International Journal of Scientific and Technological Research
ISSN 2422-8702 (Online), **DOI:** 10.7176/JSTR/5-5-12
Vol.5, No.5, 2019

Secure Transmission of 3D-QRMW Quantum Images via Quantum Fourier Transform in Blind Cloud

Omer Dogan (Corresponding author)
Canakkale Onkesiz Mart University, Graduate School of Natural and Applied Sciences,
Department of Computer Engineering, Canakkale, Turkey
E-mail: omerdogan@comu.edu.tr

Ihsan Yilmaz
Canakkale Onkesiz Mart University,
Department of Computer Engineering, Canakkale, Turkey
E-mail: iyilmaz@comu.edu.tr

Abstract
This study explores three-dimensional multi-channel quantum image representation model (3D-QRMW) which can be used in many fields such as three-dimensional medical imaging, atomic imaging, and infrared images. Quantum images are transmited between participants by Quantum Fourier Transform (QFT) in which output qubits are reordered by blind Cloud with permutation. Also key with length K=16N is applied to share signature for recipients. This allows all members to know only their signature information. Security analyzes show that quantum images in the model of 3D-QRMW are transmitted safely.

Keywords: 3D quantum image, Security of 3D quantum image, Blind Cloud, Quantum Fourier.

DOI: 10.7176/JSTR/5-5-12

1. Giriş

Son zamanlarda insanoğlu kuantum teknolojileri insanlık yararına kullanmaya başlamıştır. Kuantum teknolojilerin hem güvenlik hemde hız bakımından klasik yöntemlere göre üstün olması bu teknolojilere olan ilgiyi artırmıştır. Bu teknolojinin klasik teknolojilerde olmayan, süperpozisyon, dolanıklık, teleportasyon, super yoğun kodlama, kopyalanamama ve terslenebilirlik gibi üstün özellikleri vardır.
Kuantum teknoloji alanındaki çalışmalara her ne kadar kuantum bilgisayar alanındaki gelişmelere öncülük etse de kuantum teknolojisilerin birçok alana uygulaması da devam etmektedir. Bu alanlardan biride kuantum görüntü işlemedir. Kuantum görüntü işleme üzerine literatürde birçok çalışma bulunmaktadır. Örneğin; Venegas-Andraca ve Ball (2010) dolanık kübitleri kullanan "Entangled Image" fikrini önermişlerdir. Le ve ark. (2011) kuantum bilgisayarlar için kuantum görüntülerin esnek temsili (FRQI) modelini önermişlerdir. Bu çalışmada pozisyon ve renk bilgileri normalleştirilmiş kuantum durumları içermektedir. Sun ve ark. (2013) FRQI modelini geliştirerek Kırmızı-Yeşil-Mavi (Red-Green-Blue-RGB) üç kanallı kuantum görüntülerin temsili (MCQI) için model önermişlerdir. Zhang ve ark. (2013), her pikselin gri tonlama değerlerini saklamak için bir kubitin olasılık genliği yerine bir kubit dizisinin temel baz durumlarını kullanan sayısal görüntülerin gelişmiş kuantum temsili (NEQR) modelini geliştirmişlerdir. Li ve ark. (2013) görüntünün M-renk ve N-pozisyon bilgilerinin her ikisini de durum genliğinde tutan QSMC & QSNC modelini önermişlerdir. Zhang ve ark. (2013b) log-polar görüntülerin kuantum temsili (QUALPI) için bir model geliştirmişlerdir. Yuan ve ark. (2014), "Qubit Lattice" (Venegas-Andraca ve Bose, 2003) ve FRQI yöntemlerini kullanarak kızılötesi görüntülerin basit bir kuantum temsilini (SQR) sunmuşlardır. Abdolmaleky ve ark. (2017), NEQR modelini geliştirerek RGB üç kanallı renkli kuantum görüntülerin temsili için (QMCR) modelini önermişlerdir..
Son zamanlarda Şahin ve Yılmaz (2018a) tarafından uydu temelli, havadan uzaktan algılama, askeri hedef tespiti ile endüstriyel kalite kontrol, tıp ve biyofizikteki laboratuvar uygulamaları gibi birçok alanda kullanılacak, çok dalga boylu kuantum görüntüleme temsilini (QRMW) önerilmiştir.
Tıp alanında Radyolojik görüntülerin birçoğunun kesit alanından dolayı üç boyutlu olması, küçük ölçekli

ISSN 2422-8702 (Online), **DOI:** 10.7176/JSTR/5-5-12
Vol.5, No.5, 2019

ısıl görüntülerin üç boyuttlu bir yapıda olması gibi bir çok alanda üç boyutlu görüntüye ihtiyaç duyulmaktadır. Bu bağlamda Li ve ark. (2014), üç boyutlu görüntülerin kuantum temsili (NAQSS) için bir model önermişlerdir. Son zamanlarda da Yang ve ark. (2019) kuantum üç boyutlu termal görüntüleri incelemişlerdir. Literatüre bakıldığı zaman üç boyutlu görüntü işleme üzerine QRMW temsili kullanılarak yapılan bir çalışmaya rastlanmamıştır. Ayrıca bu temsil ile elde edilecek kuantum verinin iletilmesi üzerine de bir çalışma bulunmamaktadır. Bu nedenle üç boyutlu görüntülerin kuantum teknoloji ile güvenli bir şekilde iletilmesinin incelenmesi önemlidir.
Bu çalışmayı aşağıdaki şekilde özetleyebiliriz; Çalışmanın ikinci bölümünde daha önceki yapılan kuantum görüntü temsil modellerine değinilmiştir. Üçüncü bölümde Üç boyutlu-çok dalga boylu kuantum görüntü temsili (QRMW) açıklanmıştır. Dördüncü bölümde Üç boyutlu-çok dalga boylu kuantum görüntü temsilinde (QRMW) güvenli görüntü iletimide süreçler tanımlanmıştır. Beşinci bölümde güvenlik analizi yapılmıştır. Altıncı bölümde sonuç ve önerilere yer verilmiştir.

