Morley'in Teoremine Dayalı Gizli Görüntü Paylaşım Şeması

Vasif Nabiyev, Mustafa Ulutaş, Güzin Ulutaş
Karadeniz Teknik Üniversitesi, Bilgisayar Mühendisliği Bölümü
vasif@ktu.edu.tr, ulutas@ktu.edu.tr, gulutas@ktu.edu.tr

Özetçe

Shamir Lagrane'ın interpolasyonuna dayanan sır paylaşım yöntemini 1979'da önermiştir. Blakley, aynı yıl içerisinde hiper düzlemlerin kullanımına dayalı farklı bir yaklaşımda bulunmuştur. Son yıllardaki çalışmalar her iki yöntemi, gizli görüntülerin paylaşımı için kullanmıştır. Çalışmada düzlem geometrisindeki Morley'in üçe bölenler teoremi gizli görüntülerin paylaşımında kullanılmıştır. Taban uzunluğu ve x ekseni ile arasındaki açı gizli veriyi temsil ederken, dış üçgenin köşe noktaları pay görüntülerindeki piksel parlaklık değerlerini temsil edecektir. Elde edilen deneysel sonuçlar pay görüntülerinin gizli görüntü hakkında bilgi içermediğini göstermiştir. Yeniden yapılandırılan gizli görüntü ise yaklaşık olarak 50.39 dB PSNR değerine sahiptir.

Abstract

A Secret Image Sharing Scheme Based on Morley's Theorem

Shamir proposed a technique to share a secret among n participants. His method is based on the Lagrange's interpolation technique. Blakley proposed a different approach based on hyperplane equations to share a secret. Researchers used both methods in recent years to share a secret image among participants. We propose to use a theorem in plane geometry to share a secret image in this paper. A mathematician, Frank Morley discovered Morley's trisector theorem which states that, three points of intersections of the adjacent angle trisectors of any triangle form an equilateral triangle, called the Morley's triangle. In this study, we use the Morley's theorem to share a secret image among participants. Morley's triangle is used to code the secret pixel values. Base length and orientation angle with respect to x-axis of the Morley's triangle are the secrets whereas vertices of the outer triangle based on inner triangle constitute share pixels. Experimental results indicate that shares do not reveal information about the secret image. A small reconstruction error of magnitude one due to the round operation and trisection procedure may arise during the revealing procedure. Reconstructed secret image has about 50.39 dB PSNR which the human visual system is incapable of perceive.

1. Giriş

Ağ teknolojisinin hızlı ilerleyişi, kablosuz ve mobil cihazların sayısındaki artış, sayısal verinin internet üzerinden aktarımını yaygınlaştırmıştır. İletilen verinin askeri bir görüntü yada ticari önem taşıyan bir veri olması durumunda, veri güvenliğinin sağlanması bir zorunluluktur. Kriptografi ve steganografi, veri güvenliğinin sağlanmasında kullanılan bilinen en yaygın iki tekniktir. Kriptografi kullandığı anahtar değeri yardımıyla, veriyi farklı bir biçime dönüştürmektedir. Steganografi ise gizli veriyi dikkat çekmeyecek başka bir ortam içerisine saklama sanatıdır. Saklamada kullanılan ortam dikkat çekmeyecek herhangi bir sayısal ortam olabilir. Gizli verinin örten ortama saklanmasından sonra elde edilen yeni sayısal bilgi stego ortam olarak adlandırılmaktadır. Her iki yöntemdeki en büyük problem, şifreli verinin yada stego verinin tek bir ortamda tutulmasıdır. Ortamın kötü niyetli kişiler tarafından tahrip edilmesi yada bozulması durumunda, gizli veri yeniden elde edilemeyecek şekilde bozulacaktır. Bu nedenle son yıllarda sır paylaşım şemaları gizli verilerin paylaşımında kullanılmaktadır.

Sır paylaşım şemaları ilk olarak Shamir ve Blakley tarafından ayrı zamanlarda önerilmiştir [1, 2]. Shamir'in sır paylaşma yöntemi polinomial interpolasyona dayanırken, Blakley'in yöntemi hiper düzlem teorisinden faydalanmaktadır. Eşik sır paylaşım şeması olarak da adlandırılan her iki yöntem, gizli veriyi n kişi arasında dağıtır. Katılımcılardan her biri pay olarak adlandırılan ve gizli veri hakkında bilgi içeren değerlere sahiptir. En az k tane katılımcının bir araya gelmesi durumunda gizli veri yeniden yapılandırılabilmektedir. k-1 yada daha az katılımcının bir araya gelmesi durumunda,

gizli veri hakkında herhangi bir bilgi elde edilemeyecektir.

Thien ve Lin, 2002 yılında, Shamir'in sır paylaşım şemasını, gizli görüntülerin paylaşımında kullanmıştır [3]. Yöntemde gizli görüntü *n* kişi arasında paylaştırılmaktadır. Katılımcılara gizli görüntünün $1/k$ 'sı büyüklüğünde ve gürültü benzeri pay görüntüleri dağıtılır. Pay görüntülerinin en az *k* tanesinin bir araya gelmesi durumunda, gizli görüntü yeniden elde edilmektedir. [4]'deki çalışma pay görüntülerinin gürültü benzeri olmasının kötü niyetli kişilerin ilgisini çekeceğine vurgu yapmaktadır. Steganografi kullanılarak pay görüntülerinin örten ortam içerisine yerleştirilmesini önerdikleri çalışmada, üretilen pay değerleri örten görüntü içerisinde 2×2'lik bloklara saklanır. Bu nedenle *N*×*M* büyüklüğündeki gizli görüntüden elde edilen pay görüntülerinin saklanmasında 2*N*×2*M* büyüklüğündeki örten görüntüler kullanılmaktadır. Aynı zamanda stego görüntülerin katılımcılar tarafından doğrulanmasını sağlamak amacıyla eşlik bitinin kullanımı önerilmiştir.

[5]'deki çalışma stego görüntülerin doğrulanması esnasında eşlik bitinin kullanımının anlamlı olmadığına, bunun yerine anahtarlı özüt fonksiyonlarının daha güvenli olduğuna vurgu yapmıştır. Aynı zamanda pay değerlerini saklama esnasında yeni bir düzen önermişler ve elde edilen stego görüntülerin PSNR değerini iyileştirmişlerdir. Yeniden yapılandırılan gizli görüntüdeki 251 ve üzerindeki piksel parlaklık değerlerinin de korunabilmesi için Galois Field (2^8)'i Shamir'in polinomunda kullanmışlardır.

[6]'daki çalışma doğrulama bitlerinin üretilmesi için Çinli Kalan Teoreminden (ÇKT) faydalanmış ve doğrulama için örten bloklara 4 doğrulama biti yerleştirmiştir. Yöntem doğrulama oranını iyileştirse dahi, üretmiş olduğu stego görüntülerin PSNR değeri diğer çalışmalara kıyasla daha düşük olmuştur.

[7]'deki çalışma piksel değeri farklılıkları yöntemini kullanarak, pay değerlerinin örten görüntülere saklanmasını gerçekleştirmiştir. Önerilen yöntem aynı zamanda Rabin şifreleme sistemini de kullanmaktadır. Diğer yöntemlere kıyasla daha büyük gizli görüntüleri saklayabilmekte ve stego görüntüleri kullanarak örten görüntü piksel değerlerine erişebilmektedir.

