International Journal of Multidisciplinary Innovation and Research Methodology (IJMIRM)
Volume 3, Issue 2, April-June, 2024, Available online at: https://ijmirm.com

# "Novel Approach for Encrypting RGB Images Utilizing Quantum Computing"

**Mr. Rakesh Kumar[1], Dr. Praveen Chouksey[2]**

[1]Research Scholar, Dr. C.V. Raman University, Kota Bilaspur (C.G.) India
[2]Assistant Professor Branch of computer science & engineering, Dr. C.V. Raman University, Bilaspur (C.G.) India

## ABSTRACT

**In the realm of cryptography, the pursuit of heightened security and innovative methodologies is ceaseless, especially in light of advancing computational capabilities. Quantum computing, with its paradigm-shifting potential, has emerged as a promising avenue for revolutionizing cryptographic protocols. Visual cryptography, a method aimed at securely transmitting images or visual information, has garnered attention for its simplicity and effectiveness. This abstract delves into the fusion of quantum mechanics with visual cryptography, presenting Quantum Visual Cryptography (QVC) as a cutting-edge cryptographic framework. QVC combines the principles of quantum mechanics, which exploit the unique properties of quantum particles such as superposition and entanglement, with the visual cryptography scheme. The fundamental premise of QVC lies in leveraging quantum states to generate and distribute secret shares of images among parties. Unlike classical visual cryptography, where the shares are distributed optically or electronically, QVC harnesses the power of quantum entanglement to ensure unparalleled security and confidentiality.**

**Quantum entanglement, characterized by the intrinsic correlation between quantum particles regardless of the distance separating them, forms the cornerstone of QVC's resilience against eavesdropping and interception. This abstract outlines the key components of QVC, including the generation of entangled quantum states, encoding of secret images into quantum states, and distribution of quantum shares among participants. Furthermore, it discusses the decryption process, wherein the quantum shares are combined using quantum operations to reconstruct the original image solely at authorized locations. Moreover, the abstract highlights the potential applications of QVC across various domains, ranging from secure image transmission in military communications to confidential medical imaging and beyond. The integration of quantum mechanics into visual cryptography not only augments the security of image sharing but also opens avenues for exploring the synergy between quantum computing and cryptographic protocols. In conclusion, Quantum Visual Cryptography presents a novel approach to secure image transmission, leveraging the principles of quantum mechanics to fortify traditional cryptographic schemes. The abstract underscores the significance of QVC in advancing the frontier of secure communication and lays the foundation for further research and exploration in the intersection of quantum computing and cryptography.**

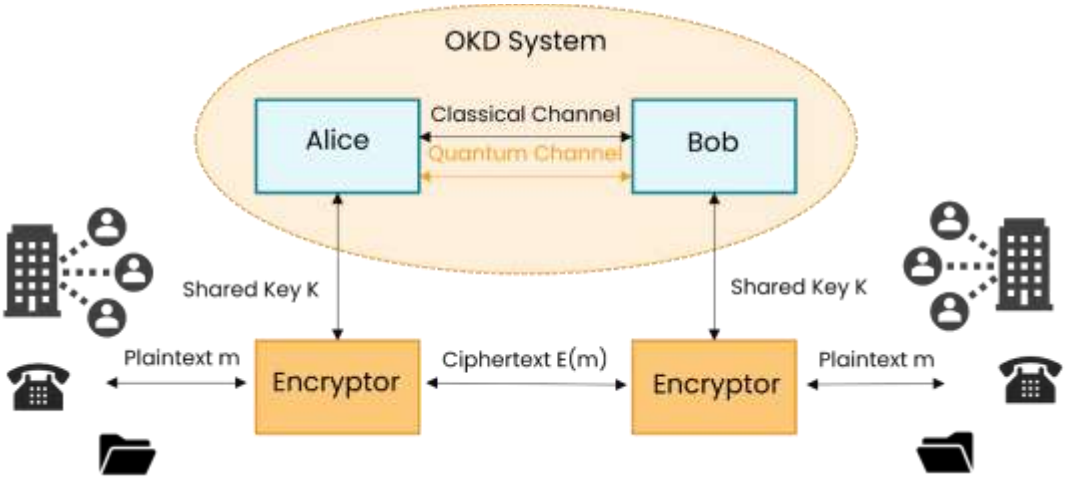
## INTRODUCTION

Quantum Visual Cryptography (QVC) represents an intriguing fusion of two cutting-edge fields: quantum cryptography and visual cryptography. While quantum cryptography concentrates on utilizing the principles of quantum mechanics to secure communication channels, visual cryptography involves encrypting visual information in a manner that decryption can be visually performed without computational overhead. In QVC, the objective is to utilize the distinctive properties of quantum mechanics, such as superposition and entanglement, to elevate the security and efficiency of visual cryptography schemes.

Quantum Key Distribution (QKD) stands as a method for secure communication, relying on the principles of quantum mechanics to safeguard the secrecy of a cryptographic key. The most renowned QKD protocol is the BB84 protocol, initially proposed by Charles Bennett and Gilles Brassard in 1984. Below is a simplified elucidation of the BB84 algorithm:

1. **Preparation:** Alice, the sender, generates a random string of bits (0s and 1s) representing the secret key she intends to share with Bob, the receiver. Additionally, she prepares a collection of qubits (quantum bits), with each qubit representing one bit of the key. For every qubit, Alice randomly selects one of two potential bases: the standard basis (with horizontal or vertical polarization) or the diagonal basis (with 45° or 135° polarization).