2. Önceki Çalışmalar

2.1. FRQI Modeli

Le ve ark. (2011) tarafından gri tonlu görüntüler üzrine oluşturulan kuantum temsil modelidir. Görüntüdeki ilgili pozisyon piksellerinin renk bilgisini alır ve her birini aşağıdaki gibi bir kuantum durumda ifade edilir. Durum genliğinde renk bilgisi tutulur ve renk bilgisini geri alma işlemi olasılıksaldır. $2^n \; x \; 2^n$ boyutlu görüntünün FRQI modelinde temsil ifadesi aşağıdaki şekildedir (Le ve ark., 2011).

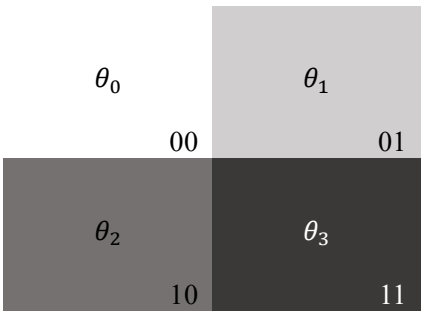
$$|I\rangle = \frac{1}{2^n} \sum_{i=0}^{2^{2n}-1} |c_i\rangle \otimes |i\rangle$$

$$|c_i\rangle = cos\theta_i \, |0\rangle + sin\theta_i \, |1\rangle$$

$$|i\rangle, i = 1,2,3,..2^n - 1$$

$$\theta = (\theta_1, \theta_2, \ldots . \theta_{2^{2n}-1}), \quad \theta_i \in [0,\pi/2]$$

Şekil 2.1 de FRQI modelinde *2x2* boyutlu örnek bir görüntü aşağıdaki gibi gösterilmişitir.



Şekil 2.1. *2x2* boyutunda örnek FRQI modeli gösterimi (Le ve ark.,2011).

ISSN 2422-8702 (Online), **DOI:** 10.7176/JSTR/5-5-12
Vol.5, No.5, 2019

2.2. QUALPI Modeli

Bu görüntü modeli Zhang ve ark. (2013b) tarafından önerilen kuantum temsil modelidir. Birçok mevcut modelde görüntüler kartezyen koordinatlarda saklanırken bu modelde boyutlandırma ve döndürme gibi bir çok karmaşık dönüşümün bu modele uygulanması için bir çok ek işleme ihtiyaç duyulmaktadır. Her bir piksel baz durumlarında tutularak, 2^q renk skalası olan bir görüntünün logaritmik-yarıçap örnekleme çözünürlüğü 2^m ve açısal yönelimleri 2^n olduğu düşünülürse bu model aşağıdaki gibi ifade edilir (Zhang ve ark.,2013b).

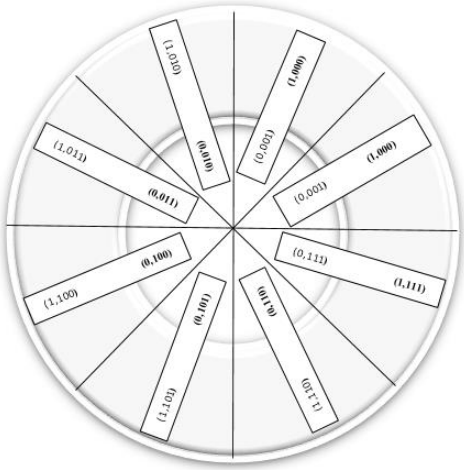
$$|I\rangle = \frac{1}{\sqrt{2^{m+n}}} \sum_{\rho=0}^{2^m-1} \sum_{\theta=0}^{2^n-1} |k(\rho,\theta)\rangle \otimes |\rho\rangle \otimes |\theta\rangle$$

$$k(\rho,\theta) = C_0, C_1, C_2 \ldots . C_{q-1}\,, \qquad k(\rho,\theta) \in [0, 2^q - 1]$$

$$\theta = tan^{-1} \frac{y - y_c}{x - x_c}$$

$$\rho = \log_{taban} \sqrt{(x - x_c)^2 + (y - y_c)^2}$$

Burada x_c ve y_c; logaritmik polar görüntünün kartezyen koordinatlarının merkezidir. *2x8* boyutunda QUALPI modelinin örnek bir logaritmik polar görüntüsü Şekil 2.2'de ifade edilmiştir.



Şekil 2.2. 2x8 boyutlarında örnek bir logaritmik polar görüntüsü (Zhang ve ark., 2013b)

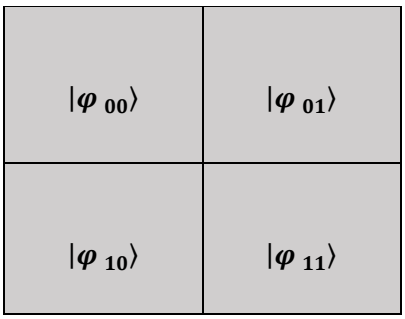
2.3. SQR Modeli

Yuan ve ark. (2014) tarafından sadece kızılötesi dalga boyundaki yani tek bantlı görüntülerin kuantum temsili için ortaya konulmuştur. Her bir piksel $|\varphi_{ij}\rangle$ olarak ifade edilir ve tensörel çarpım şeklinde tutulur. $M_1 x\, M_2$ boyutlarında bir görüntünün SQR modelinde temsil ifadesi aşağıdaki gibidir (Yuan ve ark.,2014).

$$|I\rangle = \otimes_{ij=0}^{M_1 M_2 - 1} |\varphi_{ij}\rangle$$
$$|\varphi_{ij}\rangle = cos\theta_{ij}\,|0\rangle + sin\theta_{ij}\,|1\rangle$$

i= 0,1,2,..M_1-1 , j= 0,1,2,..M_2-1

Aşağıda SQR modelinin 2x2 boyutundaki örnek bir görüntüsü Şekil 2.3.'de gösterilmiştir.