Pay görüntülerinin anlamlı hale getirilmesi ve üretilen stego görüntülerin doğrulanmasını sağlayan bu çalışmalar dışında, pay görüntülerinin büyüklüğünün küçültülmesini hedefleyen araştırmalar da yer almaktadır. [8]'deki çalışma [4]'deki çalışmaya oranla %40 oranında küçük pay görüntüleri üretmiştir. Pay görüntülerindeki küçülme oranı depolama gereksinimleri ve iletim zamanı açısından iyileştirme sağlamıştır. Fakat önerilen bu yöntem renkli görüntülere uyarlanamamaktadır. [9]'daki çalışma renkli gizli görüntüleri paylaştırırken daha küçük pay görüntüleri üretmeyi başarmıştır.

[10]'daki çalışmada, gizli görüntü paylaşım şemalarında stego görüntüleri yerine farklı görüntüler üreterek, tarafları kandırmayı amaçlayan kişileri engellenmesi hedeflenmiştir. Önermiş oldukları yöntem [3]'deki çalışmayı temel almaktadır. Gizli görüntü paylaşım şemalarında kandırılma olasılığını ortaya koyan ilk çalışma olmuştur.

Bahsi geçen araştırmalarda gizli görüntünün yeniden yapılandırılabilmesi için en az *k* tane pay görüntüsünün bir araya gelmesi gerekmektedir. Bunun sonucunda gizli görüntü elde edilir. [11]'deki çalışmada yazarlar kademeli gizli görüntü paylaşımı olarak adlandırılan yeni bir yöntem önermişlerdir. Önerilen yöntemde *k* adet pay görüntüsünün toplanması durumunda gizli görüntü belirli bir oranda yapılandırılmaktadır. Bir araya gelen kişi sayısı arttıkça , elde edilen gizli görüntü kalitesi iyileşecektir. [12]'deki çalışmada ise kademeli gizli görüntü paylaşımı için ayrık Dalgacık dönüşümü kullanılmıştır. [11]'deki yönteme kıyasla üretmiş oldukları pay görüntüleri daha küçüktür.

Son yıllarda Shamir'in yöntemine dayanan gizli görüntü paylaşım şemaları ağırlık kazansa bile, Blakley'in yöntemini gizli görüntülerin paylaşımında kullanan yeni çalışmalarda mevcuttur [13, 14]. [13]'deki çalışma gizli görüntüleri Blakley'in yöntemini kullanarak paylaştırmıştır. Yalnız üretilen pay görüntüleri gürültü özelliği taşımaktadır. [14]'deki çalışma Steganografi kullanarak Blakley'in yöntemi ile üretilen pay görüntülerinin anlamlı örten görüntüler içerisine saklanmasını sağlamıştır. Aynı zamanda bu yöntem depolama gereksinimleri ve iletim zamanında da iyileştirme sağlamıştır.

Gizli görüntü paylaşımı ile uğraşan çalışmalarda iyileştirilmesi hedeflenen belirli unsurlar vardır:

depolama gereksinimleri, iletim zamanı, anlamlı paylar, payların doğrulanması ve kandırılmaların engellenmesi. Literatürdeki bu unsurların düzeltilmesini hedefleyen gizli görüntü paylaşım şemaları ise Shamir'in yada Blakley'in yöntemini temel almaktadır.

Bu çalışmada Morley'in teoremine dayanan yeni bir gizli görüntü paylaşım tekniği önerilmiştir. Teoreme göre, herhangi bir üçgenin komşu açılarının üçe bölenlerinin kesişimi olan üç nokta bir eşkenar üçgen tanımlayacaktır. Oluşan eşkenar üçgen Morley üçgeni olarak adlandırılmaktadır. Yöntem tarafından Morley üçgeninin kenar ve *x* eksenine göre olan yönlenim bilgisi, gizli görüntü piksel değerlerini kodlamada kullanılacaktır. Morley üçgeni temel alınarak oluşturulan dış üçgenin köşe nokta koordinatları ise katılımcılara gönderilecek olan pay değerleridir. Dış üçgenin her üç noktası bilinmeden Morley üçgenini yapılandırmak mümkün olmayacaktır.

Yayının geri kalan kısmı şu şekilde düzenlenmiştir. Morley'in teoreminin detayları, Shamir ve Blakley'in sır paylaşım şemalarının prensipleri bir sonraki bölümde verilecektir. Önerilen yöntemin detayları ve elde edilen deneysel sonuçlar sırasıyla üç ve dördüncü bölümlerde yer alacaktır. Son olarak da gelecek çalışmalara yön verecek şekilde değerlendirmeler yapılacaktır.

2. Literatür Değerlendirme

Bu bölümde öncelikle Morley'in teoreminden bahsedilecektir. Teoremin ispatının da verileceği bölümün ardından sırasıyla Shamir ve Blakley'in sır paylaşım şemalarının detayları gözden geçirilecektir.

2.1. Morley'in Teoremi

ABC kenarları *a*, *b*, *c* ile gösterilen ve iç açıları sırasıyla 3α, 3β, 3γ olan herhangi bir üçgeni temsil etsin. Şekil 1'de verildiği gibi ΔABC ile gösterilen üçgenin içerisinde yer alan Morley üçgeni *XYZ*, dış üçgenin üçe bölenlerinin kesişiminden oluşur. Teorem ilk olarak 1899 yılında Frank Morley tarafından ispatlanmıştır. Bu çalışmada ise 1997'de Roy tarafından verilen ispattan bahsedilecektir [15]. İspat, bazı kritik ve kesin açıların belirlenmesi temeline dayanmaktadır.

$\angle AXZ$ ve $\angle BXY$ sırasıyla θ, μ açıları ile temsil edilsin. İspatın gerçekleşmesi için gereken $\theta = \pi/3 + \beta$ ve $\mu = \pi/3 + \alpha$ eşitliklerinin doğruluğunu göstermektir. Böylece $\angle ZXY$ açısı $\pi/3$ olarak hesaplanacaktır. Benzer şekilde Morley üçgeninin ΔXYZ diğer açıları da hesaplanabilir.

İspatın ilk aşaması $f(\theta) = f(\pi/3 + \beta)$ olduğunu göstermektir. f ile gösterilen fonksiyonun ifadesi (1)'de verilmiştir.

$$f(t) = \sin t / \sin(t + \alpha) \quad 0 < t < \pi - \alpha \qquad (1)$$

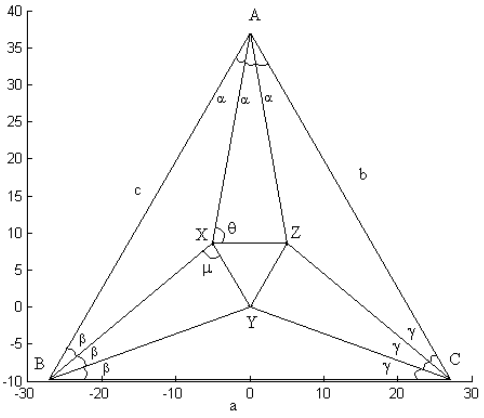
ΔAXZ üçgeninin üzerinde sinüs kuralının uygulanması ile (2)'deki ifade elde edilir.

$$\frac{AZ}{\sin\theta} = \frac{AX}{\sin(\theta + \alpha)} \Rightarrow f(\theta) = \frac{AZ}{AX} \qquad (2)$$

Benzer şekilde ΔAZC üzerinde de (3)'de verildiği gibi benzer şekilde sinüs kuralı uygulanır.

$$\frac{AZ}{\sin\gamma} = \frac{b}{\sin(2\pi/3 + \beta)} = \frac{b}{\sin(\pi/3 - \beta)} \qquad (3)$$

$3\alpha + 3\beta + 3\gamma = \pi$ olduğundan dolayı $\angle AZC$, $\pi - (\alpha + \gamma) = 2\pi/3 + \beta$ olarak hesaplansın. Sinüs



kuralının kullanımı ile (4)'deki ifade elde edilir.

