Doğruluk Oranı İyileştirilmiş (2, n) Olasılıklı Görsel Sır Paylaşma Şeması

Vasif V. NABİYEV, Mustafa ULUTAŞ, Güzin ULUTAŞ

***Özet*— Görsel Sır Paylaşma (GSP), gizli bir görüntünün gürültü benzeri paylara kodlanmasıdır. GSP yöntemlerinde, gizli görüntüdeki bir pikselin paylarda *m* pikselle kodlanıyor olması *büyüme oranı* problemini beraberinde getirmiştir. Bu problemin giderilmesi için, *m* değerini 1 olarak belirleyen ve Olasılıklı Görsel Sır Paylaşma (OGSP) olarak adlandırılan yeni bir yöntem önerilmiştir. Geleneksel GSP ve OGSP yöntemlerinde gizli görüntünün ortaya çıkarılması için insan görme sistemi yeterli olmaktadır. 2007 yılında Wang, insan görme sistemini kullanmayan ve yalnızca mantıksal işlemlere dayanan yeni bir (2, n) OGSP yöntemi önermiştir. Yöntem siyah pikselleri 1, beyaz pikselleri ise ½ olasılıkla doğru olarak koruyabilmektedir. Bu yayında, Wang'ın yönteminde kullanılan rasgele B matrislerinin içeriklerinin belirlenmesinde kullanılacak olan yeni bir yöntem önerilmiştir. Bu sayede yapılandırılan resimdeki beyaz piksellerin doğruluk oranı yükselmiştir. Test sonuçlarında, yapılandırılan görüntünün sahip olabileceği maksimum PSNR değeri, Wang'ın önerdiği yöntemle elde edilen değerden daha yüksek çıkmıştır. Böylelikle Wang'ın yönteminin, GSP şemalarının değerlendirilmesinde önemli bir parametre olan, doğruluk oranı iyileştirilmiştir.**

***Anahtar Kelimeler* —GSP, OGSP, PSNR.**

I. GİRİŞ

Sır Paylaşma (SP) şeması olarak adlandırılan yöntem ilk olarak Blakley ve Shamir tarafından 1979 yılında önerilmiştir [1, 2]. *(k, n)* eşik şeması olarak da adlandırılan bu yöntem, verinin güvenliğini n tane parçaya bölerek sağlar. Her bir parça "pay" olarak adlandırılır. Oluşturulan *n* tane pay *n* tane kişiye dağıtılır. Sırı paylaşan her bir kişinin elinde yalnız bir pay vardır. Gizli veri, ancak bu paylardan en az k tanesi bir araya getirildiğinde ortaya çıkacaktır. *k* adetten az payın bir araya getirilmesi, gizli veri hakkında hiçbir bilgi açığa çıkarmaz.

SP yöntemini temel alan ve daha yeni bir yöntem olan "Görsel Sır Paylaşımı" (GSP) Naor ve Shamir tarafından 1994 yılında önerilmiştir [3]. Bu şema için paylaşılan sır gizli bir görüntüdür (el yazısı notları, yazıcı çıktıları, resimler gibi). Bu yeni sır paylaşım tekniğinin en önemli özelliği, başka bir hesaplamaya ihtiyaç duymaksızın insan görme sistemini, gizli veriyi ortaya çıkarmada kullanmasıdır. Geleneksel şifreleme tekniklerinin, şifre çözme için gerektirdiği kompleks hesaplamalar bu yeni alanda yer almamaktadır. *(k, n)* GSP şeması için, sır sahibi olan kişi, gizli görüntüden görsel şifreleme tekniklerini kullanarak *n* tane anlamsız pay oluşturur ve sırı paylaşacağı guruptaki alıcıların her birine bir adet pay gönderir. Paylar; aslında anlam ifade etmeyen gürültü benzeri görüntülerdir. Gizli görüntünün ortaya çıkarılabilmesi için en az *k* adet kişinin kendi paylarını slayt üzerine basmaları ve bu slaytları tam olarak üst üste getirmeleri gerekmektedir. Gizli veri, görsel şifreleme teknikleri kullanılarak paylara dağıtıldığı için, kötü amaçlı kişiler herhangi tek bir paydan gizli görüntüyü elde edemeyecektir.

Naor ve Shamir tarafından önerilen bu şemayı geliştirmek amacı ile çeşitli yaklaşımlar önerilmiştir. Bazı çalışmalar, paylaşılacak olan görüntünün yalnızca siyah beyaz resim olmak yerine, gri seviye veya renkli resim olabileceğini göstermiştir [4-6]. Paylaşılacak olan sır sayısının artırılması ise ilgi çeken diğer bir konudur [7-9]. Görsel şifrelemenin doğası gereği oluşan kontrast problemlerinin giderilmesi ise çözülmeye çalışılan problemlerden biridir [10]. Tanımı gereği görsel şifrelemede, sır olarak paylaşılacak olan görüntüdeki bir piksel, paylarda birden çok alt piksel ile temsil edilmektedir. Böyle bir kodlama tekniği ise görüntü boyutlarının belirli bir oranda genişlemesine neden olmaktadır. Genişleme faktörü olarak adlandırılan bu büyüme oranı, bellekte saklama açısından ihtiyaç duyulan kapasitenin artması ile sonuçlanmaktadır. Yapılan birçok çalışma ile bu oranın küçültülmesi amaçlanmıştır.