Şekil 2.3. *2x2* boyutlarında örnek bir görüntü (Yuan ve ark.,2014)

2.4. NEQR Modeli

Zhang ve ark. (2013a) tarafından gri tonlu görüntüleri temsil etmek üzere FRQI modelinden farklı olarak renk bilgisini genlik yerine kübit dizisinin baz durumlarında tutmaktadır. Bu sebepten ötürü renk bilgisini geri alma işlemi olasılıksal olarak değil kesin olarak bilinmektedir. 2^a renk skalalı, 2^bx2^b boyutlarında bir görüntünün NEQR modelinde temsili aşağıdaki gibidir (Zhang ve ark. 2013a).

$$|I\rangle = \frac{1}{2^b}\sum_{y=0}^{2^b-1}\sum_{x=0}^{2^b-1}|f(x,y)\rangle \otimes |yx\rangle$$

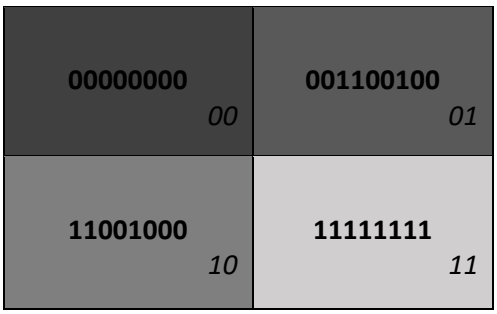
$$\frac{1}{2^b}\sum_{y=0}^{2^b-1}\sum_{x=0}^{2^b-1}\bigotimes_{i=0}^{a-1}|c_{yx}^{i}\rangle\,|yx\rangle$$

$$f(x,y) = c_{yx}^{0}c_{yx}^{1}\ldots.c_{yx}^{a-1}$$

$$c_{yx}^{i} \in [0,1], f(y,x) \in [1, 2^a - 1]$$

Burada f(x,y); uygun pikselin renk bilgisinin ikili dizge karşılığıdır.

NEQR modelinde 2^8 renk skalalı, 2x2 boyutlarında örnek bir görüntü Şekil 2.4. te gösterilmiştir.



Şekil 2.4. 2x2 boyutlarında örnek bir NEQR görüntü modeli (Zhang ve ark., 2013a)

2.5. QMCR Modeli

Abdolmalekya ve ark.(2017) tarafından gri tonlu NEQR modelinin RGB (üç renkli) görüntü temsili için geliştirilmiştir ve renk bilgisi kübit dizinin baz durumunda tutulmaktadır. Her bir renk kanalının renk skalası 2^a olan $2^b x 2^b$ boyutlarında bir üç renkli kuantum görüntünün QMCR modelinde temsili aşağıdaki gibidir (Abdolmalekya ve ark., 2017).

$$|I\rangle = \frac{1}{2^b}\sum_{y=0}^{2^b-1}\sum_{x=0}^{2^b-1}|C_{RGByx}\rangle \otimes |yx\rangle$$

$|C_{RGByx}\rangle$ kuantum durumu; yx pikselinin üç renkli kanallarının her birinde gri ton aralığı 2^a olarak kodlamak için kullanılmaktadır. Bu durum aşağıdaki şekilde gösterilmektedir (Abdolmalekya ve ark.,2017).

$$|C_{RGByx}\rangle = |R_{yx}\rangle\,|G_{yx}\rangle\,|B_{yx}\rangle$$

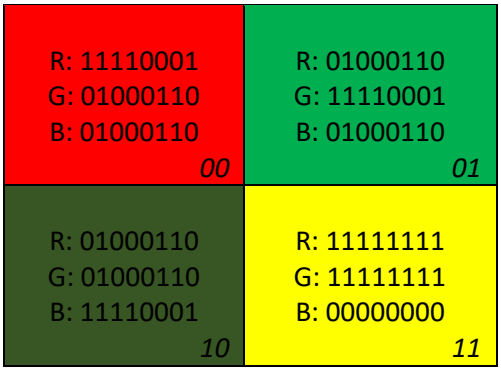
$$|R_{yx}\rangle = |r_{yx}^{a-1} r_{yx}^{a-2} \ldots\ldots r_{yx}^{0}\rangle$$

$$|G_{yx}\rangle = |g_{yx}^{a-1} g_{yx}^{a-2} \ldots\ldots g_{yx}^{0}\rangle$$

$$|B_{yx}\rangle = |b_{yx}^{a-1} b_{yx}^{a-2} \ldots\ldots b_{yx}^{0}\rangle$$

$$r_{yx}^{k}, g_{yx}^{k}, b_{yx}^{k} \in \{0,1\}\ ve\ R_{yx}, G_{yx}, B_{yx} \in \{0,1, \ldots\ldots 2^a - 1\}$$

MCR modelininde 2^8 renk skalalı, *2x2* boyutlarında örnek bir RGB görüntü Şekil 2.5. te gösterilmiştir.



Şekil 2.5. *2X2* boyutunda 2^8 skalalı örnek bir QMCR modeli (Abdolmalekya ve ark.2017)

2.6. QRMW Modeli

Şahin ve Yılmaz (2018a) tarafından ortaya konulan bu kuatum görüntü modeli temsili çok kanallı (üçten fazla) ve 2^nx2^m boyutlarına sahip görüntülerin kuantum temsili için önerilmiştir. Bu modelde görüntünün piksellerinin her birinin farklı dalga boylarındaki değerlerini tutmak için bir kübit dizisinin temel modları kullanılmıştır. Temsilde dalga boyu kanal sayısı *cn*, her bir kanaldaki renk değerlerinin maksimum 2^q olduğu bir görüntü düşünülürse, modelde 2^nx2^m boyutlarında görüntü için; renk değerleri için q-kübit ve pozisyon bilgisi için (n+m)-kübite, cn dalga boyu için ihtiyaç duyulan kübit *b*-kübit ($b=ceil(log_2 cn)$)'dir. Bu modelde 2^b kanallı, 2^nx2^m boyutlarında çok dalga boylu kuantum görüntü temsili (QRMW) aşağıdaki gibi formüle edilmiştir (Şahin ve Yılmaz, 2018a).