Şekil 1. Morley'in teoremi

$$\frac{AX}{\sin\beta} = \frac{c}{\sin(\pi/3 - \gamma)} \qquad (4)$$

(3) ve (4)'ün kullanımı ile $f(\theta)$ fonksiyonu (5)'deki gibi tanımlanır.

$$f(\theta)=\frac{b\sin\gamma\sin(\pi/3-\gamma)}{c\sin\beta\sin(\pi/3-\beta)} \quad (5)$$

$t=\pi/3+\beta \Rightarrow \sin(t+\alpha)=\sin(\pi/3+\gamma)$ ifadesinden yola çıkarak $f(\pi/3+\beta)$, $\frac{\sin(\pi/3+\beta)}{\sin(\pi/3+\gamma)}$ olarak tanımlanır. Sinüs kuralının ΔABC ile gösterilen dış üçgen üzerinde uygulanması sonucunda $b\sin 3\gamma = c\sin 3\beta$ eşitliği elde edilir. Eşitlikten (6) ile verilen ifadenin elde edilmesinde faydalanılır.

$$4b\sin\left(\frac{\pi}{3}+\gamma\right)\sin\left(\frac{\pi}{3}-\gamma\right)\sin\gamma = 4c\sin\left(\frac{\pi}{3}+\beta\right)\sin\left(\frac{\pi}{3}-\beta\right)\sin\beta \quad (6)$$

$$\frac{\sin(\pi/3+\beta)}{\sin(\pi/3+\gamma)}=\frac{b\sin\gamma\sin(\pi/3-\gamma)}{c\sin\beta\sin(\pi/3-\beta)}$$

Bu ifadeden yola çıkarak $f\left(\frac{\pi}{3}+\beta\right)=\frac{b\sin\gamma\sin(\pi/3-\gamma)}{c\sin\beta\sin(\pi/3-\beta)}=f(\theta)$ eşitliği yazılır. Buradan da $\theta=\frac{\pi}{3}+\beta$ olduğu görülmektedir.

2.2. Shamir'in Sır Paylaşım Şeması

Shamir'in sır paylaşım şeması polinomial interpolasyona dayanan bir eşik şemasıdır [1]. *S* ile gösterilen gizli verinin $(s_1, s_2, \cdots, s_n)$ ile gösterilen *n* katılımcı arasında paylaştırılacağı varsayılsın. Her katılımcı pay olarak adlandırılan gizli verinin bir parçasını alacaktır. Shamir'in metodu gizli verinin yeniden elde edilebilmesi için en az *k* tane katılımcının bir araya gelmesi gerektiğini ispatlamıştır. Gizli verinin tek bir tamsayı olduğu varsayılarak, rasgele bir asal sayı *p*, $S \in Z_p$ koşulunu sağlayacak şekilde seçilir. (7)'deki ifade kullanılarak *k*-1 dereceden polinom, *n* farklı pay değerinin üretilmesi için yapılandırılacaktır.

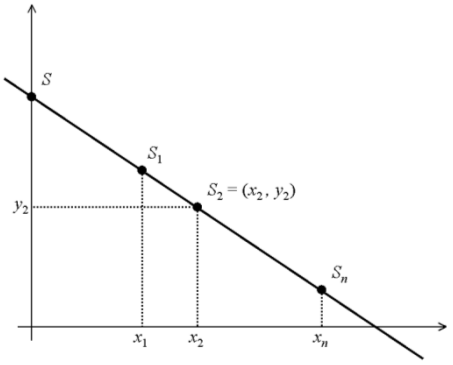
$$q(x)=\left(a_0+a_1x+\cdots+a_{k-1}x^{k-1}\right) \bmod p \quad (7)$$

Polinomun sabit terimi a_0, gizli veri *S*'yi göstermektedir. Diğer katsayılar ise $(0, p-1]$ aralığından rasgele olarak seçilecektir. Polinomun farklı *x* değerleri için üretmiş olduğu değerler pay değerlerinin oluşturulmasında (8)'deki gibi kullanılır.

$$s_1=q(1),\ s_2=q(2),\cdots,s_n=q(n) \quad (8)$$

Polinomun katsayıları yeniden yapılandırma aşamasında oluşturulan *n* değerden herhangi *k* tanesinin bir araya gelmesi sonucu, Lagrange'ın interpolasyon tekniği kullanılarak elde edilecektir. Böylece hesaplanan sabit terim değeri gizli veriyi temsil etmektedir. Gizli veriyi katılımcılar arasında paylaştırmak için kullanılan prosedür paylaştırma olarak adlandırılırken, herhangi *k* tanesinin bir araya gelmesi sonucu gizli verinin elde edilmesi işlemi yeniden yapılandırma olarak adlandırılır.

Gizli görüntü paylaşımında ise polinomun katsayıları, gizli görüntünün sıralı *k* pikselinin parlaklık değerinden oluşturulacaktır. Shamir'in yaklaşımının *k*=2 için geometrik anlamı Şekil 2'de verilmiştir. Gizli veri iki boyutlu uzayda belirlenen doğrunun *x* eksenini kestiği noktadır. Paylar ise doğru üzerinden elde edilen rasgele noktalardır. Doğru üzerindeki herhangi iki nokta, doğru denkleminin elde edilmesini ve dolayısıyla gizli verinin ortaya çıkmasını sağlayacaktır.



Şekil 2. (2, n) Shamir'in şemasının geometrik anlamı

2.3. Blakley'in Sır Paylaşım Şeması

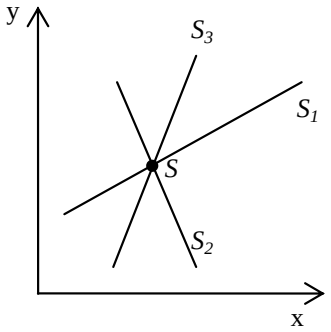
Blakley'in sır paylaşma yöntemi gizli verinin *n* kişi arasında paylaştırılması için geometrik yöntemlerden faydalanmaktadır [2]. Yönteme göre gizli veri *k* boyutlu uzayda bir noktadır. Uzayda bu noktayı kesen hiper düzlem denklemleri ise katılımcılara gönderilecek pay değerlerini oluşturacaktır.

$a_1x_1+a_2x_2+\cdots+a_kx_k=B$ denklik ifadesine çözüm oluşturan $x=(x_1, x_2, \cdots, x_k)$ kümeleri, pay değerlerine karşılık düşer. Herhangi *k* adet düzlemin

kesişmesi sonucu gizli veri yeniden yapılandırılacaktır. İki boyutlu uzay için Blakley'in şemasının (2, 3) için geometrik anlamı Şekil 3'te verilmiştir. Gizli veri *S* iki boyutlu uzayda bir nokta iken, bu noktayı kesen üç doğru denklemi ise katılımcılara gönderilecek olan pay değerleridir. Gizli verinin yeniden elde edilebilmesi için iki doğrunun bir araya gelmesi yeterli olacaktır.

3. Önerilen Yöntem

Makale kapsamında önerilen yöntem iki alt prosedürden oluşmaktadır. Paylaştırma ve yeniden yapılandırma algoritmaları. Paylaştırma algoritması, gizli veriyi katılımcılar arasında paylaştırmayı amaçlamaktadır. Yeniden yapılandırma algoritması ise herhangi üç katılımcının pay görüntülerini kullanarak gizli veriyi yeniden yapılandırmaktadır. Algoritmalara ilişkin detaylar sırasıyla verilecektir.