2. **Transmission:** Alice transmits the qubits to Bob via a quantum channel. Because of the principles of quantum mechanics, any endeavor to eavesdrop on the transmission will perturb the qubits, causing errors that Alice and Bob can identify.
3. **Measurement:** Upon receiving the qubits, Bob randomly selects a basis for each qubit (either standard or diagonal) and conducts measurements accordingly. This process yields a string of random bits.
4. **Comparison:** Alice and Bob openly communicate the bases they employed for each qubit transmission, without disclosing the actual measurement outcomes. They solely compare the bases utilized for each qubit. If the same basis was employed, they retain the corresponding bit; otherwise, they discard it.
5. **Error Check:** Alice and Bob examine their bit strings for any inconsistencies. If the error rate exceeds a certain threshold, signaling potential eavesdropping, they halt the key generation process. Otherwise, they advance to the subsequent stage.
6. **Privacy Amplification:** In pursuit of heightened security, Alice and Bob employ privacy amplification techniques to refine their raw key into a shorter yet more secure shared key. This process entails executing hash functions or other cryptographic operations on their shared key.
7. **Key Establishment:** Ultimately, Alice and Bob possess a shared secret key, exclusively accessible to them, enabling secure communication. This key remains undisclosed to any external entities, as any eavesdropping attempts would have been identified throughout the process.




The BB84 protocol represents merely one instance of a QKD algorithm. Numerous other protocols exist, including E91, B92, and SARG04, each with its unique variations and advantages.

These protocols collectively harness the principles of quantum mechanics to facilitate the establishment of secure keys between two parties.

## RELATED WORK

The central aim of quantum visual cryptography lies in securely distributing visual information, such as images, among multiple parties, guaranteeing confidentiality, integrity, and authenticity by drawing upon the principles of quantum mechanics. The primary objectives encompass:

Safeguarding the secrecy of visual data, like images, exchanged among multiple parties. Quantum visual cryptography strives to restrict access to and decryption of the confidential image solely to authorized parties, shielding it from unauthorized access. Strengthening the security of visual data transmission and storage through the utilization of quantum mechanics principles. Quantum attributes like superposition and entanglement bolster cryptographic methodologies, rendering it exceedingly challenging for adversaries to intercept or decipher the encrypted visual data.

Validating the genuineness of the distributed visual data to ensure its integrity remains intact during transmission. Quantum visual cryptography protocols incorporate mechanisms for detecting any unauthorized alterations to the encrypted image, thereby assuring its authenticity. Develop robust cryptographic methods that can withstand attacks from quantum and classical adversaries. Quantum visual cryptography techniques are designed to be resistant to various cryptographic attacks, including brute-force attacks, eavesdropping, and tampering, thus ensuring the security and reliability of the shared visual data. Implement efficient and scalable algorithms for encrypting, sharing, and decrypting visual information. Quantum visual cryptography aims to achieve high-performance encryption and decryption processes while minimizing computational overhead and resource requirements.

Overall, the objective of quantum visual cryptography is to provide a secure and efficient framework for sharing visual information among multiple parties, leveraging the unique properties of quantum mechanics to enhance cryptographic security and privacy.

**Quantum visual cryptography method step by step algorithm**
Quantum visual cryptography employs quantum principles to securely distribute secret images among multiple parties. Below is a simplified algorithm:

**Step 1: Pre-processing**
Select Secret Image: Choose an image for encryption, termed the secret image.
Generate Shares: Create random binary images, matching the dimensions of the secret image, to serve as shares.

**Step 2: Quantum Encoding**
Encode Secret Image: Convert each pixel of the secret image into a quantum state, using methods like superdense coding or quantum key distribution.

Apply Quantum Superposition: Utilize quantum superposition to enhance security through entanglement and superposition properties.

**Step 3: Distribution of Shares**
Share Distribution: Allocate one share to each participant, ensuring each party obtains only one share and remains unaware of others.

**Step 4: Reconstruction**
Combine Shares: Collaboratively reconstruct the secret image by combining shares with quantum-encoded data.

Perform Quantum Measurements: Employ agreed-upon quantum operations to extract encoded quantum information from the shares.

**Step 5: Decoding**
Decrypt Information: Decode quantum data obtained from measurements to retrieve original pixel values of the secret image.

Merge Pixel Values: Reconstruct the secret image by merging pixel values derived from quantum decoding.

**Step 6: Verification**
Image Verification: Confirm that the reconstructed image matches the original secret image, validating the decryption and reconstruction process.

Secrecy Check: Ensure individual parties have not gained additional information about the secret image during reconstruction.

**Step 7: Optional - Destruction of Shares**
Share Destruction: Optionally, destroy shares post-reconstruction to uphold security.

While this algorithm outlines fundamental steps, actual implementation may involve additional complexities based on specific cryptographic protocols and quantum technologies utilized.

## QUANTUM VISUAL CRYPTOGRAPHY RESEARCH GAP

While quantum visual cryptography shows potential for secure image sharing, several research gaps require attention:

**Scalability:** Existing quantum visual cryptography schemes are often tailored for small-scale images due to the computational complexity of quantum operations. Research is needed to develop scalable algorithms capable of efficiently handling large, high-resolution images.