$$|I\rangle = \frac{1}{\sqrt{2^{b+n+m}}} \sum_{\lambda=0}^{2^b-1} \sum_{y=0}^{2^n-1} \sum_{x=0}^{2^m-1} |f(\lambda, y, x)\rangle \otimes |\lambda\rangle \otimes |yx\rangle$$

Burada yx; pikselin pozisyonunu, λ; yx pikseliyle ilişkili dalga boyunu göstermektedir. $|f(\lambda, y, x)\rangle$ durumu ise yx pikselinin ilgili λ dalga boyunun renk değerini göstermektedir ve aşağıda şekilde ifade edilmektedir.

$$|f(\lambda, y, x)\rangle = \left|c_{\lambda_{yx}}^{0} c_{\lambda_{yx}}^{1} \ldots c_{\lambda_{yx}}^{q-1}\right\rangle$$

$$\left|c_{\lambda_{yx}}^{k}\right\rangle \in \{0,1\}\ \text{ve}\ |f(\lambda, y, x)\rangle \in [0, 2^q\text{-}1]$$

$$|yx\rangle = |y^0 y^1 \ldots y^{n-1} x^0 x^1 \ldots x^{m-1}\rangle,\ y^i, x^k \in \{0,1\}$$

$$|\lambda\rangle = |\lambda^0\lambda^1 \dots \lambda^{b-1}\rangle,\ \lambda^i \in \{0,1\}$$

Burada $|yx\rangle$; birinci *n*-kübite $|y^0y^1 \dots y^{n-1}\rangle$ dikey pozisyonu, ikinci *m*-kübite $|x^0x^1 \dots x^{m-1}\rangle$ yatay pozisyonu kodlamaktadır.

Bu modelde renk aralığı [0-255] ve kanal sayısı 4 olan *2x2* boyutlarında görüntüye ait kuantum görüntü temsil örneği Şekil 2.6.'da gösterilmiştir.

C_0(R): 11111001 C_1(G): 00001011 C_2(B): 00011010 C_3(A): 11111111 *00*	C_0(R): 00001001 C_1(G): 11101011 C_2(B): 00001010 C_3(A): 11111111 *01*
C_0(R): 00000001 C_1(G): 00001011 C_2(B): 11111010 C_3(A): 11111111 *10*	C_0(R): 11111001 C_1(G): 11010101 C_2(B): 00001010 C_3(A): 11111111 *11*

Şekil 2.6. *2x2* boyutunda örnek bir RGBα görüntü örneği (Şahin ve Yılmaz ,2018a)

3. Üç Boyutlu Çok Dalga Boylu Kuantum Görüntü Modeli

Şahin ve Yılmaz (2018a QRMW) tarafından geliştirilen çok dalga boylu kuantum görüntü modeli kullanılarak üç boyutlu çok dalga boylu kuantum görüntü temsil modeli (3D-QRMW) aşağıdaki şekilde ifade edilir. 3D-QRMW modelinde dalga boyu kanal sayısı *cn*, her bir kanaldaki renk değerlerinin maksimum 2^q olduğu üç boyutlu bir kuantum görüntü düşünülürse, modelde $2^2x2^nx2^n$ ölçülerindeki görüntüde; renk değerleri için *q*-kübit ve pozisyon bilgisi için (*2n+2*)-kübite, *cn* dalga boyu için ihtiyaç duyulan kübit *b*-kübit (b=ceil($\log_2$cn)) şeklinde olacaktır. 2^b kanallı, $2^2x2^nx2^n$ şeklinde üç boyutlu çok dalga boylu kuantum kuantum görüntü temsili (3D-QRMW) aşağıdaki gibi formüle edilebilir.

$$|I\rangle = \frac{1}{\sqrt{2^{b+2n+2}}} \sum_{\lambda=0}^{2^b-1} \sum_{z=0}^{2^2-1} \sum_{y=0}^{2^n-1} \sum_{x=0}^{2^n-1} |f(\lambda,z,y,x)\rangle \otimes |\lambda\rangle \otimes |zyx\rangle$$

$$= \frac{1}{\sqrt{2^{b+2n+2}}} \sum_{\lambda=0}^{2^b-1} \sum_{z=0}^{2^2-1} \sum_{y=0}^{2^n-1} \sum_{x=0}^{2^n-1} \left|c^0_{\lambda_{yx}} c^1_{\lambda_{yx}} \dots c^{q-1}_{\lambda_{yx}}\right\rangle \otimes |\lambda^0\lambda^1 \dots \lambda^{b-1}\rangle \qquad (3.1)$$

$$\otimes |z^0 \dots z^{2-1} y^0 y^1 \dots y^{n-1} x^0 x^1 \dots x^{n-1}\rangle$$

$$\left|c^k_{\lambda_{zyx}}\right\rangle \in \{0,1\}\ , |f(\lambda,z,y,x)\rangle \in [0,2q\text{-}1]\ , \lambda^i \in \{0,1\},\ z^p, y^i, x^k \in \{0,1\},$$