Şekil 3. (2, 3) Blakley şemasının geometrik gösterimi

3.1. Paylaştırma Algoritması

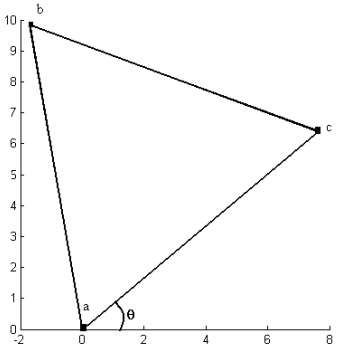
Paylaştırma algoritması D ile gösterilen gizli görüntüyü Morley'in teoremini kullanarak (S_1, S_2, S_3)ile gösterilen üç pay görüntüsüne parçalamaktadır. Gizli görüntü ve pay görüntüleri piksel parlaklık değerleri $[0, 255]$ aralığında değişen gri seviye görüntülerdir. *M*×*N* büyüklüğündeki gizli görüntü $D = \{ d_i \mid i = 1, 2, \ldots, (M \times N) \}$ ile gösterilsin. Algoritma, gizli görüntünün iki pikselden oluşan alt birimleri üzerinde işlem yapacaktır. Sıralı iki pikselden oluşan ve U^j ile gösterilen gruplar (9)'daki gibi belirlenir.

$$U = \left\{ U^j \mid j = 1, 2, \cdots, (M \cdot N)/2 \right\}$$
$$U^j = (d_i, d_{i+1}),\ j = \left\lfloor \frac{i+1}{2} \right\rfloor \quad (9)$$

U^j grubunun elemanları sırasıyla U_1^j, U_2^j şeklinde referanslanmaktadır. Grup elemanları, Morley'in teoremindeki iç üçgeni oluşturmak için kullanılacaktır. Grubun ilk elemanı U_1^j, iç üçgenin kenar uzunluğunu temsil ederken, diğer elemanı üçgenin *x* ekseni ile yaptığı açıyı belirleyecektir. İşlem görmekte olan grup U^k ile gösterilsin. Bu durumda *s* ile gösterilen kenar uzunluğu ve yönlenim açısı *θ,* (10)'daki ifadenin kullanımı ile belirlenir.

$$s = U_1^k + sbt, \theta = U_2^k \quad (10)$$

Kenar ve açı değerleri için değişim aralıkları, gri seviye görüntülerdeki piksel parlaklık değişim aralığı $[0-255]$ olduğu için sırasıyla $s \in [const-(255+const)]$ ve $\theta \in [0-255]$ şeklindedir. *sbt* ile gösterilen sabit terim, gizli görüntüdeki siyah pikseller olması durumunda, anlamsız kenar bilgilerinin oluşmasına engellemek amacıyla kullanılmıştır. Diğer yandan üçgenin yönlenimini gösteren açı değerinin siyah piksellerden dolayı 0 olması, herhangi bir probleme sebep olmayacaktır. Morley'in teoremindeki iç üçgen; kenar uzunluğu ve yönlenim açısı bilgileri yardımıyla Şekil 4'teki gibi yapılandırılır.



Şekil 4. Kenar uzunluğu 10 ve yönlenim açısı 40°olan Morley'in iç üçgeninin yapılandırılması.

Üçgenin bir köşesi şekilden de gözlemlenebileceği gibi başlangıç noktasına konumlandırılmıştır. Gizli görüntüdeki sıralı iki piksel parlaklık değerinin (10, 40) olması durumunda (a, b, c)köşeleri ile tanımlanan üçgen Şekil 4'te verilmiştir. Kenar uzunluğu olan eş kenar üçgenin $|ac|$ kenarı şekilden

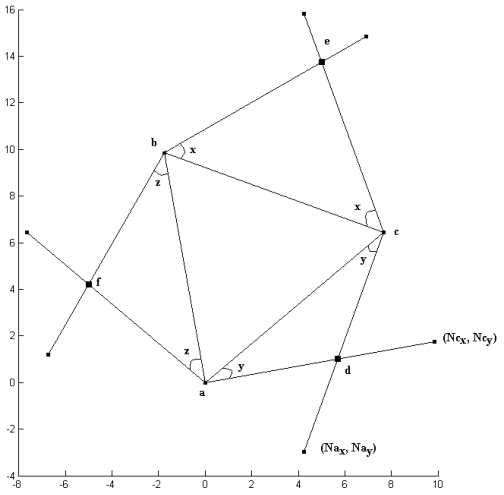
de gözlemlenebileceği gibi *x* ekseni ile θ=40° açı yapmaktadır. Bir sonraki aşama Δabc ile gösterilen üçgenin kenarlarını taban alan ve taban açıları sırasıyla (x, y, z) olan ikizkenar üçgenlerin yapılandırılmasıdır. İkizkenar üçgenler için seçilecek olan taban açı değerlerinin toplamı 120°'ye eşit olmak zorundadır. Seçilecek olan taban açı değerleri $[0^{\circ} - 60^{\circ}]$ aralığındadır. Seçilecek olan rasgele taban açı değerleri aynı (s, θ) değerleri için bile farklı dış üçgenlerin oluşumunu sağlayacaktır. Dış üçgenin köşe noktalarının koordinatları ise pay görüntülerinde karşılık düşen piksel parlaklık değerlerini oluşturur. Gizli görüntü paylaşım şemaları pay görüntülerindeki rasgeleliği sağlamak amacıyla paylaştırma algoritmasından önce karıştırma algoritmaları kullanmaktadır. Oysa önerilen yöntem, ikizkenar üçgenleri yapılandırırken taban açılarını rasgele seçmesi sayesinde karıştırma algoritmalarına ihtiyaç duymamaktadır.

Taban açıları (x, y, z) olan üç ikizkenar üçgenin yapılandırılması paylaştırma algoritmasının bir sonraki adımı olmaktadır. Bir nokta etrafında başka bir noktanın döndürülmesi prensibi kullanılarak ikizkenar üçgenler yapılandırılır. İç üçgenin *a* ve *c* noktaları, taban kenarı $|ac|$ ve taban açıları *y* olan ikiz kenar üçgenin yapılandırılmasında kullanılır. Her iki noktadan biri diğerinin etrafında döndürülmektedir. İlk varsayım *a* noktası etrafında *c* noktasının $-y^{\circ}$ döndürülmesidir. Ardından *c* noktası etrafında *a* noktası y° döndürülür. *c* ve *a* noktalarının koordinatları sırasıyla (c_x, c_y), (a_x, a_y) ile gösterilsin. İlk varsayımdaki dönüşüm işlemine ait matematiksel ifade (11)'de verilmiştir. (Nc_x, Nc_y) koordinatları *c* noktasının *a* noktası etrafında $-y^{\circ}$ döndürülmesi sonucu elde edilen yeni noktanın koordinat değerleridir. Aynı şekilde *a* noktasının de döndürme işleminden sonraki yeni koordinatları (Na_x, Na_y) olarak hesaplanır.

$$\begin{aligned} Nc_x &= (c_x - a_x)Cos(-x) - (c_y - a_y) * Sin(-x) \\ Nc_y &= (c_x - a_x)Cos(-x) + (c_y - a_y) * Sin(-x) \end{aligned} \quad (11)$$

(Na_x, Na_y) ve (Nc_x, Nc_y) noktaları kullanılarak iki doğru belirlenir. (Na_x, Na_y) ve (c_x, c_y), (Nc_x, Nc_y) ve (a_x, a_y) noktalarından geçen doğrular oluşturulur. Bu iki doğrunun kesişim noktası ise Şekil 5'de görüldüğü gibi ikizkenar üçgenin *d* ile gösterilen tepe noktasını verecektir.

