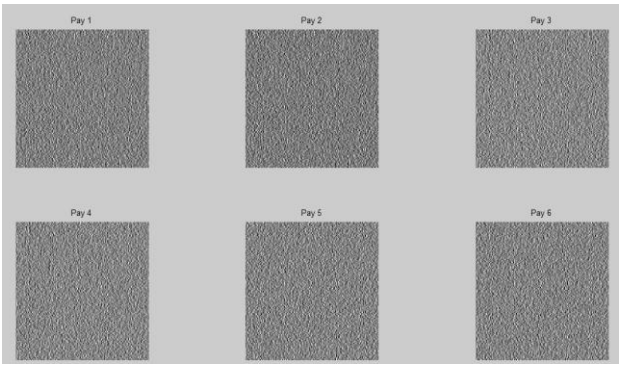
Şekil 11. 1. durumda üretilen paylar



Şekil 12. 2. durumda renkli görüntünün halftone görüntüye dönüşüm şeması



Şekil 13. 2. durumda renkli görüntünün katmanlara ayrılmış hali ve katmanların halftone görüntüsü

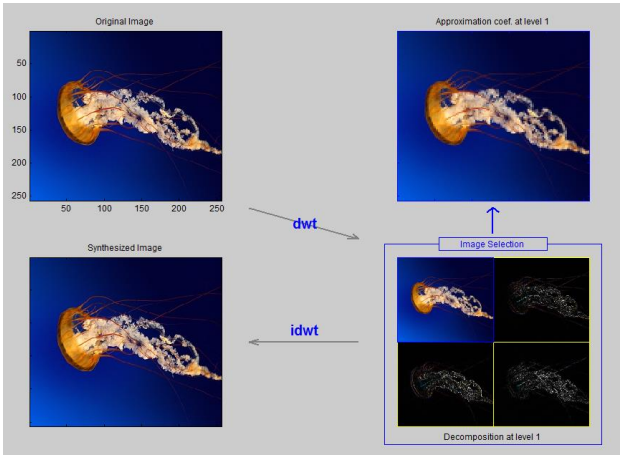


Şekil 14. 2. durumda renkli görüntüden pay üretimi

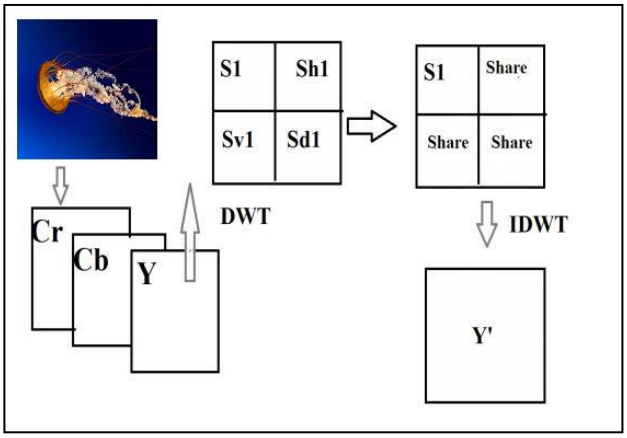
3.2. Stego Görüntü Oluşturma

Seçilen RGB formatındaki kapak görüntüleri YCbCr formatına dönüştürülmüştür. Elde edilen yeni formattaki Y katmanı görüntünün parlaklık katmanıdır ve pay görüntüleri bu katmana gömülmektedir.