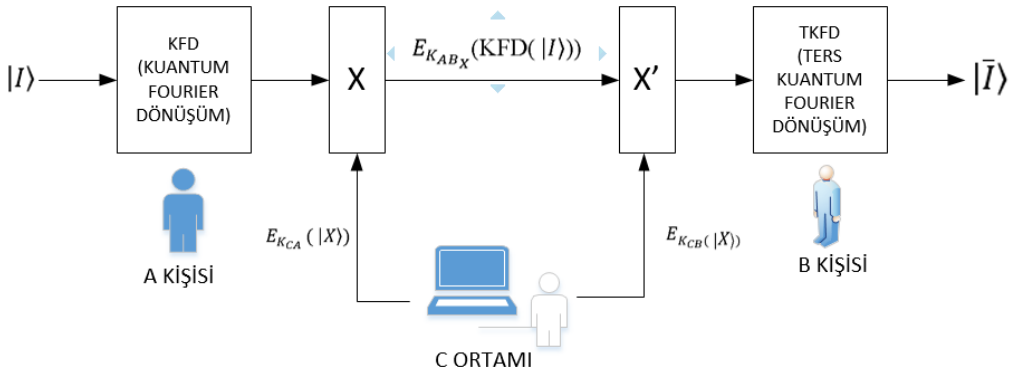
zyx üç boyutlu görüntünün pozisyonunu**,**λ; zyx pikseliyle ilişkili dalga boyunu gösterir. Bu temsilde $|f(\lambda,z,y,x)\rangle$ durumu ise zyx pikselinin ilgili λ dalga boyununun renk değerini göstermektedir. $|zyx\rangle$; birinci *n*-kübite $|z^0 \dots z^{2-1}\rangle$ üçüncü boyut pozisyonunu, $|y^0y^1 \dots y^{n-1}\rangle$ dikey pozisyonu, ikinci *n*-kübite $|x^0x^1 \dots x^{n-1}\rangle$ yatay pozisyonu kodlamaktadır.

4. Üç Boyutlu Çok Dalga Boyutlu Kuantum Görüntü Modelinde Güvenli Görüntü İletimi

Aşağıdaki Şekil 4.1. de önerilen yaklaşımın akış diyagramı çizilmiştir. Diyagrama göre A kişisi B kişisine C ortamını (kör bulut ortamı) kullanarak güvenli bir şekilde üç boyutlu çok dalga boylu kuantum

ISSN 2422-8702 (Online), **DOI:** 10.7176/JSTR/5-5-12
Vol.5, No.5, 2019

görüntüleri (3D-QRMW) iletmek istiyor. Fakat iletilecek veri bir dizi güvenlik önlemi alındıktan sonra C ortamının anlamayacağı hale getiriliyor. Aşağıda gösterilen işlemler sayesinde görüntü çok üst düzey güvenlik önlemi alınarak iletilmiş olacaktır.



Şekil 4.1. 3D-QMWR Kuantum Görüntünün KFD ile Kör Bulut Ortamına Aktırılmasını Gösteren Akış Diyagramı

Bu yönteme göre C ortamından B kişisine aktarılacak görüntünün doğrulanması için A kişisi ile B kişisi arasında C ortamı haricinde bir kuantum iletişim kanalı olmalı ve böylelikle B kişisi A kişisinden gelen görüntülerin doğruluğuna emin olmalıdır. Böylece B kişisi $|I\rangle$ görüntüsünü C ortamından alabilir ve doğrulayabilir.

4.1. Sürecin Başlatılması

Şahin ve Yılmaz (2018b) tarafından NEQR görüntülerinin iletilmesi için geliştirilen algoritmadaki anahtar uzunluğu K| = 16N çıkarılarak aynı yöntem izlenirse, 3D-QRMW modelinde üç boyutlu çok kanallı kuantum görüntüler aşağıdaki şekilde güvenli olarak iletilebilir.

a. |I⟩ kuantum verisinin iletilebilmesi için A kişisi ile B kişisi arasında gizli kuantum anahtar dağılım protokolü hazırlanır ve bu durum K_{AB} ifadesiyle temsil edilir. A kişisi ile C ortamı arasında gizli kuantum anahtar dağılım protokolü hazırlanır ve bu durum K_{AC} ifadesiyle temsil edilir. B kişisi ile C ortamı arasında gizli kuantum anahtar dağılım protokolü hazırlanır ve bu durum K_{CB} ifadesiyle temsil edilir. Bu gizli anahtarlar gelebilecek saldıralara karşı güvenliği artırmak için kullanılmaktadır. Şifreleme algoritması için 4.5 ve 4.6 denklemleri kullanılacaktır. Tüm bu kullanılan gizli anahtarlar |K| = 16N uzunluğunda olacaktır.
K_{AB}, K_{CA}, K_{CB} gizli anahtarları sadece bir defa oluşturulacaktır. Sonrasında herbir gizli anahtar 16 bitlik parçalara ayrılabilecektir. Gizli anahtarların her bir parçası, C ortamı (kör bulut ortamı) tarafından belirlenen permütasyona göre KFD çıktısının her bir kübitine uygulanacaktır. Her farklı aşamada farklı birer K_{AB}, K_{CA}, K_{CB} gizli anahtarları üretilecektir.

b. Bu adımda A kişisi 3D-QRMW modeli kullanarak denk. 3.1.'de gösterildiği gibi kuantum görüntüleri ifade eder.

c. C ortamı (kör bulut ortamı) {1,2,3….N} aralığında bir permütasyon (P) durumları oluşturur.

$$P=\begin{bmatrix} 1 & 2 & \cdots & N \\ P(1) & P(2) & \cdots & P(N) \end{bmatrix}$$

P(i) 'nin ikili (binary) gösterimi aşağıdaki gibidir:

$$P_{binary}(i) = P^0(i)P^1(i) \dots P^{n-1}(i)$$

$$P^j(i) \in \{0,1\}$$

Yukarıdaki denklemde ifade edilen n değeri; $n = log_2(P(i))$ şeklindedir . C ortamı(kör bulut ortamı) temel kuantum hesaplamalar ile $P_{binary}(i)$ yi kullanarak; $|P(i)\rangle$ kuantum durumunu hazırlar. Sonrasında kör bulut ortamı aşağıda belirtilen işlemi yaparak $|P\rangle$ durumunu hazırlar.

$$|P\rangle = \otimes_{i=0}^{N} |P(i)\rangle \qquad (4.2)$$

C ortamı A ve B kişisi ile bu şifrelenmiş kuantum permütasyon durumlarını aşağıdaki gibi oluşturur.