(k, n) GSP şemalarının başarımını test etmekte kullanılan dört parametre mevcuttur. Bu parametrelerden ilki *güvenliktir*. *k* adetten az payın bir araya getirilmesi sır hakkında hiçbir bilgi ortaya çıkarmamalıdır. İkinci parametre *doğruluktur*. En az *k* adet payın bir araya gelmesi ile ortaya çıkarılan sırın, orijinaline olan benzerliğidir. Diğer bir kriter ise *hesaplama karmaşıklığıdır*: payları üretmede gereken işlem sayısı ile ölçülür. Son kriter ise gizli görüntüdeki bir pikselin paylarda kaç piksel ile kodlandığına bağlı olarak değişen *büyüme oranıdır*.

Büyüme oranı kriterini iyileştirmeye çalışan bazı çalışmalar "olasılıklı görsel sır paylaşma" (OGSP) şemalarını önermişlerdir [11-14]. Bu çalışmalarda, sır olarak paylaşılacak olan görüntüdeki her bir piksel paylarda tek piksel kullanılarak kodlanır. Böylelikle payların boyutu orijinal görüntünün boyutu ile aynı kalır. Orijinal görüntüdeki piksellerin, yeniden yapılandırılan görüntüde aynı olarak elde edilebilmesi belirli bir olasılık

V. NABİYEV, Karadeniz Teknik Üniversitesi
M. ULUTAŞ, G. ULUTAŞ , Ondokuz Mayıs Üniversitesi

dahilindedir. Gizli görüntüdeki pikseller, yeniden yapılandırılma işleminden sonra bire bir aynı kalmaz. Fakat bölgesel olarak bakıldığında resmin, orijinal görüntüsünü koruduğu gözlemlenebilir. Her ne kadar OGSP teknikleri, hesaplama karmaşıklığını ve büyüme oranını azaltsa da, doğrulukta kayıplara sebep olmaktadır.

2007 yılında Wang, mantıksal işlemlere dayalı yeni bir *(2, n)* OGSP şeması ileri sürmüştür [14]. Bu şema XOR ve AND işlemlerini kullanarak siyah beyaz resimleri rastlantısal bir teknikle kodlar. Geleneksel OGSP' den farklı olarak, yeniden yapılandırma işlemi için insanın görme sistemi yeterli değildir. Elde etmiş olduğu sonuçların karşıtlık açısından geleneksel tekniklerden daha iyi olduğunu deneysel sonuçlarla göstermiştir.

Bu makalede, Wang tarafından önerilen tekniğin kontrast değerini iyileştirerek, yeniden yapılandırılan resimlerin doğruluk değerinin yükseltilmesi sağlanmıştır. Önerilen tekniğin Wang'ın çalışmasından üstün olduğu, yeniden yapılandırılan resimlerin PSNR değerlerinin test edilmesi ile gösterilmiştir.

Yayının geri kalanı şu şekilde düzenlenmiştir. İkinci kısımda GSP ve OGSP şemalarının ayrıntılarından bahsedilmiştir. Üçüncü kısımda ise Wang'ın önermiş olduğu *(2, n)* şeması açıklanarak önermiş olduğumuz yöntem, ayrıntıları ile verilmiştir. Son olarak önerilen teknik ile elde edilen test görüntüleri verilmiş ve sonuçlar yorumlanmıştır.

II. GSP VE OGSP YÖNTEMLERİ

A. Görsel Sır Paylaşma (GSP)

(k, n) GSP şemasında orijinal görüntünün siyah ve beyaz piksellerden oluştuğu varsayılmıştır. Orijinal görüntüdeki her bir piksel, paylarda m adet alt piksel olarak kodlanır. GSP şeması $n \times m$ büyüklüğündeki mantıksal S matrisi ($S = [s_{ij}]$) tarafından tanımlanır. Sütun sayısını gösteren m değeri, gizli görüntüdeki tek bir pikselin paylarda kaç pikselle temsil edeceğini gösterir. Eğer *i.* paydaki *j.* alt piksel siyah ise $s_{ij} = 1$, aksi takdirde $s_{ij} = 0$ 'dır. $i_1, i_2, \ldots, i_k$ ile gösterilen paylar, alt pikselleri uygun bir şekilde örtüşecek şekilde üst üste getirildiklerinde sır ortaya çıkacaktır. S matrisindeki satırlara OR mantıksal işleminin uygulanması sonucu oluşan vektörün Hamming ağırlığı, ilgili pikselin insan görme sistemi tarafından nasıl algılanacağını göstermektedir. Siyah ve beyazı ayırt etmek için sabit bir eşik değeri olsun ve d ($1 \le d \le m$) ile gösterilsin. Resmin görünebilirliği açısından, α ile gösterilen kontrastın sıfırdan büyük olması gerekir. İlgili piksel için belirlenen S matrisinin satırlarının OR'lanması sonucu oluşan $1 \times m$ lik vektör V ile gösterilsin. Bu durumda eğer $H(V) \ge d$ ise, yeniden yapılandırılan piksel insan görme sistemi tarafından siyah, eğer $H(V) \le d - \alpha m$ ise beyaz olarak algılanacaktır.