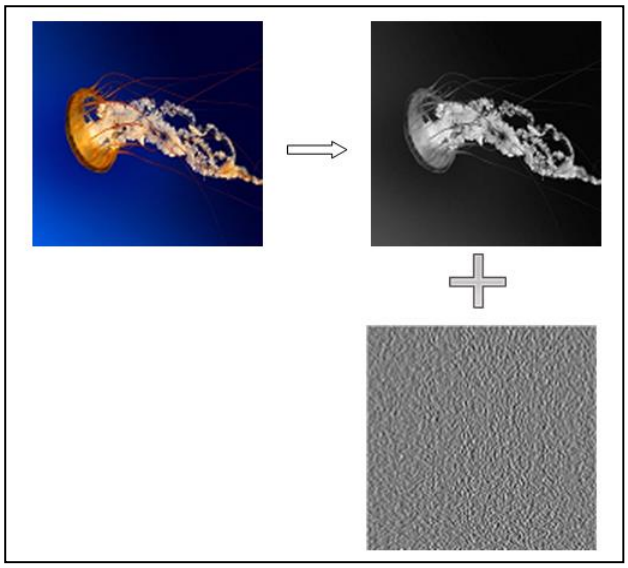
Y katmanına 1. seviyeden 2 boyutlu Ayrık dalgacık dönüşümü uygulanarak, Şekil 15 ve Şekil 16'daki gibi alt bantlar elde edilir. Şekil 16'da verildiği gibi yatay, dikey ve köşegen alt bantlara paylar gömülür. Her bir kapak görüntüsünün üç alt bandına tek bir pay görüntüsü, Şekil 17'deki gibi gömülmektedir. Bu yüzden pay sayısı kadar kapak görüntüsü seçilmelidir.



Şekil 15. Rastgele bir pay görüntüsünün 1. dereceden dalgacık ayrıştırması



Şekil 16. Kapak görüntüsünden dalgacık dönüşümü ile stego görüntü elde etme



Şekil 17. Kapak görüntüsüne pay gömme

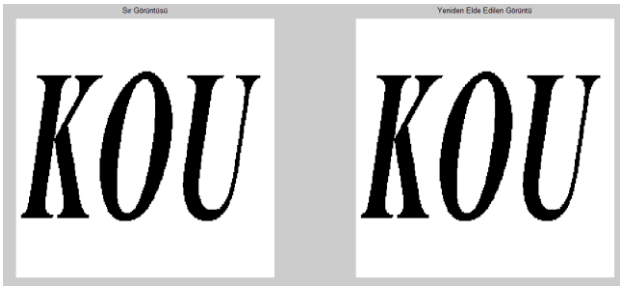
3. Bulgular

Bu çalışmada, paylar, görsel verilerden Shamir algoritması kullanılarak elde edildi. Seçilen kapak görüntülerinin Y katmanına dalgacık dönüşümü uygulandıktan sonra elde edilen alt bantlara paylar gömüldü ve elde edilen stego görüntüler katılımcılara dağıtıldı. Bir araya gelen katılımcılardan alınan stego görüntülerden ters dalgacık dönüşümü ile paylar tekrar elde edildi. Payların XOR yöntemiyle birleştirilmesi sonucunda elde edilen görüntü üzerindeki değişiklikler ve sır görüntüsü ile elde edilen görüntü arasındaki farklılıklar incelendi. Kullanılan görsel veriler MATLAB paket programında uygun kodlar yazılarak sonuçlar elde edildi. MATLAB paket programındaki dalgacık kodlarından yararlanıldı. Uygulamalarda sır görüntüsü olarak ikili ve 24 bit RGB olmak üzere 256x256 boyutunda iki sır görüntüsü ve rastgele seçilen altı tane, 24 bit, 256x256 boyutunda, RGB kapak görüntüleri kullanılarak analiz edildi ve sır paylaşımından elde edilen sonuçların PSNR değerleri hesaplandı.

Çizelge 2. PSNR Hesaplamaları

Kullanılan yöntem	Sır görüntüsü ve elde edilen görüntü arasındaki PSNR hesabı	Sır görüntüsünün halftone görüntüsü ve elde edilen görüntü arasındaki PSNR hesabı
İkili görüntü	Sonsuz	Sonsuz
RGB görüntü ve 1. uygulama	15.8123	Sonsuz
RGB görüntü ve 2. uygulama	15.8123	Sonsuz

Çizelge 2'de gösterildiği gibi ikili görüntülerde sır görüntüsüyle elde edilen görüntü arasında herhangi bir piksel kaybı olmamaktadır ve Şekil 18'deki gibi birebir aynı görüntü elde edilmektedir.