$$|P_A\rangle = E_{K_{CA}}(|P\rangle) \tag{4.3}$$

$$|P_B\rangle = E_{K_{CB}}(|P\rangle) \tag{4.4}$$

E_K ilk olarak Kim ve ark.(2015) tarafından tek kullanımlık (one-time pad) şifrelemede kullanılmıştır. Ayrıca Yılmaz (2017) tarafından da sahte saldırılara karşı protokol güvenliğini artırmada kullanılmıştır. Bu şifreleme algoritmasının güvenliğini daha da artırmak için, Zhang ve ark.(2016) tarafından yeniden düzenlenerek aşağıdaki form kazandırılmıştır.

$$E_K(|I\rangle) = \bigotimes_{i=0}^{N-1} \sigma_x^{K_{16i}} \sigma_z^{K_{16i+1}} T \sigma_x^{K_{16i+2}} \sigma_z^{K_{16i+3}} T \sigma_x^{K_{16i+4}} \sigma_z^{K_{16i+5}} T \sigma_x^{K_{16i+6}} \sigma_z^{K_{16i+7}} \dots T \sigma_x^{K_{16i+14}} \sigma_z^{K_{16i+15}} |I_i\rangle \tag{4.5}$$

$$T = \frac{i}{\sqrt{3}}(\sigma_x - \sigma_y + \sigma_z) \tag{4.6}$$

Burada T değerinin kullanılmasından dolayı şifrelenmiş mesajın taklit edilmesi zorlaşacaktır. Yukardaki denklemde anahtar uzunluğu |K|=16N olarak kullanılmıştır.

c. C ortamı kuantum kanal vasıtasıyla şifrelenmiş $|P_A\rangle$ 'yı A kişisine gönderir. A kişisi $|P_A\rangle$ şifresini çözer ve P yi elde etmek için ölçüm yapar.

d. A kişisi KFD (Kuantum Fourier Dönüşüm)'yi üç boyutlu-QRMW kuantum görüntüye uygular ve aşağıdaki ifadeyi elde eder.

$$\begin{aligned} &KFD(|I\rangle) \\ &= \frac{1}{\sqrt{2^{b+2n+2}}} \sum_{\lambda=0}^{2^b-1} \sum_{Z=0}^{2^2-1} \sum_{Y=0}^{2^n-1} \sum_{X=0}^{2^n-1} (KFD(|c_{ZYX}^0 \dots c_{ZYX}^{q-1} Z_{ZYX}^0 \dots Z_{ZYX}^{n-1} Y_{ZYX}^0 \dots Y_{ZYX}^{n-1} X_{ZYX}^0 \dots X_{ZYX}^{n-1}\rangle) \\ &= \frac{1}{\sqrt{2^{b+2n+2}}} \frac{1}{\sqrt{2^N}} \sum_{\lambda=0}^{2^b-1} \sum_{Z=0}^{2^2-1} \sum_{Y=0}^{2^n-1} \sum_{X=0}^{2^n-1} \left(|0\rangle + e^{2\pi 0.x_{ZYX}^{n-1}} |1\rangle\right) \otimes \dots \\ &\quad \otimes \left(|0\rangle + e^{2\pi 0.x_{ZYX}^{n-2} x_{ZYX}^{n-1}} |1\rangle\right) \otimes \dots \otimes \left(|0\rangle + e^{2\pi 0.c_{ZYX}^0 c_{ZYX}^1 \dots x_{ZYX}^{n-1}} |1\rangle\right) \end{aligned} \tag{4.7}$$

N=q+2n 'dir. Bu şekilde işlemlere devam edilirse:

$$\bigotimes_{i=0}^{N-1} |I_i\rangle = \frac{1}{\sqrt{2^{b+2n+2}}} \sum_{\lambda=0}^{2^b-1} \sum_{Z=0}^{2^2-1} \sum_{Y=0}^{2^n-1} \sum_{X=0}^{2^n-1} \bigotimes_{i=0}^{q-1} |C_{ZYX}^i\rangle \bigotimes_{j=0}^{n-1} |z_Z^j\rangle \bigotimes_{j=0}^{n-1} |y_Y^j\rangle \bigotimes_{j=0}^{n-1} |x_X^j\rangle$$

$$KFD(|I\rangle) = \frac{1}{\sqrt{2^N}} \bigotimes_{i=0}^{N-1} KFD(|I_i\rangle)$$

sonucu elde edilir.

4.2. İmzalama Sürecinin Başlatılması

a. A kişisi C ortamı tarafından oluşturulan permütasyonu kullanarak KFD($|I_i\rangle$) tekrar aşağıdaki gibi düzenler.

$$|A(K)\rangle = SWAP(P(i))(KFD(|I_i\rangle)) \qquad i = 0\dots\text{N-1} \tag{4.8}$$

b. A kişisi 4.8 deki tüm kübitleri K_{AB} ile şifreler ve aşağıdaki $|A(S)\rangle$'yi elde eder.

$$|A(S)\rangle = E_{K_{AB_{P_A(i)}}}(|A(K)\rangle) \qquad i = 0\dots\text{N-1} \tag{4.9}$$

c. A kişisi kuantum kanal kullanarak $|A(S)\rangle$ 'yi B kişisine gönderir. A kişisi KFD($|I_i\rangle$) 'yi K_{AB} ile şifreleyerek AC($|S\rangle$) elde eder ve C ortamına gönderir.

$$|AC(S)\rangle = E_{K_{AB_{P_A(i)}}}(KFD(|I_i\rangle)) \quad (4.10)$$

d. C ortamı $|AC(S)\rangle$ 'yi K_{CB} ile şifreleyerek CB($|S\rangle$) elde eder ve B kişisine kuantum kanal ile gönderir.