Tanım 1. *(k, n)* GSP şeması, B_0 ve B_1 ile gösterilen n×m büyüklüğündeki mantıksal matrislerden oluşan iki küme ile temsil edilebilir. Beyaz bir piksel paylaşılacağı zaman kişi B_0 mantıksal matrisinin satırlarından birini rastgele olarak seçer ve ilgili paya yerleştirir. Siyah bir piksel paylaşılacağında ise B_1 matrisinden seçilen rastgele bir satır ilgili payı kodlamada kullanılacaktır. B_0 veya B_1 matris kümelerinden rasgele seçilen bir matris, n tane paydaki m adet alt pikselin gri seviyesini belirlemeye yardımcı olacaktır. Naor ve Shamir'in tanımı gereği, bir GSP şeması ancak aşağıdaki koşulları sağladığı takdirde geçerli olacaktır.

1. B_0 veya B_1 kümelerinden seçilen herhangi bir matrisin, n tane satırının herhangi k tanesinin OR'lanması sonucu oluşan vektörün (V), seçildiği kümeye bağlı olarak; B_0 'dan seçilen bir matris için $H(V) \le d - \alpha m$ veya B_1 'den seçilen bir matris için $H(V) \ge d$ olmalıdır.
2. $\{1, 2, \ldots, n\}$'nin herhangi alt kümeleri $\{i_1, i_2, \ldots, i_q\}$ $(q \langle k)$ için, B_0 ve B_1 matrislerinin içermiş olduğu matrislerin sıklığı eşit olmalıdır.

İlk parametre kontrast olarak adlandırılırken, ikinci parametre şemanın güvenliğini garanti eder. İkinci koşul sayesinde, k adetten az sayıda payın üst üste getirilmesi ile sırın elde edilemeyeceği garanti edilir.

(k, n) GSP şemalarının nasıl kurulabileceğini göstermek amacıyla, *(2, 2)* durumu bir örnek ile açıklanacaktır. B_0 ve B_1 matrisleri aşağıdaki şekilde tanımlanabilir.

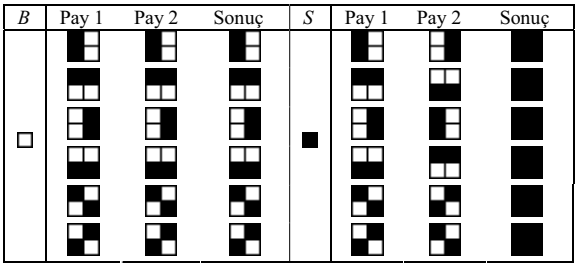
$$B_0 = \left\{ \begin{matrix} \textit{kolonları n permütasyonu ile} \\ \textit{elde edilen tüm matrisler} \end{matrix} \begin{pmatrix} 1 & 0 & 1 & 0 \\ 1 & 0 & 1 & 0 \end{pmatrix} \right\}$$

$$B_1 = \left\{ \begin{matrix} \textit{kolonları n permütasyonu ile} \\ \textit{elde edilen tüm matrisler} \end{matrix} \begin{pmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \end{pmatrix} \right\}$$

B_0 ve B_1 kümelerini oluşturan matrislerin satırlarının görünme olasılıkları birbirlerine eşittir. Bu da belirli bir örüntünün belirli bir renge ait olduğu bilgisinin gizli görüntüyü ele geçirmeye çalışan saldırganlar tarafından çıkarılmasına engel olacaktır. Permütasyon işleminin gerçekleştirileceği matrislerden de anlaşılacağı üzere, B_0 kümesini oluşturan herhangi bir matrisin satırlarının OR'lanması sonucu oluşan vektörün Hamming uzaklığı *2* iken (beyaz pikseli temsil eder), B_1 kümesindeki bir matris için hesaplanan Hamming uzaklığı *4* olacaktır. Aradaki fark, insan gözünün siyah ve beyaz arasında ayrım yapmasını sağlayacak karşıtlığı oluşturmaktadır.

Kodlama işlemi esnasında, gizli görüntüdeki beyaz pikselin kodlanması için B_0 kümesinden rasgele bir matris seçilecektir (R_0). Birinci payda karşı düşen alt piksel grubunun içeriği R_0 'ın birinci satırı tarafından belirlenirken, ikinci payın karşı düşen piksel grubu ikinci satır tarafından belirlenecektir. Benzer şekilde siyah pikselin kodlanması için kullanılacak olan matris ise B_1 kümesindeki matrisler arasından seçilecektir. Görüntüdeki tüm siyah ve beyaz pikseller için bahsedilen kodlama gerçekleştirildiğinde, sırrı paylaşacak olan kişilere dağıtılacak olan paylar oluşturulmuş olmaktadır. Açıklanan kodlama işlemine ilişkin bir örnek Tablo 1'de verilmektedir.

Tablo 1. (2,2) şeması için siyah ve beyaz piksellerin kodlanması.



Gizli görüntüdeki her bir pikselin, paylarda kaç alt piksel ile temsil edileceği GSP şemalarının oluşturulmasındaki parametrelerden biridir. Verilen örnekte bu değer *2* olarak seçilebileceği halde resmin en boy oranında bozulmaya neden olmaması için her iki doğrultuda da *2* olacak şekilde, yani *4* olarak belirlenmiştir. Şemanın karşıtlığını belirten α değeri, kodlanmış beyaz piksel ile siyah pikselin Hamming uzaklıkları arasındaki farktır. α değerinin büyük olması, tekrar yapılandırılan resmin karşıtlığını, bir başka deyişle görünebilirliğini iyileştirecektir. Verilen bu örnekte α değeri ikidir.