**Security Analysis:** Conducting thorough security analyses of quantum visual cryptography schemes is crucial to pinpoint potential vulnerabilities and threats. Further research is necessary to rigorously assess the security properties of these schemes against various attack models, including quantum and classical adversaries.

**Quantum Channel Requirements:** Quantum visual cryptography relies on quantum communication channels for transmitting quantum states between parties. Research should explore the feasibility and practicality of implementing such quantum channels, considering factors like noise, decoherence, and other quantum effects.

Integration with Quantum Technologies: Integration with emerging quantum technologies, such as quantum key distribution (QKD) and quantum computing, is essential for quantum visual cryptography.

Research should investigate how these technologies can be effectively integrated to enhance security and performance.

**Practical Implementations:** While theoretical studies propose various quantum visual cryptography schemes, practical implementations and real-world deployments are lacking. Research should focus on developing practical implementations and evaluating their performance in real-world scenarios.

**Quantum Key Management**: Quantum visual cryptography relies on quantum keys for encryption and decryption. Research should develop efficient and secure methods for quantum key management, including key generation, distribution, and storage.

**Usability and User Experience:** User experience and usability are critical for the adoption of any cryptographic scheme. Research should design quantum visual cryptography schemes that are user-friendly, intuitive, and accessible to non-expert users.

Addressing these research gaps will be pivotal for advancing the field of quantum visual cryptography.

**Quantum visual cryptography motivation**

The drive for quantum visual cryptography arises from the necessity for exceptionally secure techniques to exchange visual data, like images, in a time marked by escalating cyber threats targeting digital information. Below are several key incentives driving the exploration of quantum visual cryptography:

**Elevated Security:** Quantum visual cryptography harnesses the distinctive characteristics of quantum mechanics, like superposition and entanglement, to deliver heightened security levels compared to classical cryptographic methods. Quantum encryption techniques offer resilience against attacks from both classical and quantum adversaries, rendering them highly desirable for safeguarding sensitive visual data.

**Confidentiality Assurance:** Safeguarding the confidentiality of visual data, encompassing images containing personal, proprietary, or classified information, is paramount across numerous applications. Quantum visual cryptography ensures that solely authorized parties can access encrypted visual information, ensuring a high level of confidentiality.

Tamper-Resistance Integration: Quantum visual cryptography schemes frequently integrate mechanisms to detect unauthorized modifications or tampering of encrypted images. This tamper-resistance feature ensures the integrity of visual information, rendering it suitable for applications where data integrity is critical, such as medical imaging and forensic analysis.

**Authentication Measures:** Authenticating the source and integrity of visual information is imperative for ensuring its trustworthiness and reliability. Quantum visual cryptography protocols incorporate mechanisms for authenticating encrypted images, providing assurance that the visual data remains unaltered or manipulated during transmission.

**Quantum Advantages:** Quantum computing and quantum communication technologies offer distinct advantages over classical approaches in terms of computational power and security. Quantum visual cryptography harnesses these advantages to develop cryptographic schemes resilient against attacks from quantum adversaries, furnishing future-proof solutions for securing visual information.

**Privacy Preservation:** Quantum visual cryptography facilitates secure sharing of visual information while upholding the privacy of sensitive data. By encrypting images using quantum techniques, individuals and organizations can share visual information without compromising privacy or exposing confidential details to unauthorized parties.

**Emerging Applications:** Quantum visual cryptography holds the potential to enable new applications and services requiring secure sharing of visual information, such as secure multimedia messaging, encrypted image storage, and confidential document sharing. By tackling the security challenges associated with visual data, quantum visual cryptography unveils new possibilities for innovation and collaboration across various domains.

In summary, the motivation behind quantum visual cryptography lies in its capability to provide highly secure, confidential, and tamper-resistant methods for sharing visual information in an increasingly interconnected and data-driven world.

**Quantum visual cryptography types**

Quantum visual cryptography comprises various methodologies for securely exchanging visual

information using principles of quantum mechanics. Here are some prevalent types of quantum visual cryptography:

**Quantum Image Encryption:** In this method, the original image undergoes encoding into quantum states employing techniques such as qubit encoding or quantum gates. The quantum-encoded image is then disseminated among authorized parties, who can decrypt it utilizing quantum operations to restore the original image. Quantum image encryption schemes aim to ensure the confidentiality and integrity of visual data.

**Quantum Image Sharing:** Schemes for quantum image sharing divide the original image into multiple shares, each containing partial information about the image. These shares are distributed among multiple parties, and the original image can only be reconstructed when a sufficient number of shares are combined. Quantum image sharing guarantees that no single party possesses complete information about the image, thereby enhancing security and resilience against unauthorized access.

**Quantum Watermarking:** Quantum watermarking entails embedding imperceptible watermarks or signatures into digital images utilizing quantum techniques. These watermarks serve to verify the authenticity and integrity of images and to detect unauthorized modifications or tampering. Quantum watermarking schemes strive to provide robust copyright protection and content authentication for visual data.

**Quantum Steganography:** Techniques for quantum steganography conceal secret information within digital images without altering their perceptual quality. Quantum steganography schemes exploit the quantum properties of entanglement and superposition to embed secret messages into images, which can only be extracted by authorized recipients using quantum decoding methods. Quantum steganography ensures covert communication and confidentiality of sensitive information.