Diğer ikizkenar üçgenler de yukarıda anlatıldığı gibi yapılandırılmaktadır. Bu üçgenlerin tepe noktaları da sırasıyla *e* ve *f* olarak gösterilsin. İkizkenar üçgenlerin kenarlarının kesişinceye kadar uzatılması dış üçgenin oluşturulmasındaki son adım olacaktır. Dış üçgenin köşe noktaları sırasıyla $(|be|, |ad|)$, $(|ec|, |af|)$ ve $(|bf|, |cd|)$ ile verilen doğruların kesiştirilmesi sonucu (12)'deki gibi elde edilir.



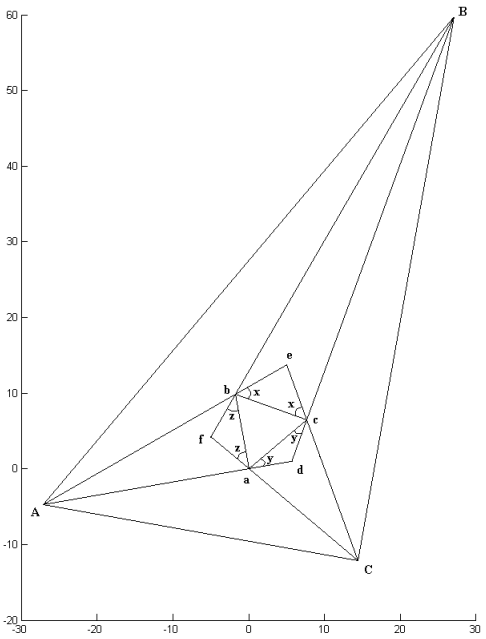
Şekil 5. İkizkenar üçgenlerin tepe noktalarının belirlenmesi

$$\begin{aligned} (A_x, A_y) &= (|be| \cap |ad|) \\ (B_x, B_y) &= (|ec| \cap |af|) \\ (C_x, C_y) &= (|bf| \cap |cd|) \end{aligned} \quad (12)$$

Dış üçgenin köşe koordinatları Şekil 6'da gösterildiği gibi (A_x, A_y), (B_x, B_y) ve (C_x, C_y) olarak elde edilmiştir. Şekilden de gözlemlenebileceği gibi dış üçgenin köşe noktaları koordinat düzleminde birinci bölgede olmayabilir. İlk bölge haricindeki diğer bölgelerde negatif değerler mevcuttur. Bu nedenle dış üçgenin yapılandırılmasının ardından birinci bölgeye transferi gerekmektedir. Dış üçgenin koordinatlarının birinci bölgeye transferi için kullanılan ifade (13)'de verilmiştir. min()

fonksiyonu argümanlarının en küçüğünü döndürmektedir.

$$x^*_{\min} = \min(A_x, B_x, C_x)$$
$$y^*_{\min} = \min(A_y, B_y, C_y) \tag{13}$$
$$x^*_{\min} < 0 \Rightarrow \begin{cases} A_x = A_x + \left|x^*_{\min}\right| \\ B_x = B_x + \left|x^*_{\min}\right| \\ C_x = C_x + \left|x^*_{\min}\right| \end{cases} y^*_{\min} < 0 \Rightarrow \begin{cases} A_y = A_y + \left|y^*_{\min}\right| \\ B_y = B_y + \left|y^*_{\min}\right| \\ C_y = C_y + \left|y^*_{\min}\right| \end{cases}$$



Şekil 6. Belirlenen dış üçgen ve koordinatları.

Kullanılan öteleme fonksiyonu ile beraber her ne kadar üçgen birinci bölgeye taşınmış olsa da, bazı köşeler x veya y ekseni üzerinde olabilir. Bu nedenle yöntem ötelemeden sonra rasgeleliğin sağlanması ve siyah değerine sahip pay piksellerinin çok fazla sayıda oluşumuna engel olmak amacıyla, rasgele bir öteleme kullanılmasını önermiştir. Her iki yönde (r_x, r_y) parametreli kullanılarak (14)'de verildiği gibi rasgele bir öteleme gerçekleştirilmektedir.

$$r_x = \left\lfloor \frac{x^*_{\min} + x^*_{\max}}{2} \right\rfloor \quad r_y = \left\lfloor \frac{y^*_{\min} + y^*_{\max}}{2} \right\rfloor \tag{14}$$

Böylece işlem görmekte olan ikili gizli piksel grubu için U^k, üretilen dış üçgenin köşe noktalarının koordinatları katılımcılara gönderilecek olan pay görüntülerin piksel parlaklık değerlerini oluşturacaktır. 8 bit derinlikteki gizli görüntü için 256 mümkün kenar uzunluğu ve yine 256 mümkün açı kombinasyonu pay görüntü derinliğini belirlemede kullanılacaktır. Ötelemede kullanılan sabit terimin 5 olarak seçilmesi durumunda, üretilen dış üçgenlerin köşe noktalarının koordinatlarının $[0-2048]$ aralığında değişim gösterdiği gözlemlenmiştir. Üçgen köşe koordinatlarını temsil etmede kullanılan 22 bit değer algoritma tarafından üç parçaya bölünmektedir.

Dış üçgenin köşe noktası *A*, 11 bit iki sayı (A_x, A_y)ile temsil edilmektedir. Her bir sayı 8 ve 3 bitten oluşan iki kısma ayrılmaktadır. Oluşan dört alt bölme kullanılarak üretilen *R, G, B* değerleri, (15)'deki ifade yardımıyla hesaplanmaktadır. Dış üçgenin diğer kenarları da aynı şekilde üç adet 8 bitlik sayı ile temsil edilerek karşılık düşen pay görüntüsünün piksel parlaklık değeri oluşturulacaktır.

İfadeden de gözlemlenebileceği gibi gizli görüntüdeki iki adet piksel değeri, pay görüntüsündeki pikselin üç kanalındaki parlaklık değeri ile temsil edilmektedir. *N*×*M* büyüklüğündeki bir gizli görüntü için üretilen renkli pay görüntülerinin büyüklüğü $(N \times M/2)$ olmaktadır. (15)'deki ifadede yer alan ' $\wedge$ ' ve '<<' sembolleri sırasıyla bit düzeyinde "VE" ve "Kaydırma" işlemlerine karşı düşmektedir.

$$\begin{aligned} R &= \lfloor A_x/8 \rfloor \\ G &= \lfloor A_y/8 \rfloor \\ B &= ((A_x \wedge 7) << 3) \vee (A_y \wedge 7) \end{aligned} \tag{15}$$

Paylaştırma algoritmasını kısaca özetlemek gerekirse: gizli görüntü öncelikle iki pikselden oluşan gruplara bölünür. Bir sonraki aşamada sıradaki iki piksel parlaklık değeri kullanılarak oluşturulan Morley'in üçgeninin kenarlarında rasgele seçilen (x, y, z) taban açıları ile ikiz kenar üçgenler oluşturulmaktadır. Taban açıları $[0^\circ - 60^\circ]$ aralığında rasgele olarak seçilir. Ardından dış üçgen ikizkenar üçgenlerin kenar bilgileri kullanılarak oluşturulur. Dış üçgen, negatif koordinatları engellemek amacıyla koordinat düzleminde birinci bölgeye ötelenmektedir. Üçgenin köşe koordinatları ise üretilecek pay görüntülerinin

karşılık düşen piksel parlaklık değerlerini oluşturmaktadır.