$$|CB(S)\rangle = E_{K_{CB}}(|AC(S)\rangle) \quad (4.11)$$

4.3. İletilen Verilerin Doğrulanması

a. B kişisi K_{BC} gizli anahtarıyla $|CB(S)\rangle$ 'yi çözer ve $|AC(S)\rangle$ 'yi elde eder. Sonra B kişisi K_{AB} gizli anahtarıyla $|AC(S)\rangle$ 'yi çözer ve $KFD(|I_i\rangle)$'yi elde eder. B kişisi bu durumua ters kuantum fourier uygulayarak (TKFD), $|I_i\rangle$ durumunu elde ettikten sonra ölçüm yaparak tıbbi görüntüye ulaşacaktır.

b. B kişisi K_{AB} gizli anahtarı ile $|A(S)\rangle$ 'yi çözer ve $|A(K)\rangle$'yı elde eder.

c. B kişisi C ortamında uygun permütasyon durumu ister. C ortamı B kişisine $|P_B\rangle$ 'yi kuantum kanal yoluyla iletir. B kişisi $|P_B\rangle$ şifresini çözer ve ölçüm yaptığında P durumunu elde eder. B kişisi C ortamından aldığı permütasyon sonucunu $|A(K)\rangle$ ile $SWAP$ kapısında işleme sokar ve $KFD(|I_i\rangle)$'yi elde eder.

$$KFD(|I_i\rangle) = SWAP\big(P(i)\big)\,(|A(K)\rangle)$$

i=0…N-1 (4.12)

d. B kişisi TKFD (Ters Kuantum Fourier Dönüşüm) işlemi yaparak, $|I_i\rangle$ durumunu elde ettikten sonra ölçüm yaparak kuantum görüntüye ulaşacaktır. B kişisi şimdi C ortamından ve A kişisinden aldığı görüntüleri kıyaslayacaktır. Eğer iki durum birbirine eşitse problem yoktur. Fakat iki durum birbirinden farklı ise B kişisi $E_{K_{CB}}$ gizli anahtarı ile veriyi şifreler ve $|CB(S)\rangle$ durumunu elde eder ve C ortamına gönderir.

$$|BC(S)\rangle = E_{K_{BC}}(|I_i\rangle) \quad (4.13)$$

e. C ortamı B kişisinden gelen $|BC(S)\rangle$ durumunu K_{BC} gizli anahtarı ile çözer ve elde ettiği sonuca ölçüm yaptığında bir sonuç elde eder.

f. C ortamı A kişisinden tekrar aynı veriyi göndermesini ister. A kişisi veriyi $E_{K_{AC}}$ ile şifreyerek $|AC(S)\rangle$ durumunu elde eder ve C ortamına gönderir.

$$|AC(S)\rangle = E_{K_{AC}}(|I_i\rangle) \quad (4.14)$$

g. C ortamı A kişisinden gelen $|AC(S)\rangle'yi$ K_{AC} gizli anahtarı ile çözer ve elde ettiği sonuca ölçüm yaptığında bir sonuç elde eder. C ortamı hem A kişisinden hem de B kişisinden elde ettiği sonuçları kıyaslar. Eğer sonuçlar aynıysa işlem tamamlanır fakat sonuçlar farklı ise tüm işlemler iptal edilir.

5. Güvenlik Analizi

Güvenliği üst düzeye çıkarmak için herhangi bir saldırı olduğu zaman her iki kişiden de imzalama protokollerinin tekrar istenilmesi ve eğer durumu sağlayamıyorsa sürecin iptal edilmesi sonucu sistemin durması büyük önem taşımaktadır. Ayrıca tüm süreçlerde yapılan işlemlerin temel amacı güvenliği sağlamak ve saldırganın işini çok zorlaştırmaktadır. Saldırgan eğer doğru veriyi elde etmek istiyorsa tüm aşamaları tek tek doğrulaması gerekmektedir. Bu da saldırgan açısından oldukça karmaşık bir durum oluşturmaktadır.

5.1. Sistemin Yanıltılmasının İmkansız Olması

İlk olarak saldırının içeriden olduğunu düşünürsek ; B kişisinin yanlış kişi olduğunu ve A kişisiyle imzalama sürecini başlatmak istediğini varsayalım. B kişisi tüm imzalama protokollerini bilse bile, C ortamından dolayı A kişisiyle doğru imzayı oluşturamaz. Yani B kişisi C ortamı olmadan A kişisinin imzasını oluşturamaz. A kişisi ile normal imzalama protokollerini geçip *I* dan *I'* verisini elde etse bile C ortamından herhangi bir veri alamayacağı için tek başına o verinin doğruluğunu ispatlayamayacaktır.
İkinci olarak herhangi bir saldırgan A kişisinin imzasını taklit etmeyi denerse herhangi bir şey yapamayacaktır. Çünkü KFD(Kuantum Fourier Transform)'dan sonra elde edilen durumlar, A kişisinin doğru imzasını oluşturmasını sağlamak için C ortamının izni ile tekrar düzenlecektir. Eğer saldırgan bir

şekilde doğru izni alsa bile C ortamı her defasında imzalama sürecini değiştirecektir. C ortamı her zaman uygulanan protokollerin bir parçası olmalıdır. Saldırı sonucu KFD ile elde edilen durumlar değişse bile, kişinin her iki ortamdan aldığı verileri kıyaslaması ve eğer verilerin birbiri ile eşelşmemesi gibi bir durumla karşılaşması sonucu verileri kabul etmemesi saldırıyı etkisiz kılacaktır.

5.2. Sistemin Durumları Reddetmesinin İmkânsız Olması

Tüm protokollerin C ortamı tarafından yapılmasından dolayı A kişisi ve B kişisi imzalama sürecini reddedemezler. C ortamı protokoldeki bazı iletişim adımlarını kontrol etmektedir. Örneğin A kişisi C ortamına farklı bir veri gönderirse, C ortamı A kişisinden aldığı veriyi ve B kişisinden aldığı veriyi kontol ederek kıyaslar. Bu şekilde C ortamı imzalama protokolünün geçerli olup olmadığına karar verebilir.