B. Olasılıklı Görsel Sır Paylaşma (OGSP)

2004 yılında Yang tarafından olasılıklı görsel sır paylaşma olarak adlandırılan yeni bir yöntem önerilmiştir. Yeni yöntemin ürettiği payların büyüklüğü, geleneksel yöntemlerden farklı olarak, paylaşılacak olan gizli görüntü ile aynı kalmaktadır. Üretilen payların boyutlarının, gizli görüntü ile aynı kalması, bellekte saklama kapasitesi açısından önemli ölçüde kazançları da beraberinde getirmektedir. Yeni şema beyaz piksellerin siyah ve beyaz bölgede görünme sıklığını, insan gözünün siyah ve beyazı ayırt etmesini sağlayacak şekilde kullanmaktadır. Yang, yayınında vermiş olduğu tanım bağıntıları ile *(2, 2), (2, n), (k, k) ve (k, n)* şemalarının nasıl oluşturulabileceğini göstermiştir.

Olasılıklı yöntemi geleneksel yöntemden ayıran en önemli fark, kodlanacak olan görüntüdeki pikseli birden çok alt pikselle paylarda temsil etmek yerine tek bir piksel ile kodlamasıdır. Orijinal görüntünün yeniden yapılandırılması için gereken yalnızca gerekli (*(k, n)* lik bir şema için en az k adet payın üst üste getirilmesidir. Bu da geleneksel yöntemdeki OR'lanma işlemine karşı düşmektedir. Geleneksel yöntem beyaz pikseli temsil etmek için $x_0 B y_0 S$ (x_0 adet beyaz, y_0 adet siyah), siyah pikseli temsil etmek için ise $x_1 B y_1 S$ kullanır. Bir pikselin kaç alt pikselle temsil edildiği m ile gösterilecek olursa, $x_0 + y_0 = x_1 + y_1 = m$ olacaktır. OGSP şemalarında ise m değeri 1'e eşit olacaktır. Geleneksel yöntemde kullanılan, n×m büyüklüğündeki B_0 ve B_1 matrislerinin yerini, n×1 büyüklüğündeki B_0 ve B_1 matrisleri alacaktır. Beyaz piksellerin kodlanması esnasında, B_0 kümesinden rasgele bir matris seçildikten sonra, rasgele seçilen satırlardaki değerler paylara dağıtılacaktır. Siyah piksellerin kodlanması esnasında kullanılacak olan matris B_1 matrisleri arasından seçilecektir. Yeniden yapılandırılma esnasında oluşacak görüntüyü, üst üste getirilen payların, piksel düzeyinde oluşturdukları Hamming ağırlıkları belirleyecektir. Siyah ve beyaz bölgelerdeki beyaz sıklığı, yeniden yapılandırılan resmin, insan gözü tarafından ayırt edilebilmesini sağlayacaktır. p_0, yeniden yapılandırılan resmin beyaz bölgesinde beyaz pikselin görünme olasılığını temsil eder. p_1 ise, siyah bölgede beyaz görünme olasılığını verecektir. Beyaz ve siyahın ayırt edilmesini belirleyecek parametrelerden biri olan değişmez eşik olasılığı p_{th} ile gösterilsin.

(k, n) OGSP şeması ancak aşağıdaki üç durumu sağlıyorsa geçerlidir:

1. B_0 ve B_1 kümelerindeki her bir matrisin herhangi k satırlarının oluşturduğu sütun vektörü *V* ile gösterilsin. *L(V)* ise ilgili vektörün satırlarının OR'lanması sonucu elde edilen değer olsun. B_0 kümesinden elde edilen *L(V)* değerleri λ kümesini, B_1 den elde edilen değerler ise γ kümesini oluştursun.

2. λ ve γ kümeleri, $(p_0 \geq p_{th})\, ve\, (p_1 \leq p_{th} - \alpha)$ koşullarını sağlayacaktır.

3. $\{1, 2, \ldots, n\}$'nin herhangi alt kümelerinde $\{i_1, i_2, \ldots, i_q\}$ $(q \langle k)$, p_0 ve p_1 değerleri eşit olacaktır.

Böyle bir şemanın nasıl yapılandırılacağını gösterebilmek amacıyla , *(2, 2)* OGSP şemasının [14]'de verilen tanım bağıntısı kullanılacaktır. μ_{ij}, Hamming ağırlığı *i* olan bütün *n×1* 'lik kolon matrislerini temsil eder. *j* indisi ise, matrisin B_0 veya B_1 'e ait olduğunu gösterecektir, $j \in \{0, 1\}$. Örneğin *n=3* iken, $\mu_{2,0}$ kümesine ait matrisler aşağıdaki şekildedir.

$$\mu_{2,0} = \left\{ \begin{bmatrix} 0 \\ 1 \\ 1 \end{bmatrix}, \begin{bmatrix} 1 \\ 0 \\ 1 \end{bmatrix}, \begin{bmatrix} 1 \\ 1 \\ 0 \end{bmatrix} \right\}$$

Tanım 2. $B_0 = \{\mu_{0,0}, \mu_{2,0}\}$ ve $B_1 = \{\mu_{1,1}\}$. B_0 ve B_1, (2, 2) OGSP'nin oluşturulması için gerekli *2×1* lik matrislerin kümesidir. Bu durumda B_0 ve B_1 ait matrisler aşağıdaki şekilde verilebilir.