3.2. Yeniden Yapılandırma Algoritması

Katılımcılardan elde edilen pay görüntüleri gizli görüntüyü elde etmede kullanılır. Pay görüntüleri yeniden yapılandırma esnasında 1×3 büyüklüğündeki bloklara ayrılmaktadır. Pay görüntülerinden elde edilen karşılıklı bloklar dış üçgenin yapılandırılmasında kullanılacaktır. Dış üçgenin köşe noktaları kenarları oluşturmaktadır. Kenarların eğim bilgisi kullanılarak iç açılar elde edilecek ve içteki Morley üçgeni yapılandırılacaktır. Morley üçgeninin kenar bilgisi ve *x* eksenine göre yönlenimi, yeniden yapılandırılan gizli görüntünün karşılık düşen piksel değerlerini oluşturacaktır.

Katılımcılardan elde edilen ve SH^1, SH^2, SH^3 ile gösterilen pay görüntüleri (16)'da verilmiştir.

$$SH^k = \left\{ SH_{ij}^k \;\middle|\; i \in \{1 \cdots N\},\ j \in \left\{1 \cdots \frac{M}{2}\right\},\ k = [1-3] \right\} \quad (16)$$

Her pay piksel değeri üç kanal bilgisinden oluşmaktadır. Pay görüntülerindeki karşılık düşen piksel parlaklık değerleri dış üçgenin köşe noktalarını belirler. İlk pay görüntüsünde *m* ile gösterilen pay değeri (17)'de verilmiştir. Pay değeri üç kanaldaki değerler kullanılarak yapılandırılacaktır.

$$sh_m^1 = \left\{ sh_{m1}^1, sh_{m2}^1, sh_{m3}^1,\ m = \{1 \cdots N \times M/2\} \right\} \quad (17)$$

Diğer pay görüntülerinden elde edilen renkli piksel parlaklık değerleri sh_m^2, sh_m^3 ile gösterilsin. Bu piksellerden elde edilen değerler ise dış üçgenin diğer köşelerinin elde edilmesinde kullanılacaktır. *A* ile gösterilen köşenin koordinatları (A_x, A_y), ilk pay görüntüsünden elde edilen kanal renk bilgilerinin $sh_{m1}^1, sh_{m2}^1, sh_{m3}^1$ kullanımı ile (18)'deki gibi hesaplanır.

$$\begin{aligned} A_x &= \left(sh_{m1}^1 << 3\right) \vee \left(sh_{m3}^1 >> 3\right) \\ A_y &= \left(sh_{m2}^1 << 3\right) \vee \left(sh_{m3}^1 \wedge 7\right) \end{aligned} \quad (18)$$

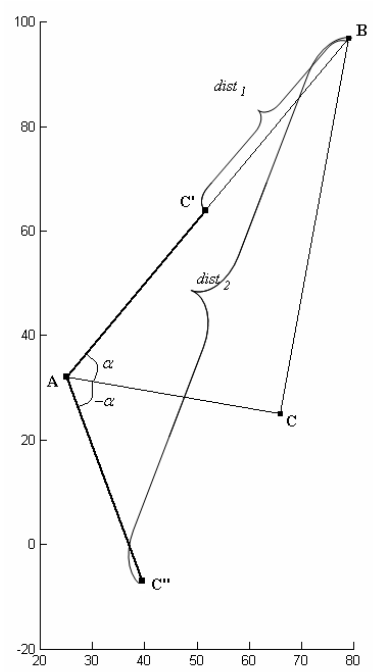
$>>$ ve $\vee$ işaretleri sırasıyla sağa kaydırma ve bit düzeyine VEYA'lama işlemlerine karşı düşmektedir. Dış üçgenin diğer köşeleri de iki ve üçüncü pay görüntülerinden gelen değerlerin kullanımı ile hesaplanacaktır. Dış üçgenin elde edilen üç köşe bilgisi kenarları tanımlayacaktır. Üç kenarın eğim bilgisi iç açıların hesaplanmasını sağlayacaktır. slp_1, slp_2, slp_3 ile gösterilen eğim bilgileri (19)'daki ifadenin kullanımı ile hesaplanır.

$$\begin{aligned} slp_1 &= \left(C_y - A_y\right) / \left(C_x - A_x\right) \\ slp_2 &= \left(B_y - A_y\right) / \left(B_x - A_x\right) \\ slp_3 &= \left(C_y - B_y\right) / \left(C_x - B_x\right) \end{aligned} \quad (19)$$

Yeniden yapılandırma sürecindeki bir sonraki aşamanın iç açıların üç eşit parçaya bölünmesi olduğu için, açıların doğru bir şekilde tespiti önem kazanmaktadır. Kenarların eğimi iç açıların belirlenmesinde kullanılacaktır. α ile gösterilen iç açılardan bir tanesi (20)'deki ifade yardımıyla hesaplanacaktır.

$$\begin{aligned} & slp_1 \cdot slp_2 = -1 \Rightarrow \alpha = 90 \\ & \left(slp_1 = \infty\right) \vee \left(slp_1 = -\infty\right) \Rightarrow \alpha = \arctan\left(180 / \left(slp_2 \cdot \pi\right)\right) \\ & \left(slp_2 = \infty\right) \vee \left(slp_2 = -\infty\right) \Rightarrow \alpha = \arctan\left(180 / \left(slp_1 \cdot \pi\right)\right) \\ & slp_2 > slp_1 \Rightarrow \alpha = \arctan\left(\left(\left(slp_2 - slp_1\right) / \left(1 + slp_1 \cdot slp_2\right)\right) \cdot \frac{180}{\pi} \right) \\ & slp_1 > slp_2 \Rightarrow \alpha = \arctan\left(\left(\left(slp_1 - slp_2\right) / \left(1 + slp_1 \cdot slp_2\right)\right) \cdot \frac{180}{\pi} \right) \end{aligned} \quad (20)$$

Dış üçgenin diğer açıları olan β, γ'da benzer şekilde hesaplanır. (slp_1, slp_3) ve (slp_2, slp_3) değerleri sırasıyla ilgili açı değerlerinin hesaplanmasında kullanılacaktır. Yeniden yapılandırma sürecinde bir sonraki aşama olarak (α, β, γ) ile gösterilen iç açılar üç eşit parçaya ayrılacaktır. Döndürme transformasyonu açının üç eşit parçaya bölünmesinde kullanılacaktır. Algoritmanın işleyişini göstermek amacıyla α açısı üç eşit parçaya ayrılacaktır. Anlatılan adımlar diğer açılar için de geçerli olacaktır. $|AC|$ ve $|AB|$ arasındaki açı α olsun. *C* köşesi *A* etrafında $\alpha/3$ ve $2\alpha/3$ derece döndürülerek açının üçe bölme işlemi gerçekleştirilecektir. Yalnız dönme işleminin saat yönünde mi yoksa saatin ters yönünde mi olacağı basit bir yöntem ile belirlenecektir. *C* noktasının *A* noktası etrafında saat yönünde ve saate ters yönde α kadar döndürülmesi sonucu elde edilen noktalar Şekil 7'de görüldüğü gibi sırasıyla C'' ve C' olsun. Üretilen noktaların *B* kenarına olan uzaklığını gösteren $dist_1$ ve $dist_2$, (21)'deki ifade yardımıyla hesaplanacaktır.