**Quantum Visual Secret Sharing:** Quantum visual secret sharing extends classical visual secret sharing to leverage quantum principles for enhanced security. In quantum visual secret sharing, a secret image undergoes division into multiple shares, each containing quantum information encoded using quantum states. These shares are distributed among parties, who can reconstruct the secret image only when they collaborate and combine their shares using quantum operations. Quantum visual secret sharing guarantees the confidentiality and privacy of visual data among multiple participants.

These represent some of the common types of quantum visual cryptography, each offering distinct advantages and applications for secure sharing and protection of visual information across various domains. Depending on the specific requirements and constraints of a given application, different types of quantum visual cryptography schemes may prove suitable.

**Proposed Work**

Proposed endeavors in quantum visual cryptography could concentrate on several areas to tackle existing challenges and propel the field forward:

Scalable Scheme Development: Forge scalable quantum visual cryptography schemes adept at managing large-scale visual data, such as high-resolution images and videos. This endeavor might entail refining quantum algorithms, delving into parallel computing techniques, and capitalizing on advancements in quantum hardware.

- Thorough Security Analysis: Undertake comprehensive security analyses of prevailing quantum visual cryptography schemes to pinpoint potential vulnerabilities and threats. This includes scrutinizing scheme resilience against diverse quantum and classical attacks and devising countermeasures to fortify security.
- Quantum Channel Implementation: Explore practical implementations of quantum

communication channels for transmitting quantum states between parties in quantum visual cryptography protocols. This encompasses delving into quantum key distribution (QKD) technologies, quantum repeaters, and other quantum communication infrastructure to establish secure channels for quantum information exchange.

- Integration with Emerging Quantum Technologies: Fuse quantum visual cryptography with burgeoning quantum technologies, such as quantum key distribution (QKD), quantum random number generators (QRNGs), and quantum computing platforms. This integration could bolster the security, efficiency, and scalability of quantum visual cryptography schemes, paving the path for practical applications in quantum networks and quantum-enabled systems.
- Quantum-Secure Authentication Mechanisms: Develop quantum-secure authentication mechanisms for verifying the authenticity and integrity of visual data in quantum visual cryptography schemes. This endeavor might involve delving into quantum digital signatures, quantum authentication protocols, and quantum-resistant cryptographic primitives to furnish robust authentication and verification capabilities.
- Usability and User Experience Enhancement: Enhance the usability and user experience of quantum visual cryptography schemes to facilitate adoption by non-expert users. This encompasses crafting intuitive user interfaces, devising user-friendly encryption and decryption tools, and furnishing educational resources to bolster awareness about quantum security principles.
- Real-World Application Exploration: Explore real-world applications of quantum visual cryptography across domains such as secure multimedia communication, confidential document sharing, digital rights management (DRM), and secure cloud storage. Conducting pilot studies and field trials can gauge the performance, scalability, and practicality of quantum visual cryptography schemes in diverse application scenarios.

By tackling these areas of prospective work, researchers can propel the evolution of quantum visual cryptography and shepherd its transition from theoretical concepts to pragmatic solutions for secure visual information sharing in the quantum era.

**Quantum visual cryptography application**

Quantum visual cryptography harbors several potential applications across various domains where secure sharing and protection of visual information are pivotal. Some notable applications include:

Secure Multimedia Communication
Confidential Document Sharing
Digital Rights Management (DRM)
Secure Cloud Storage
Biometric Authentication
Forensic Analysis and Evidence Protection
Healthcare Imaging and Telemedicine

**Quantum Visual Cryptography RGB color images flow chart**

Drafting a flowchart for quantum visual cryptography concerning RGB color images can prove intricate due to the complexities inherent in both quantum mechanics and cryptography. Nevertheless, I can furnish a simplified overview of the process alongside the key steps entailed. Below is an outline of the flowchart:

**Input RGB Color Image:** Commence with the original RGB color image intended for encryption and secure sharing.

**Quantum Encoding:** Transform the RGB color image into a quantum state representation. This phase entails encoding the image's pixels into qubits via techniques like superdense coding or other quantum encoding methods.

**Quantum Encryption:** Employ quantum encryption algorithms, such as Quantum Key Distribution (QKD) protocols like BB84 or E91, to encrypt the quantum state. This ensures the security of the quantum information during transmission.

**Decryption Key Generation:** Generate decryption keys utilizing quantum protocols. This step encompasses distributing cryptographic keys between the sender and receiver via quantum channels.