6. Sonuç

Verilerin kuantumsal olarak bulut ortamına güvenli iletilmesi ve tekrar güvenli şekilde elde edilmesi oldukça büyük önem taşımaktadır. Literatür incelendiği zaman QRMW yapısı kullanılarak buna benzer herhangi bir çalışmanın yapılmadığı görülmektedir. Bu şekilde üç boyutlu görüntülerin kauntumsal forma dönüştürülmesine dayalı bazı çalışmalar mevcuttur.

Ortaya konulan bu çalışma göstermektedir ki kuantum teknolojinin üstün özellikleri kullanırak verilerin en güvenli şekilde iletilmesi ve bu verilere dışardan gelebilecek tehlikelere karşı önlem alınmasına, bu teknoloji çok büyük bir imkan tanımaktadır. Yapılan çalışmada kullanıcıların imzalama prtokolleri kullanarak aralarındaki veriyi şifrelemesi ve ardından sadece kendi içlerinde yaptıkları permütasyon işlemleri ile süreç çok güvenli hale gelmektedir. Ayrıca A kişisi ile B kişisi arasında olan permüstasyon ve imzalama sürecinden C ortamının haberinin olmaması, A kişisi ile C ortamının permüstasyon ve imzalama sürecinden B kişisinin haberinin olmaması ve B kişisi ile C ortamının permüstasyon ve imzalama sürecinden A kişisinin haberinin olmamasından dolayı verilerin aktarılması ve kuantum görüntülerin çok güvenli şekilde iletilmesine olanak sağlamaktadır. Ayrıca tüm bu süreçlere ilave olarak kuantum fourier dönüşüm (KFD) ile de verinin şifrelenmesi güvenliği en üst düzeye çıkarmaktadır.

Dışarıdan gelebilecek hatalı verilere karşı C kişisinin aldığı verileri kıyaslamasıda sürecin sağlıklı ilerlemesinde büyük önem arz etmektedir. C kişisinin kıyaslaması sonucu eğer gelen veriler tutarlı değilse C ortamına tekrar göndermesi ve C ortamının A kişisine aldığı veriyi tekrarlaması ve her iki kişiden aldığı verileri kıyaslaması da yanlış bir veri olup olmadığını ispatlayarak problemin nereden kaynaklandığını da çözmeye imkan tanımaktadır.

Başlangıçta görüntünün 3D-QRMW ile kuantumsal forma dönüştürülmesi ve ardından KFD ile şifrelenmesi zaten büyük ölçüde kuantum görüntünün gizlenmesini sağlamıştır. KFD ile yapılan işlem veriyi anlamsız kübitlere ayırarak bir parçasının bile kendi başına bir anlam ifade etmediğini göstermektedir. Sonrasında imzalama süreçleri ve permütasyon işlemleri ile anlamsız veriler daha da soyut bir hal almış olup, parçaları bir araya getirilse bile uygulanan işlemlerin aynı sıra ile uygulanamaması sonucu verinin hiçbir şekilde elde edilemeyeceğini göstermektedir. Yani problemi çözüp kuantum görüntüye ulaşmak isteyen kişinin, kuantum kanal yoluyla iletişimde olduğu kişi veya ortamla arasındaki tüm protokolleri biliyor olması gerekmektedir.

References

Abdolmalekya M, Naserib M, Batlec J, Faroukd A, Gong. L. ,“Red-green-blue multi-channel quantum representation of digital images”, Int J Light Elec Opt; 128: 121-132,2017.

Le PQ, Dong F, Hirota K. A “flexible representation of quantum images for polynomial preparation, image compression and processing operations” , Quantum Inf Proc ; 10: 63-84, 2011.

Li H., Zhu Q., Zhou R., Song L., Yang X., 2014. Multi-dimensional Color Image Storage and Retrieval for a Normal Arbitrary Quantum Superposition State. Quantum Inf. Process., 13(4): 991-1011.

Sun B, Iliyasu A, Yan F, Dong F, Hirota K. "RGB-multi-channel representation for images on quantum computers", J Adv Comp Intel Intel Inf; 17: 404-417, 2013.

Şahin, E. , Yılmaz. İ, " QRMW: quantum representation of multi wavelength images", Turk J Elec Eng & Comp Sci, 26: 768- 779, 2018a.

Şahin E, Yilmaz İ, "Security of NEQR Quantum Image by Using Quantum Fourier Transform with Blind Trent", International Journal Of Information Security Science, E.Şahin et al., Vol.7, No.1,2018b

Venegas-Andraca SE, Bose S. Storing, "processing and retrieving an image using quantum mechanics". Proc SPIE Conf Quantum Inf Comput 5105: 137-147.

Venegas-Andraca SE, Ball JL. "Processing images in entangled quantum systems", Quantum Inf. Proc., 9: 1-11,2010.

Yang J, Q.Li B, Li R, Mei X, "Quantum 3D thermal imaging at the micro-nanoscale", Royal Society Of Chemistry" Nanoscale,2019,DOI:10.1039/c8nr09096c:2249-2263..

Yuan S, Mao X, Xue Y, Chen L, Xiong Q, "Compare A. Sqr: a simple quantum representation of infrared images", Quantum Inf Proc; 13: 1353-1379, 2014.

W. Zhang, D. Qiu, and X. Zou, "Improvement of a quantum broadcasting multiple blind signature scheme based on quantum teleportation," Quantum Information Processing, vol. 15, no. 6, pp. 2499–2519, 2016. [Online]. Available: https://doi.org/10.1007/s11128-016-1289-9

Zhang Y, Lu K, Gao Y, Wang M. "Neqr: a novel enhanced quantum representation of digital images", Quantum Inf Proc; 12: 2833-2860, 2013a.

Zhang Y, Lu K, Gao Y, Xu K. A "novel quantum representation for log-polar images", Quantum Inf Proc; 12:3 103-3126, 2013b.

Acknowledgement

This work is produced under the master thesis of Ömer Doğan.