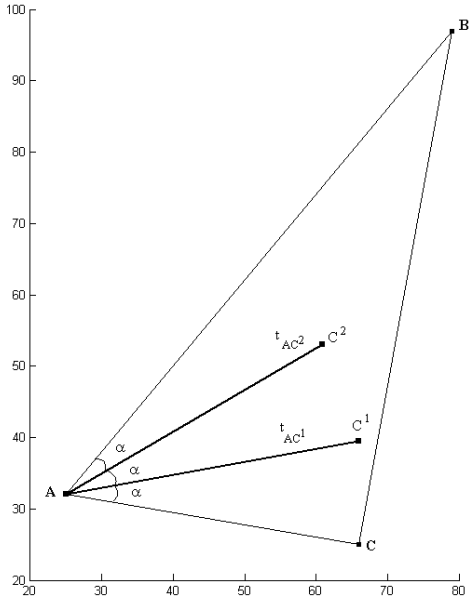
Şekil 7. *B* ve (C', C'') noktaları arasındaki uzaklıklar.

$$dist_1 = \sqrt{(B_y - C'_y)^2 + (B_x - C'_x)^2}$$
$$dist_2 = \sqrt{(B_y - C''_y)^2 + (B_x - C''_x)^2} \quad (21)$$

B noktasına olan uzaklıklar, açının bölünmesi işleminde kullanılacak olan döndürme işleminin yönünü belirleyecektir. $dist_1 < dist_2$ olması durumunda saat yönünde dönüş işlemi gerçekleştirilecekken, aksi takdirde saat yönünün tersi kullanılacaktır. Dönme yönü belirlendikten sonra, *C* noktası *A* etrafında $\alpha/3$ ve $2\alpha/3$ derece döndürülür. Döndürme işleminin ardından elde edilen yeni noktalar Şekil 8'de gösterildiği gibi C^1 ve C^2 olsun. (A, C^1) ve (A, C^2) ikilisi, α açısını üçe bölen ve t_{AC^1}, t_{AC^2} ile gösterilen doğrulardır. Diğer açıları üç eşit açıya bölen dört doğru ise $t_{BA^1}, t_{BA^2}, t_{CB^1}, t_{CB^2}$ ile gösterilsin. Morley'in üçgeni elde edilen bu doğruların doğru bir şekilde kesiştirilmesi ile elde edilecektir. *a*, *b* ve *c*, sırasıyla *AB*, *BC* ve *AC* kenarlarına yakın doğruların kesişim noktaları olsun. (22) ile verilen ifade Morley üçgeninin köşe noktalarını belirlemede kullanılacaktır.

$$a = t_{AC^1} \cap t_{CB^2} \quad b = t_{AC^2} \cap t_{BA^1} \quad c = t_{CB^1} \cap t_{BA^2} \quad (22)$$

Şekil 9'da yeniden yapılandırılan Morley üçgeni gösterilmiştir.



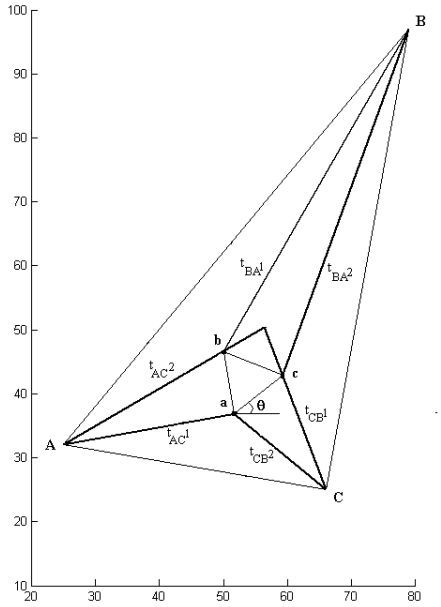
Şekil 8. C^1 ve C^2 ile gösterilen yeni noktalar.

Morley üçgeninin köşeleri kullanılarak, üçgenin kenar uzunluğu ve x eksenine göre yönlenimi belirlenecektir, (s, θ). Elde edilen değerler ise yeniden yapılandırılan gizli görüntünün karşılık düşen piksel parlaklık değerlerini oluşturur. Pay görüntülerinde karşılık düşen bloklar üzerinde yukarıda anlatılan adımlar uygulanarak gizli görüntünün piksel parlaklık değerleri oluşturulacaktır.

4. Deneysel Sonuçlar

Önerilen yöntemin gerçeklenebilirliğini gösterebilmek amacıyla yapılan çeşitli deneyler ve sonuçları bu bölümde verilmiştir. Algoritmaların kodlanması Windows XP Professional işletim sistemine sahip bir makine üzerindeki Matlab simülasyon ortamında gerçekleştirilmiştir. Serbest görüntü işleme yazılımı olan IrfanView, renkli test

görüntülerinin gri seviyeye çevrilmesinde, yeniden boyutlandırılmasında ve farklı formatlara



çevrilmesinde kullanılmıştır.

Şekil 9. Yeniden yapılandırılan Morley üçgeni.

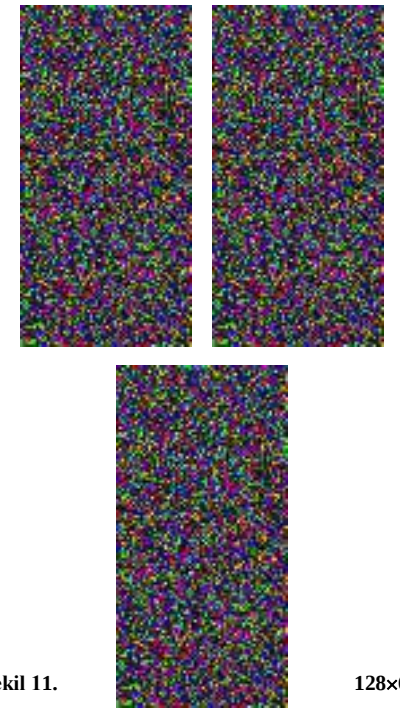
128×128 büyüklüğündeki Şekil 10'da verilmiş olan gri seviye Lena görüntüsü gizli görüntü olarak kullanılmıştır. Önerilen yöntem gizli görüntüyü Morley teoremini kullanarak üç pay görüntüsüne parçalamaktadır. Gizli görüntü iki pikselden oluşan gruplara ayrılmakta ve üretilen pay değerleri, karşılık düşen pay görüntüsündeki renkli piksele kodlanmaktadır. Bu nedenle üretilen renkli pay görüntü büyüklüğü 128×64 olarak tespit edilmiştir. Önceki bölümde anlatıldığı gibi gizli görüntüdeki piksel grubu, Morley üçgenine ait kenar ve x eksenine göre yönlenim bilgisini içermektedir. Karşılık düşen pay görüntüdeki piksel değerleri ise, dış üçgenin köşe koordinatlarını barındırmaktadır. Böylece, pay görüntülerinden herhangi birinin tek başına bir anlam ifade etmeyeceği rahatlıkla söylenebilir. Bir adet pay görüntüsü dış üçgene ait tek bir köşe bilgisi içerirken, iki adet pay görüntüsü üçgene ait yalnızca bir kenarın bilinmesine sebep olacaktır. Kenar bilgisini kullanarak gizli veriyi barındıran Morley üçgenini yapılandırmak mümkün olmayacaktır. Önerilen yöntem gizli görüntünün yeniden yapılandırılabilmesi için her üç pay görüntüsünü de gerektirmektedir.