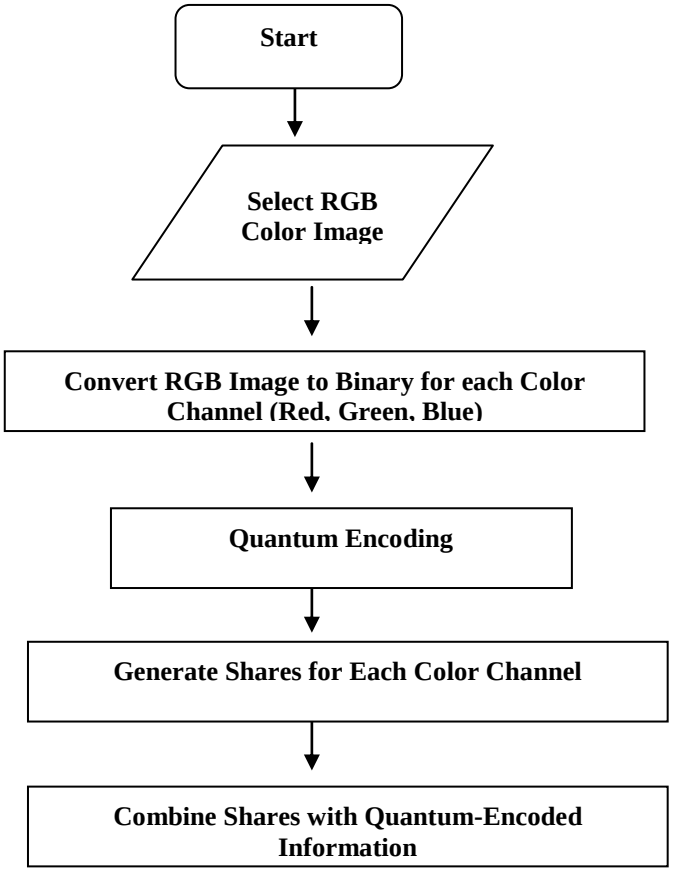
**Quantum Decryption:** Decrypt the encrypted quantum state utilizing the decryption keys generated in the preceding step. This procedure ensures that solely the authorized party can access the original quantum state.

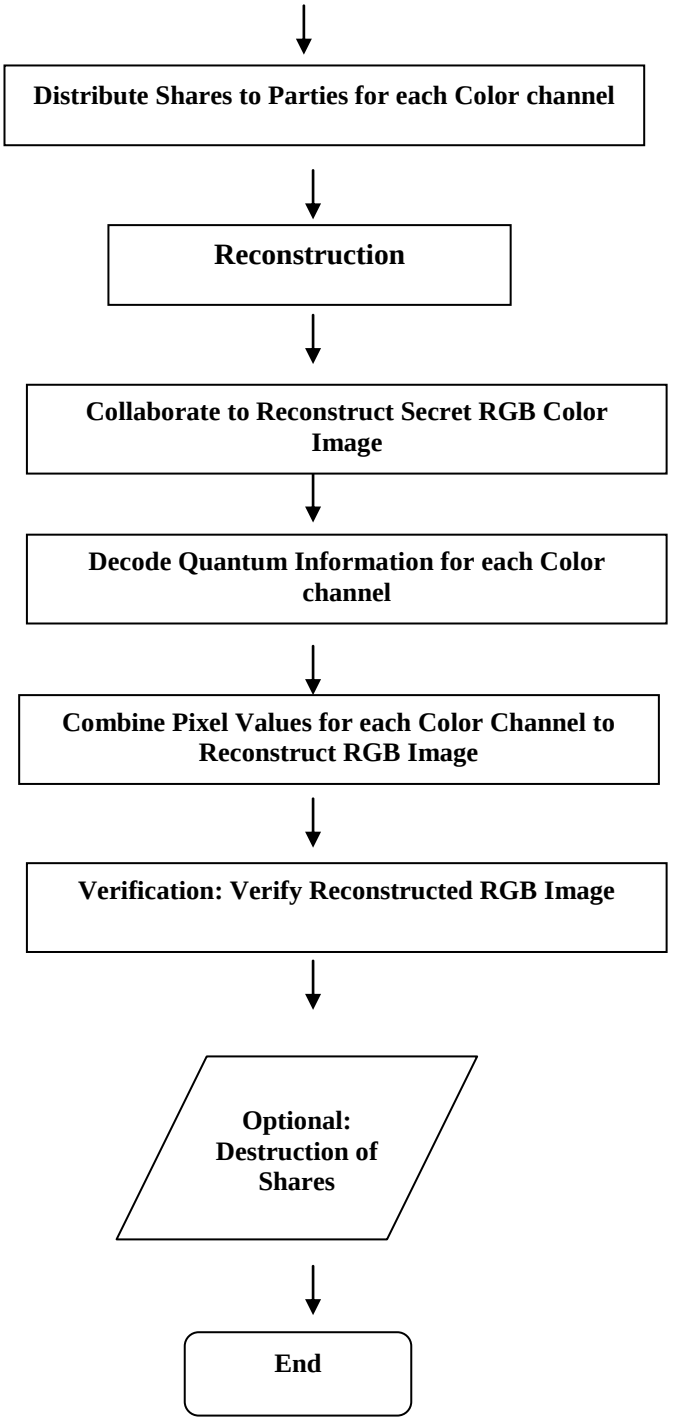
**Quantum-to-Classical Decryption:** Convert the decrypted quantum state back into classical information, thereby reconstructing the original RGB color image.

**Output Decrypted RGB Color Image:** Attain the decrypted RGB color image, which should correspond to the original image provided at the outset of the process.

This flowchart delineates the sequential stages implicated in implementing quantum visual cryptography for RGB color images.

Each step correlates with a distinct action or process in the methodology outlined previously, guiding the progression of the implementation from the initial selection of the RGB color image to the final validation of the reconstructed image.