$$B_0 = \{\mu_{0,0}, \mu_{2,0}\} = \left\{ \begin{bmatrix} 0 \\ 0 \end{bmatrix}, \begin{bmatrix} 1 \\ 1 \end{bmatrix} \right\} \quad B_1 = \{\mu_{1,1}\} = \left\{ \begin{bmatrix} 1 \\ 0 \end{bmatrix}, \begin{bmatrix} 0 \\ 1 \end{bmatrix} \right\}$$

$$\lambda = \left\{ L\left(\begin{bmatrix} 0 \\ 0 \end{bmatrix} \right), L\left(\begin{bmatrix} 1 \\ 1 \end{bmatrix} \right) \right\} = \{0, 1\}$$

$$\gamma = \left\{ L\left(\begin{bmatrix} 1 \\ 0 \end{bmatrix} \right), L\left(\begin{bmatrix} 0 \\ 1 \end{bmatrix} \right) \right\} = \{1, 1\}$$

λ ve γ 'da pikselin beyaz olma olasılığı olan p_0 ve p_1 sırayla 0.5 ve 0'dır. Bu nedenle bu şemaya ait eşik olasılığı olan $p_{th} = 0.5$ ve karşıtlık $\alpha = 0.5$ 'dir.

III. (2, N) OLASILIKLI GÖRSEL SIR PAYLAŞMA YÖNTEMİ

Bu bölümde öncelikle Wang tarafından önerilen *(2, n)* OGSP şemasının tanımı verilecek daha sonra ise yayın kapsamında önerilen yöntemden bahsedilecektir.

A. Wang'ın (2, n) OGSP şeması

Wang tarafından önerilen bu şema XOR ve AND gibi mantıksal işlemlerin kullanımına dayanır [14]. Gizli görüntünün ortaya çıkarılması sırasında insan görme sistemi yerine, özel bir yazılım gerektirmeden görüntüleme yazılımlarının olanakları kullanılabilmektedir. Önerilen yöntem, orijinal görüntüdeki siyah pikselleri kesin doğrulukla yeniden yapılandırabilirken, beyaz pikselleri doğru olarak yapılandırma olasılığı 0.5'dir. Önerilen şemanın payları oluşturmak için gerçekleştirdiği adımlar aşağıdaki şekilde verilebilir.

Girişler: n ile ifade edilen bir tamsayı değeri ($n \geq 2$) ve A ile gösterilen gizli görüntü.

Adım 1: $B_1, B_2, \ldots, B_{n+1}$ ile gösterilen $(n+1)$ adet matris üret.

Adım 2: $C_1, C_2, \ldots, C_n$ ile gösterilen n adet ara matrisi $C_i = B_i \,\&\, A, i = 1, 2, \ldots, n$ denklemini kullanarak hesapla.

Adım 3. $A_1, A_2, \ldots, A_n$ ile gösterilen n adet payı $A_i = C_i \oplus B_{n+1}, i = 1, 2, \ldots, n$ denklemini kullanarak hesapla.

Gizli görüntünün (A') oluşturulması için gerçekleştirilecek olan yapılandırma işlemi Denklem 1'de verilmektedir.

$$A' = A_i \oplus A_j, i, j \in \{1, 2, \cdots, n\} \; ve \; i \neq j \qquad (1)$$

$A_i(s,t)$ basitçe A_i olarak gösterilsin. Yukarıda bahsedilen yapılandırma adımları göz önüne alındığında A ile gösterilen gizli görüntüdeki herhangi bir siyah pikselin i ile gösterilen paya kodlanması esnasında $C_i = B_i \,\&\, 0 = 0$ olacaktır. Buradan da i ile gösterilen paydaki piksel değeri $A_i = B_{n+1} \oplus 0 = B_{n+1}$ olacaktır. Böylece gizli görüntünün yeniden yapılandırılması esnasında $A' = A_i \oplus A_j = B_{n+1} \oplus B_{n+1} = 0$ olacaktır. Buradan da kodlanan siyah piksellerin yeniden yapılandırma esnasında kesin doğrulukla oluşturulacağını göstermektedir.

A'daki beyaz (*'1'*) piksel için $C_i = B_i \,\&\, 1 = B_i$ ve $A_i = B_{n+1} \oplus B_i$ olacaktır. Böylece gizli görüntünün yeniden yapılandırılması için i ve j ile gösterilen payların bir araya getirilmesi sonucu (2) deki ifade elde edilecektir.

$$A' = B_{n+1} \oplus B_i \oplus B_{n+1} \oplus B_j = B_i \oplus B_j \qquad (2)$$

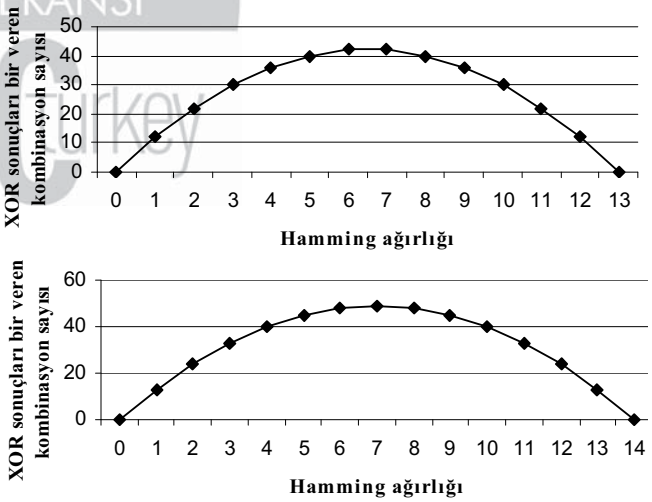
Yukarıdaki ifadeden de görüleceği gibi, beyaz bir pikselin doğru olarak kodlanma olasılığı ½'dir. Bu olasılık aynı zamanda XOR fonksiyonunun sonucunda *1* görülme olasılığını temsil etmektedir.