Şekil 10. 128×128 büyüklüğündeki gizli görüntü.

İlk deneyde gizli görüntü üç katılımcı arasında paylaştırılmıştır. Üretilen 128×64 büyüklüğündeki pay görüntüleri Şekil 11'de verilmiştir. Pay görüntüleri gürültü özelliği taşımakta ve gizli görüntü hakkında herhangi bir bilgi içermemektedir. Ancak şekilde verilen üç pay görüntüsünün bir araya gelmesi sonucu gizli görüntü yeniden yapılandırılabilecektir. Yeniden yapılandırma sürecinde, pay görüntülerindeki piksel parlaklık değerleri Morley üçgenini yapılandırmada kullanılacaktır.

Fakat dış üçgenin köşe koordinatlarının reel olmasına rağmen paylaştırma sürecinde tamsayıya çevirmek için gerçekleştirilen yuvarlama işlemleri yeniden yapılandırılan gizli görüntüde bazı hataların oluşumuna sebep olacaktır. Morley üçgenine ait kenar ve yönlenim bilgisi ± 1 piksellik hatalarla elde edilebilecektir. Bu nedenle deneysel sonuçlarda elde edilen gizli görüntünün PSNR (Peak to Signal Noise Ratio) ölçümü gerçekleştirilmiştir. PSNR (23)'deki gibi tanımlanır. 255 değeri gri seviye görüntüdeki en büyük değere sahip piksel parlaklık değerini temsil etmektedir.

$$PSNR = 10 \times \log_{10} (255)^2 / MSE \, dB$$
$$MSE = 1/M \times N \sum_{i=1}^{N} \sum_{j=1}^{M} \left(S'_{ij} - S_{ij} \right)^2 \qquad (23)$$



Şekil 11. 128×64 büyüklüğündeki pay görüntüleri.

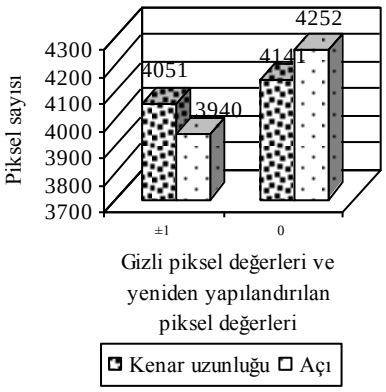
Gizli görüntü ve yeniden yapılandırılan gizli görüntü sırasıyla S, S' ile temsil edilmektedir. Yapılan testlerde yeniden yapılandırılan gizli görüntünün yaklaşık olarak 50.39 dB PSNR'ye sahip olduğu tespit edilmiştir. Literatürdeki çalışmalarda $[40,\infty)$dB aralığında PSNR'ye sahip görüntülerin iyi bir görsel kaliteye sahip olduğuna vurgu yapılmaktadır. Böylece Şekil 12'de verilen yeniden yapılandırılan gizli görüntünün iyi bir görsel kaliteye sahip olduğu söylenebilir.

Diğer bir deney ise yeniden yapılandırma esnasında meydana gelen hata sayısını tespit etmek amacıyla gerçekleştirilmiştir. Şekil 13'ten de gözlemlenebileceği gibi gizli görüntüdeki 128×128=16384 pikselin yarısı Morley üçgenlerinin kenar bilgisini taşırken diğer yarısı ise yönlenim bilgilerini içermektedir. Kenar bilgilerinin 4051 tanesi mutlak 1 farkla yapılandırılırken, açı bilgisinin 3940 tanesi mutlak 1 farkla elde edilmektedir.

Şekil 12. Yeniden yapılandırılan gizli görüntü PSNR=50.39 dB.

5. Değerlendirme

Bu makalede düzlem geometrisindeki Morley'in teoremine dayanan yeni bir (3, 3) gizli görüntü paylaşım şeması önerilmiştir. Morley'in teoremindeki dış üçgenin köşe noktaları pay görüntülerindeki piksel parlaklık değerlerini oluştururken, Morley'in üçgeninin kenar ve yönlenim bilgisi gizli piksel değerlerini kodlamada kullanılmaktadır. Elde edilen deneysel sonuçlarda pay görüntülerinin gizli görüntü hakkında herhangi bir bilgi ortaya çıkarmadığı gözlemlenmiştir. Yuvarlama işlemlerinden dolayı meydana gelen yeniden yapılandırma hataları ise insan gözü tarafından ayırt edilemeyecek derecededir.



Şekil 13. Yeniden yapılandırma esnasında meydana gelen yuvarlama hataları.

Kaynakça

[1] Shamir, A., "How to Share a Secret", Communications of ACM, vol. 22, no. 11, pp. 612-613, 1979.

[2] Blakley, G.R., "Safeguarding Cryptographic Keys", Proceedings of the National Computer Conference, pp. 313-317, 1979.

[3] Thien, C.-C., Lin, J.-C., "Secret Image Sharing", Computers and Graphics, vol. 26, pp. 765-770, 2002.

[4] Lin, C.-C., Tsai, W.-H., "Secret image sharing with steganography and authentication", Journal of Systems and Software, vol. 73, no. 3, pp. 405-414, 2004.

[5] Yang, C.-N., Chen, T.-S., Yu, K.H., Wang, C.-C., "Improvements of image sharing with steganography and authentication", Journal of Systems and Software, vol. 80, no. 7, pp. 1070-1076, 2007.

[6] Chang, C.-C., Hsieh, Y.-P., Lin, C.-H., "Sharing secrets in stego images with authentication", Pattern Recognition, vol. 41, pp. 3130-3137, 2008.

[7] Lin, P.-Y., Lee, J.-S., Chang, C.-C., "Distortion-Free Secret Image Sharing Mechanism using Modulus Operator", Pattern Recognition, vol. 42, pp. 886-895, 2009.

[8] Wang, R.-Z., Su, C.-H., "Secret Image Sharing with Smaller Shadow Images", Pattern Recognition Letters, vol. 27, no. 6, pp. 551-555, 2006.

[9] Chang, C.-C., Lin, C.-C., Lin, C.-H., Chen, Y.-H., "A Novel Secret Image Sharing Scheme in Color Images Using Small Shadow Images", Information Sciences, vol. 178, no. 11, pp. 2433-2447, 2008.

[10] Zhao, R., Zhao, J.-J., Dai, F., Zhao, F.-Q., "A New Image Secret Sharing Scheme to Identify Cheaters", Computer Standarts & Interfaces, vol. 31, no. 1, pp. 252-257, 2009.

[11] Chen, S.-K., Lin, J.-C., "Fault-tolerant and progressive transmission of images", Pattern Recognition, vol. 38, pp. 2466-2471, 2005.

[12] Huang, C.-P., Li, C.-C., "A Secret Image Sharing Method Using Integer wavelet Transform", Journal on Advances in Signal Processing, vol. 2007, Article ID 63281, 13 pages, 2007.

[13] Chen, C.-C., Fu, W.-Y, "A Geometry Based Secret Image Sharing Approach", Journal of Information Science and Engineering, vol. 24, no. 5, pp. 1567-1577, 2008.

[14] Ulutas, M., Nabiyev, V., Ulutas, G., "Improvements in Geometry-Based Secret Image Sharing Approach with Steganography", Mathematical Problems in Engineering, vol. 2009, Article ID 187874, 11 pages, 2009. doi:10.1155/2009/187874

[15] Barbara, R., "Two short proofs of Morley's Theorem", The Mathematical Gazette, Vol. 81, No. 492, pp. 447-450, 1997.