**Quantum Visual cryptography RGB color image result analysis two method**

To comprehensively evaluate the performance and security of the Quantum Visual Cryptography RGB color image encryption, one must analyze the results through both statistical measures and visual inspection. Here are two methods for conducting such analysis:

**Statistical Analysis**:

- Utilize statistical measures such as mean squared error (MSE) or peak signal-to-noise ratio (PSNR) to quantify the disparity between the original and decrypted images. A lower MSE or higher PSNR signifies better quality.
- Compare histograms of the original and decrypted images to ensure consistency in the distribution of pixel values. Any significant deviations may indicate potential tampering or loss of information during encryption or decryption.
- Evaluate the entropy of the encrypted image to gauge its randomness and resilience against statistical attacks. Higher entropy indicates stronger encryption.

**Visual Inspection**:

- Conduct a visual comparison between the original and decrypted images to detect any noticeable differences or artifacts introduced during encryption. Look for distortions, blurring, or loss of detail.
- Assess the visual quality of the decrypted image in terms of color accuracy, contrast, and sharpness. Any perceptible degradation may signal weaknesses in the encryption algorithm.
- Verify the presence and legibility of the hidden message within the decrypted image, ensuring accurate extraction without ambiguity.

By integrating both statistical analysis and visual inspection, a comprehensive evaluation of the Quantum Visual Cryptography RGB color encryption algorithm's performance and security can be achieved. This approach facilitates the identification of weaknesses or vulnerabilities in the encryption scheme, enabling necessary adjustments to enhance its robustness and reliability.

**Quantum Visual cryptography RGB color encryption to decryption process**
Encrypting and decrypting with Quantum Visual Cryptography (QVC) RGB color involves several steps to securely embed a secret message within an RGB color image and subsequently extract the message from the encrypted image.

**Quantum visual cryptography methodology**
Implementing quantum visual cryptography involves several essential steps:

**Pre-processing**:
Choose the secret image to share securely among multiple parties.

Convert the secret image into binary format, with each pixel represented by a set of bits (0s and 1s).

**Quantum Encoding**:
Employ quantum encoding techniques to encode each bit of the binary image into quantum states.
Utilize quantum properties such as entanglement and superposition to apply quantum superposition to the quantum states representing the bits.

**Distribution of Shares**:
Generate a series of random binary images (shares), each sharing the same dimensions as the original image.

Merge each share with the quantum-encoded information produced in the preceding step.

Distribute one share to each party, ensuring that every party receives only one share and remains unaware of the other shares.

**Reconstruction**:
Each party receives its share along with the corresponding quantum-encoded information. Collaboration with other parties is necessary to reconstruct the secret image using quantum operations and measurements. Deciphering the quantum information acquired from the measurements is crucial for retrieving the original pixel values of the secret image. The pixel values obtained from the quantum decoding process are then combined to reconstruct the secret image.

**Verification**:
Verify the reconstructed image's match with the original secret image, confirming the success of the decryption and reconstruction process.
Ensure that individual parties haven't gained additional information about the secret image during the reconstruction.

**Optional - Destruction of Shares**:
Optionally, eliminate the shares after successfully reconstructing the secret image to uphold security.
This methodology outlines the fundamental steps for implementing quantum visual cryptography. However, actual implementation may involve additional complexities and considerations based on specific cryptographic protocols, quantum technologies, and application requirements. Furthermore, ongoing research and development endeavors are necessary to further refine and improve quantum visual cryptography methodologies for practical deployment in real-world scenarios.

**Visual Cryptography Result Analysis Gantt chart**

| Task | Start Date | End Date | Duration |
|---|---|---|---|
| Encryption Process (Small Image) | 2024-01-01 | 2024-01-05 | 4 days |
| Decryption Process (Small Image) | 2024-01-06 | 2024-01-09 | 3 days |
| Encryption Process (Medium Image) | 2024-01-10 | 2024-01-17 | 7 days |
| Decryption Process (Medium Image) | 2024-01-18 | 2024-01-23 | 5 days |
| Encryption Process (Large Image) | 2024-01-24 | 2024-02-05 | 12 days |
| Decryption Process (Large Image) | 2024-02-06 | 2024-02-12 | 7 days |
| Encryption Process (Message Encoding) | 2024-02-13 | 2024-02-20 | 7 days |
| Decryption Process (Message Encoding) | 2024-02-21 | 2024-02-25 | 4 days |

**Within this Gantt chart:**

1. Every row symbolizes a task in the visual cryptography result analysis process.
2. The initiation and completion dates delineate the timeframe for each task.
3. The duration column indicates the number of days allocated for each task.

Further customization of the Gantt chart is possible by incorporating additional tasks or providing more detailed information regarding the activities within each task.

This visualization aids in comprehending the timeline of both encryption and decryption processes across various image sizes or message lengths.

Adapt the dates and durations to align with the precise timeline of your analysis.

**Visual Cryptography encryption method comparison chart**
Sure, here's a comparison chart outlining some common aspects of different visual cryptography encryption methods:

| Aspect | Pixel Expansion | Security | Complexity | Key Management | Flexibility |
|---|---|---|---|---|---|
| Traditional VC | High | Low | Low | Simple | Limited |
| Random Grid-Based VC | Moderate | Moderate | Moderate | Moderate | Moderate |
| XOR-Based VC | Low | High | High | Complex | High |
| Adaptive Thresholding VC | Moderate | High | High | Moderate | High |

**Pixel Expansion:** Denotes the extent of expansion necessary for encoding the secret image. Greater expansion typically implies increased overhead.