Wang tarafından önerilen *(2, n)* OGSP şeması, gizli görüntü A ile yeniden yapılandırılan görüntü A' arasında *0* bitlerini aynı tutmayı başarırken, *1* bitlerini doğru kodlayabilme olasılığı ½'dir. Bu nedenle de bu şemaya ilişkin α değeri ile gösterilen kontrast değeri ½'dir. Olasılıksal bir yöntem olan bu şemanın kontrast değerinin ölçümünde (3) bağıntısı kullanılmıştır.

$$\alpha = \frac{p_0 - p_1}{1 + p_1} \qquad (3)$$

B. Önerilen (2, n) OGSP şeması

2007 yılında Wang tarafından önerilen yöntemde, orijinal gizli görüntüdeki beyaz piksellerin yeniden doğru bir şekilde yapılandırma olasılığı XOR fonksiyonuna giriş olarak verilen iki rasgele matrisin (B_i *veya* B_j) karşılıklı piksellerin değerlerine bağlıdır. *(2, n)* GSP şeması için oluşturulması gereken rasgele B matrisi sayısı *n+1* dir. Son matris hariç (B_{n+1}) geri kalan matrisler, beyaz piksellerin doğru bir şekilde yeniden yapılandırılmasında rol oynayacaktır. Makalede önerilen yöntemde, tüm bu matrisler birbirlerinden bağımsız olarak rasgele anlamda üretilmektedir. N tane matrisin herhangi ikisinin karşılıklı elemanlarının XOR sonucunun *1* verme olasılığı ½'dir. Yeniden yapılandırma sonucunda oluşan görüntünün doğruluk oranını yükseltebilmek, algoritmanın beyaz pikselleri yeniden üretmedeki başarı oranını yükselterek gerçekleşecektir. Bu nedenle B matrisleri birbirlerinden bağımsız olarak üretilmek yerine, n adet matrisin karşılık düşen piksellerine yerleştirilecek değerler seçilirken, XOR sonucunun farklılık durumunda *1* verdiği göz önüne alınmalıdır. n boyutlu bir diziden seçilen ikili kombinasyonların XOR sonuçlarının *1* verme olasılığını yükseltmek, yöntemin başarısını yükseltmekle eşdeğerdir. *n=13* ve *n=14* elemanlı bir vektörün sahip olabileceği farklı Hamming ağırlıklarına bağlı olarak, iki elemanlı kombinasyonların XOR sonuçlarının *1* verdiği durumların sayısına ait grafik Şekil 1'de verilmiştir. Alınan ikili kombinasyonların en çok sayıda bir verdiği durum, simetri nedeni ile n değerinin çift veya tek olmasına göre değişmektedir. Toplam pay sayısını gösteren n değerinin çift olduğu durumlarda tek bir maksimum değer varken, tek olduğu durumlarda iki maksimum değer vardır.



Şekil 1. Sırasıyla n=13 ve n=14 için farklı hamming ağırlıklı vektörlerin, kendi ele-manlarının ikili kombinasyonlarının XOR sonuçlarının değerlendirilmesi.

B matrislerindeki karşılıklı pikselleri n boyutlu vektörler oluşturmaktadır. Matrislerin Wang tarafından önerildiği şekilde ayrık olarak oluşturulması yerine, karşılıklı elemanlarının oluşturduğu vektörlerin sınırlı bir rasgelelik kullanılarak seçilmesi yeniden yapılandırılan resmin doğruluğunu artıracaktır. B mat-

rislerini oluşturmak için önerilen yöntem Şekil 2'de verilmektedir. Orijinal görüntünün *N×M* boyutlarında olduğu varsayılmıştır.

Gösterimde *B* matrislerinin karşılıklı elemanlarına yerleştirilecek olan değerleri içeren vektör *v* ile gösterilmektedir. *V* vektörünün içeriği *E* ile gösterilen vektör uzayından seçilen rasgele bir vektörün içeriği olacaktır. *E* uzayının oluşturulması esnasında toplam pay sayısının çift veya tek olması durumu göz önüne alınmaktadır. Çift olması durumunda değer atamada kullanılacak vektörler kümesi elemanlarının Hamming ağırlıkları, toplam pay sayısının yarısına eşittir. $\mu_{n/2}$ ifadesi, Hamming ağırlığı $n/2$ olan $1\times n$ boyutundaki vektörleri temsil etmektedir. Bu durumda tek sayı olan bir n değer için, *E* kümesi $\mu_{\lfloor n/2\rfloor}$, $\mu_{\lfloor n/2\rfloor+1}$ değerlerinden oluşacaktır. Uygun bir şekilde oluşturulan *E* kümesinden rasgele seçilen bir vektör değerini taşıyan v vektörünün içeriği, *B* matrislerinin o an işlem görmekte olan karşılıklı piksellerinin içeriğini oluşturacaktır. *B* matrislerinin, *j* ve *k* ile gösterilen koordinatlarındaki piksel değerleri *v* vektörünün içeriğine uygun olarak doldurulur. Böylelikle gizli görüntünün yeniden yapılandırılması aşamasında n pay içerisinden seçilecek rasgele iki payın *1* üretme olasılığı yükseltilmiş olacaktır.