Şekil 18. İkili görüntülerde sır görüntüsü ve elde edilen görüntü

RGB görüntülerde ise elde edilen görüntü ile sır görüntülerinin halftone halleri arasında Şekil 19'da verildiği gibi, herhangi bir fark olmamaktadır. İki uygulamada da sır görüntüsünün halftone hali ile elde edilen görüntü birebir aynıdır. Format değişikliğinden ve piksel değer aralığından kaynaklı olarak sır görüntüsünün RGB formatı ile elde edilen görüntü arasındaki PSNR değeri 15.8123 olarak elde edilmektedir.

Şekil 19. RGB görüntülerde sır görüntüsü, sırrın halftone görüntüsü ve elde edilen görüntü

4. Tartışma ve Sonuç

Bu çalışmada sunduğumuz yöntem ile, Lekshmi (2015) de yapılan ikili görüntülerde halftone algoritmasının uygulanmasının gereğinin olmadığı gösterilmektedir. Halftone algoritmasının uygulanmaması sonucunda, programın bir adım eksik işlem yapması nedeniyle algoritma daha hızlı sonuç verecektir.

Bu çalışmada, RGB görüntülerde kullanılan halftone algoritması Floyd-Steinberg halftone algoritmasıdır. Lekshmi (2015) çalışmasında halftone görüntü elde etmek için kullanılan Otsus Threshold yöntemi yerine kullanılan Floyd-Steinberg halftone yöntemi aynı sonuçları vermektedir.

5. Kaynaklar

Ergen B., Baykara M., 2011. Dalgacık Ve Dalgacık Paket Ayrıştırması İle İmgelerden Gürültü Temizlemesi Analizi. *e-Journal of New World Sciences Academy*, 6, **2**, 518-526.

Lekshmi S. J., Anil A. R., 2015. Secure Visual Secret Sharing Based On Discrete Wavelet Transform. *ICTACT Journal On Image And Video Processing*, 6, **1**, 1072-1075.

Leung B. W., Ng F. Y., Wong D. S., 2009. On The Security Of A Visual Cryptography Scheme For Color Images. *ELSEVIER Pattern Recognition,* 42, 929-940.

Liu F., Wu C.K., Lin X.J., 2008. Colour Visual Cryptography Schemes. *IET Inf. Secur*., 2, **4**, 151-165.

Liu G., Zhang Z., Dai Y., 2010. Improved LSB-matching Steganography for Preserving Second-order Statistics*. Journal Of Multimedia,*5, **5,** 458-463.

Naor M., Shamir A., 1994. Visual Cryptography. *The Proceedings Of The Conference on Advances in Cryptology EUROCRYPT'94*, 950, 1-12.

Patil S., Tajane K., Sirdeshpande J., 2013. Analysing Secure Image Secret Sharing Schemes Based On Steganography. *Internatıonal Journal Of Computer Engineering & Technology* (IJCET), 4, **2**, 172-178.

Saichandana B., Srinivas K., Kumar R. K., 2010. Visual Cryptography Scheme For Color Images. *International Journal of Computer Engineering and Technology (IJCET),* 1, **1**, 207-212.

Shyu S. J., 2009. Image Encryption By Multiple Random Grids. *ELSEVIER Pattern Recognition*, 42, 1582-1596.

Qiao W., Yin H., Liang H., 2009. A Kind of Visual Cryptography Scheme For Color Images Based On Halftone Technique. *2009 International Conference on Measuring Technology and Mechatronics Automation,* 294, 393-395.

Verma J., Khemchandani V., 2012. A Visual Cryptographic Technique To Secure Image Shares. *International Journal Of Engineering Research And Applications (IJERA)*, 2, **1**, 1121-1125.

Wu X., Sun W., 2014. Extended Capabilities For XOR-Based Visual Cryptography. *IEEE Transactions On Information Forensics And Security*, 9, **10**, 1592-1605.

İnternet kaynakları

1- ab.org.tr/ab06/bildiri/100.pdf, (10.06.2017)