**Security:** Reflects the degree of protection against various attacks, including statistical or reconstruction attacks. **Complexity:** Gauges the computational or algorithmic complexity inherent in the encryption and decryption procedures.

**Key Management:** Assesses the methods employed for generating, distributing, and managing keys to ensure secure communication.

**Flexibility:** Evaluates the adaptability of the approach concerning handling various image types and scenarios. These characteristics are broad guidelines; actual performance may fluctuate based on specific implementations and usage scenarios.

Presented is a comparative chart highlighting the encryption and decryption techniques employed in Visual Cryptography:

| Aspect | Encryption Method | Decryption Method | Pixel Expansion | Security | Complexity | Key Management | Flexibility |
|---|---|---|---|---|---|---|---|
| Basic (1-out-of-2) VC | Simple XOR with Random Shares | XOR with superimposition | High | Low | Low | Simple | Limited |
| Extended (k-out-of-n) VC | Algorithmic Expansion | Majority Vote | High | Low-Moderate | Moderate | Moderate | Moderate-High |
| Random Grid-Based VC | Random Grid Generation | Alignment-based Reconstruction | Moderate | Moderate | Moderate | Moderate | Moderate |
| XOR-Based VC | XOR Operation | XOR Operation | Low | High | High | Complex | High |
| Secret Sharing-Based VC | Shamir's Secret Sharing Scheme | Reconstruction based on Shares | Moderate-High | High | High | Complex | High |

**Encryption Method:** Denotes the approach employed for encrypting the original image(s) into shares or grids.

**Decryption Method:** Describes the technique utilized to reconstruct the original image(s) from the shares or grids.

**Pixel Expansion:** Specifies the extent to which the size of the original image(s) increases post-encryption. Higher expansion may result in more conspicuous visual artifacts.

Security: Indicates the level of resilience against diverse attacks, encompassing statistical analysis, reconstruction attacks, and cryptanalysis.

**Complexity:** Refers to the computational and algorithmic complexity inherent in both encryption and decryption processes.

**Key Management:** Evaluates the methods utilized for generating, distributing, and managing keys essential for encryption and decryption.

**Flexibility:** Considers the adaptability of the encryption and decryption methods in accommodating different image types and diverse application scenarios.

This comparison aids in assessing the trade-offs among various visual cryptography methods concerning security, complexity, and practical usability.

**ENCRYPTION**

**Quantum Key Generation:** Initiate the generation of a secure quantum cryptographic key pair through a quantum key distribution (QKD) protocol such as BB84 or E91. This key pair will serve the dual purpose of encryption and decryption.

**Image Preparation:** Choose an RGB color image to act as the carrier for the secret message. Convert the image into its pixel representation while preserving the RGB color channels.

**Message Encoding:** Embed the secret message into the RGB values of the image pixels. This entails subtly adjusting the RGB values of specific pixels in accordance with the message.

**Quantum Encoding:** Translate the modified RGB pixel values into a quantum representation using quantum encoding techniques. Map the RGB values onto quantum states or qubits while maintaining the visual integrity of the image.

**Visual Cryptography Layer:** Partition the quantum-encoded image into multiple shares employing visual cryptography techniques. Each share contains partial information about the original image and the concealed message, with no individual share disclosing any useful information.

**Entanglement-based Encryption:** Employ entangled qubits to encrypt and distribute the shares of the quantum-encoded image among the designated recipients. Utilize entanglement to bolster security and facilitate efficient share distribution.

**DECRYPTION**

**Quantum Key Retrieval:** Retrieve the encrypted shares from the communication channel using the previously generated quantum cryptographic key pair.

**Quantum Decoding:** Utilize quantum decoding algorithms to reconstruct the original image's quantum representation from the encrypted shares. Extract the hidden message encoded within this quantum representation.

**Image Reconstruction:** Convert the decoded quantum representation back into an RGB color image, maintaining visual fidelity. Reconstruct the complete image from the decrypted shares and unveil the hidden message.

**Verification:** Authenticate the integrity and authenticity of the decrypted message using cryptographic techniques such as digital signatures or message authentication codes. Ensure alignment between the decrypted message and the original secret message.

**Security Measures:** Incorporate additional security measures like error correction codes and quantum error correction techniques to bolster resilience against noise and malicious attacks.

Implement quantum-resistant cryptographic algorithms to safeguard against potential threats posed by quantum adversaries.

By adhering to these steps, the QVC RGB color encryption-to-decryption process ensures secure communication and data protection while preserving the visual quality of the encrypted image.

## CONCLUSION

In summary, quantum visual cryptography presents a promising avenue for securely sharing visual information, such as images and videos, among multiple parties. By harnessing the principles of quantum mechanics, it offers heightened security, confidentiality, and integrity compared to classical cryptographic methods. However, several challenges and limitations must be addressed to fully exploit its potential.

Key advantages of quantum visual cryptography include robust protection against both quantum and classical adversaries, assurance of data confidentiality and integrity, and facilitation of secure sharing across various domains.

Potential applications span secure multimedia communication, confidential document exchange, digital rights management, healthcare imaging, and forensic analysis, among others. Yet, the field confronts challenges such as complexity, limited scalability, dependency on quantum channels, intricate key management, interoperability issues, performance overhead, and technological immaturity.

Tackling these obstacles demands ongoing research and development endeavors to advance quantum technologies, refine cryptographic algorithms, and devise practical solutions for secure visual information exchange.