$$
\begin{aligned}
&\textit{if } n \circ 2 == 0 \\
&\quad E = \left\{ \mu_{n/2} \right\} \\
&\quad K = C_{n/2}^{n} \\
&\quad v = \left\{ v^i \mid v^i \in E, i \in \left\{ 1, 2, \ldots, K \right\} \right\} \\
&\quad v^i = \left\{ v_j^i \mid \ j \in \left\{ 1, 2, \ldots, n \right\} \right\} \\
&\textit{if } n \circ 2 == 1 \\
&\quad E = \left\{ \mu_{\lfloor n/2 \rfloor}, \mu_{\lfloor n/2 \rfloor+1} \right\} \\
&\quad K = C_{\lfloor n/2 \rfloor}^{n} + C_{\lfloor n/2 \rfloor+1}^{n} \\
&\quad v = \left\{ v_i \mid v_i \in E, i \in \left\{ 1, 2, \ldots, \ K \right\} \right\} \\
&\quad v^i = \left\{ v_j^i \mid \ j \in \left\{ 1, 2, \ldots, n \right\} \right\} \\
&B = \left\{ B^i \mid i \in \left\{ 1, 2, \ldots, n \right\} \right\} \\
&B^i = \left\{ B_{jk}^i \mid \ j \in \left\{ 1, 2, \ldots, N \right\}, \ k \in \left\{ 1, 2, \ldots, M \right\} \right\} \\
&B_{jk}^i = v_i^m, \ i \in \left\{ 1, 2, \ldots, n \right\}, m = \left(rand \times \left(K - 1 \right) \right) + 1
\end{aligned}
$$

Şekil 2. *B* matrislerini oluşturmak için önerilen yöntem.

E kümesi aslında OGSP yönteminin *(2, n)* şemalar için siyah pikselleri kodlamada kullanmış olduğu küme bağıntısı ile eş değerdir. Bu nedenle, aslında önerilen yöntem sonucunda oluşan *B* matrislerinin içeriği, tümüyle siyah piksellerden oluştuğu varsayılan gizli bir görüntü üzerinde *(2, n)* OGSP yöntemi kullanılarak üretilen paylarla eşdeğerdir.

IV. SONUÇLAR

Önerilen yöntemin, Wang'ın yönteminden üstünlüğünü gösterebilmek amacı ile yapılan testlerde Şekil 3'de verilen 256×256 boyutlarındaki renksiz "Lena" görüntüsü Floyd-Steinberg yöntemi ile yalnız siyah ve beyaz piksellerden oluşan görüntüye dönüştürülerek kullanılmıştır. Her iki yöntem de Matlab 7.0 ortamında programlanmıştır. Testler, Intel® Core 2 Duo 1.66 GHz işlemcili ve 1 GB RAM'i olan taşınabilir bir bilgisayar üzerinde gerçekleştirilmiştir. İşletim sistemi olarak Windows XP Professional kullanılmıştır.

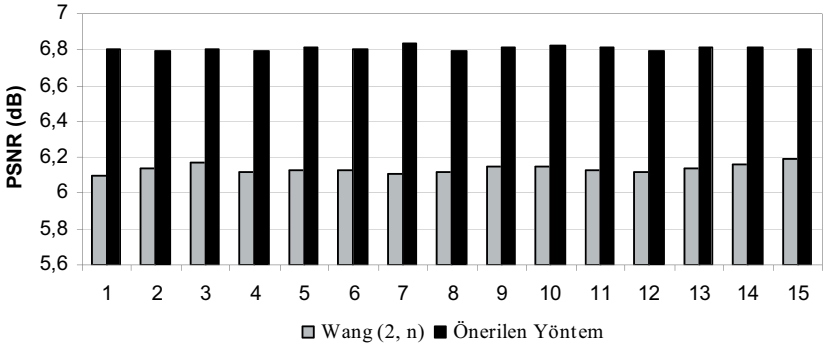
Şekil 3. 256×256 büyüklüğündeki test görüntüsü

Değerlendirme için her iki yöntem tarafından yeniden yapılandırılan resimlerin doğruluk oranı dikkate alınmıştır. Doğruluk oranını belirleyebilmek için PSNR değerleri hesaplanmıştır. Sabit bir n değeri için, yeniden yapılandırma aşamasında oluşabilecek C_n^2 farklı durum göz önüne alınmıştır. Kombinasyonların XOR'lanması sonucu elde edilen görüntülerin, orijinal görüntüden farkı doğruluk oranı hakkında yorum yapılabilmesini sağlamıştır. PSNR değerlerinin hesaplanması için kullanılan ifade Denklem 4'de verilmiştir.