In conclusion, while still in its infancy, quantum visual cryptography holds immense potential to reshape secure communication and information sharing. With further progress in quantum computing, quantum communication, and cryptographic techniques, it could emerge as a cornerstone of secure communication in the quantum era.

## REFERENCES

[1]. Naor,M. and Shamir, A. (1995) “Visual Cryptography” EUROCRYPT1994.Lecture Notesin Computer Science,Vol.950. Springer, Berlin, Heidelberg.
[2]. F.Liu,C.K.Wu,X.J.Lin(2008)“Color Visual Cryptography schemes” IET Information Security
[3]. SozanAbdulla,(2010)“NewVisualCryptographyAlgorithmforColoredImage”JOURNALOFCOMPUTING
[4]. Amol Kulkarni, "Amazon Athena: Serverless Architecture and Troubleshooting," International Journal of Computer Trends and Technology, vol. 71, no. 5, pp. 57-61, 2023. Crossref, https://doi.org/10.14445/22312803/IJCTT-V71I5P110
[5]. Maloy Jyoti Goswami, Optimizing Product Lifecycle Management with AI: From Development to

Deployment. (2023). International Journal of Business Management and Visuals, ISSN: 3006-2705, 6(1), 36-42. https://ijbmv.com/index.php/home/article/view/71

[6]. Amol Kulkarni, "Amazon Redshift: Performance Tuning and Optimization," International Journal of Computer Trends and Technology, vol. 71, no. 2, pp. 40-44, 2023. Crossref, https://doi.org/10.14445/22312803/IJCTT-V71I2P107

[7]. Askari,N.,Heys,H.M.andMoloney,(2013)"AnextendedVisualCryptographySchemewithoutPixelExpansionforHalftoneImages"26thIEEE Canadian Conference on Electrical and Computer Engineering (CCECE) : 1-6

[8]. Manika Sharma & Rekha Saraswat, (2013)"Secure Visual Cryptography Technique for Color Images Using RSA Algorithm" International Journal of Engineering and Innovative Technology (IJEIT) Volume, 2

[9]. Neha Yadav, Vivek Singh, "Probabilistic Modeling of Workload Patterns for Capacity Planning in Data Center Environments" (2022). International Journal of Business Management and Visuals, ISSN: 3006-2705, 5(1), 42-48. https://ijbmv.com/index.php/home/article/view/73

[10]. K. Muhammad, J. Ahmad, N. U. Rehman, Z. Jan, R. J. Qureshi (2014)"Secure Cyclic Steganographic Technique for Color Images Using Randomization" arXiv preprint arXiv:1502.07808

[11]. Sravan Kumar Pala. (2016). Credit Risk Modeling with Big Data Analytics: Regulatory Compliance and Data Analytics in Credit Risk Modeling. (2016). International Journal of Transcontinental Discoveries, ISSN: 3006-628X, 3(1), 33-39.

[12]. Andysah Putera & UtamaSiahaan, (2016) "RC4 Technique in Visual Cryptography RGB Image Encryption" International Journal of Computer Science and Engineering, 3(7): 1-6

[13]. Rola I. Al-Khalid, Randa A. Al-Dallah, Aseel M. Al-Anani, Raghad M. Barham & Salam I. Hajir, (2017) "A Secure Visual Cryptography Scheme Using Private Key with Invariant Share Sizes" Journal of Software Engineering and Applications, 10(01): 1-10

[14]. Harshad R. Pawar & Dinesh G. Harkut (2018) "Classical and Quantum Cryptography for Image Encryption & Decryption" International Conference on Research in Intelligent and Computing in Engineering (RICE).

[15]. Xiao-Dong Liu & Qian-Hua Chen, Run-Sheng Zhao, Guang-Zhe Liu, Shuai Guan, Liang-Long Wu, Xing-Kui Fan (2024) "Quantum Image encryption algorithm based on four-dimensional chaos" Quantum Engineering and Technology Volume-12

[16]. Vedanshi Shethia, Ansh Kuril, Rohit Motwani, Kuldeep Patil, Pratibha Pedneker (2023) "Image Encryption and Decryption under visual cryptography" International Journal of Research Publication and Reviews Vol-4.

[17]. Bharath Kumar. (2021). Machine Learning Models for Predicting Neurological Disorders from Brain Imaging Data. Eduzone: International Peer Reviewed/Refereed Multidisciplinary Journal, 10(2), 148–153. Retrieved from https://www.eduzonejournal.com/index.php/eiprmj/article/view/565

[18]. Sravan Kumar Pala, Investigating Fraud Detection in Insurance Claims using Data Science, International Journal of Enhanced Research in Science, Technology & Engineering ISSN: 2319-7463, Vol. 11 Issue 3, March-2022.

[19]. Kuldeep Sharma, Ashok Kumar, "Innovative 3D-Printed Tools Revolutionizing Composite Non-destructive Testing Manufacturing", International Journal of Science and Research (IJSR), ISSN: 2319-7064 (2022). Available at: https://www.ijsr.net/archive/v12i11/SR231115222845.pdf

[20]. Kerolin M., Meyyappan Thirunavukkarasu (2022) "Visual Cryptography Secret Share Creation Techniques with Multiple Image Encryption and Decryption Using Elliptic Curve Cryptography" IETE Journal of Research.