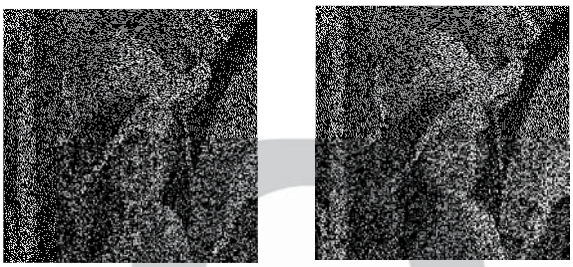
$$
\begin{aligned}
PSNR &= 10\log_{10}\frac{Maks^2}{MSE}\,dB \\
MSE &= \frac{1}{N\times M}\sum_{i=1}^{N}\sum_{j=1}^{M}\left(x_{ij}-a_{ij}\right)^2
\end{aligned}
\qquad (4)
$$

*Mak*s, görüntüdeki piksellerin sahip olabileceği parlaklık değeri aralığının üst sınırını gösterir. Makalede işlenilen görüntünün siyah beyaz olması sebebi ile bu değer 1 olarak alınmıştır. Verilen ifadede, PSNR değeri, *N×M* boyutlarındaki *X* ile gösterilen gizli görüntünün, *A* ile gösterilen orijinal görüntüden ne kadar farklı olduğunun bir ölçütüdür. Daha yüksek PSNR'ye sahip yeniden yapılandırma sonucu oluşan görüntü orijinale daha çok benzemektedir. x_{ij} ve a_{ij}, sırasıyla test ve orijinal görüntünün *(i, j)* koordinatlarındaki piksel değerlerini göstermektedir.

Şekil 4'de *n*=6 değeri için önerilen yöntemle oluşturulan 6 farklı payın aralarında oluşturabilecek olduğu 15 farklı kombinasyonun, üretecek olduğu yeniden yapılanmış resimlere ilişkin PSNR değerleri verilmektedir. Şekilden de görüldüğü gibi, Wang tarafından önerilen yöntemin yeniden yapılandırdığı görüntülerin PSNR değerleri 6.1dB düzeyinde olmasına karşılık önerilen yöntemle 6.8 dB düzeyine yükselmiştir. Gösterilen serilerde maksimum değer oluşumu sağlayan pay kombinasyonlarının üretmiş olduğu sonuç görüntüler Şekil 5.a ve Şekil 5.b'de gösterilmektedir.



Şekil 4. PSNR değerleri ile yöntemlerin karşılaştırma sonuçları.



(a) (b)

Şekil 5.(a) (b) Sırasıyla Wang'ın yöntemi ve önerilen yöntem ile yeniden yapılandırılan görüntüler.

V.DEĞERLENDİRME

Yapılan çalışmada 2007 yılında Wang tarafından önerilmiş olan tekniğin üretmiş olduğu yeniden yapılandırılan görüntünün PSNR değerinin iyileştirilmesi amaçlanmıştır. Bu kapsamda yöntem tarafından kullanılan rastgele matrislerin üretimi için yeni bir yöntem önerilmiştir. Sonuçlar kısmında da vurgulandığı gibi, her iki yöntemin yeniden yapılandırdığı resimler arasında sayısal ve görsel bir farklılık mevcuttur. İlerleyen çalışmalarda, ilgili yöntemin (k, n) şemasına genelleştirilmesi amaçlanmıştır.

KAYNAKLAR

[1] G. R. Blakley, "Safeguarding Cryptographic Keys," *Proceedings of the National Computer Conference, American Federation of Information Processing Societies Proceedings, New York, USA*, pp. 313-317, June 1979.

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

[3] M. Naor, A. Shamir, "Visual Cryptography," *Advances in Cryptology - Eurocrypt'94, LNCS*, vol. 950, pp. 1-12, 1995.

[4] Hou, Y.-C., "Visual cryptography for color images", *Pattern Recognition*, vol. 36, pp. 1619-1629, 2003.

[5] Lin, C.-C., Tsai, W.-H., "Visual cryptography for gray-level images by dithering techniques", *Pattern Recognition Letters*, vol. 24, no. 1-3, pp. 349–358, 2003.

[6] Shyu, S. J., "Efficient visual secret sharing scheme for color images", *Pattern Recognition*, vol. 39, no. 5, pp. 866–880, 2006.

[7] Wu, C. C., Chen, L. H., "A study on visual cryptography", *Master Thesis, Institute of Computer and Information Science, National Chiao Tung University*, Taiwan,1998.

[8] Wu, H.-C., Chang, C.-C.,"Sharing visual multi-secrets using circle shares", *Computer Standards & Interfaces*, vol. 28, no.1, pp. 123–135, 2005.

[9] Shyu, S. J., Huang, S.-Y., Lee, Y.-K., Wang, R.-Z., "Sharing multiple secrets in visual cryptography", *Pattern Recognition*, vol. 40, no. 12, pp. 3633-3651, 2007.

[10] Cimato, S., De Prisco, R., De Santis, A., "Colored visual cryptography without color darkening", *Theoretical Computer Science*, vol. 374, no. 1-3, pp. 261–276, 2007.

[11] R. Ito, H. Kuwakado and H. Tanaka, "Image Size Invariant Visual Cryptography," *IEICE Transaction on Fundamentals*, no. 10, pp. 2172-2177, 1999.

[12] C.N. Yang, New visual secret sharing schemes using probabilistic method, *Pattern Recognition Letters*, vol. 25, no. 4, pp. 481–494, 2004.

[13] S. Cimato, R. De Prisco, and A. De Santis, "Probabilistic Visual Cryptography Schemes," *The Compututer Journal*, vol. 49, no. 1, pp. 97-107, 2006.

[14] D. Wang, L. Zhang, N. Ma, and X. Li, "Two Secret Sharing Schemes Based on Boolean Operations," *Pattern Recognition*, vol. 40, pp. 2776-2785, 2007.