Securing the Future: Advanced Encryption for Quantum-Safe Video Transmission

Yashas Hariprasad, *Student Member, IEEE,* S.S. Iyengar, *Life Fellow, IEEE,* Naveen Kumar Chaudhary, *Senior Member, IEEE*
Corresponding Author: S.S. Iyengar (email: iyengar@cs.fiu.edu)

***Abstract*—The rapid growth of digital communication and video transmission has brought about an urgent need for robust encryption methods to ensure the security and integrity of video data. Traditional encryption techniques, while effective, face increasing challenges from advancing computing capabilities. Quantum cryptography has emerged as a promising solution to secure video transmission. In this article, we propose a novel cutting-edge Hybrid Quantum Video Encryption Framework. Our key idea is to integrate the strengths of quantum encryption and the classical video transmission paradigm to enhance the security of video transmission. By combining the proposed quantum encryption framework which uses a pseudorandom number generated key to perform a row-wise XOR operation along with the secure SSL-encrypted HTTP transmission over the internet, this framework provides a robust defense against threats. The experimental simulation conducted under the new computational integrated paradigm shows the strong encryption capability of the proposed method. The superior performance of the proposed method (ranges from 10-15 % compared to the existing methods) as validated through statistical analysis, outperforms the state-of-the-art video encryption frameworks in terms of Information Entropy and Correlation Coefficient for encrypted plain images offering a significant advancement in the field of secure video transmission.**

***Index Terms*—Quantum Video Encryption, Quantum Computing, Secure Video Transmission**

I. Introduction

THE advent of digital communication has revolutionized the way information is transmitted and shared across various networks. With the widespread use of video transmission over the internet, ensuring the security and integrity of these video streams has become increasingly crucial [35]. Traditional encryption methods have been effective in safeguarding data during transmission, but advancements in computing power and algorithmic techniques have posed significant challenges to their robustness [1]. Videos and videoconferencing are now routinely used in a variety of settings, including corporate meetings, political campaigns, and educational settings. Major videoconferencing solutions like Zoom, Webex, and Microsoft Teams have experienced exponential growth as a result of the rise in users recently. A surge in digital exposure and video manipulation is a result of this expansion [2]. As a result, the demand for more secure and reliable encryption techniques has emerged.

Quantum computing, a groundbreaking computational approach utilizing properties such as entanglement and quantum superposition, holds great potential for solving complex problems in parallel computing. However, it poses a serious threat to traditional encryption techniques that are purely based on computational complexity [3], [4], [35]. As a result, quantum cryptography has become an important area of study. Quantum picture encryption is one such multidisciplinary field of study that combines quantum cryptography and quantum information processing to guarantee the security of quantum pictures.

In the realm of video transmission security, Quantum Key Distribution (QKD) has emerged as a promising solution, as highlighted by recent developments [5]. QKD revolutionizes the secure exchange of encryption keys over a public channel, ensuring the confidentiality and authenticity of the shared keys. Leveraging photon characteristics like inseparability and quantum uncertainty, quantum communication introduces formidable obstacles for potential attackers aiming to breach sensitive information.

More importantly, a distinctive attribute of QKD techniques is the generation of keys with complete randomness. This independence from computational complexity in security systems for communication ensures that advancements in computational power and mathematical methods do not compromise the security of quantum cryptosystems [8]. The cryptographic keys are generated with complete randomness, a feature derived from the inherent uncertainty of quantum systems. Unlike traditional cryptographic methods, QKD leverages the principles of quantum mechanics to produce keys that are unpredictable. This randomness arises from the behavior of individual quantum particles, such as photons, which cannot be precisely measured or controlled due to fundamental quantum uncertainty. Consequently, the keys generated through QKD offer a higher level of security since they are not susceptible to prediction or brute-force attacks. The randomness of the keys is guaranteed by the laws of quantum physics themselves [8]

Furthermore, the laws of quantum mechanics play a crucial role in this context. According to Heisenberg's uncertainty principle, an attacker attempting to intercept a photon and measure its state would face inherent limitations in extracting useful information. This principle acts as a safeguard, detecting any effort to measure the state of a single photon and

This research was sponsored by the Army Research Office and NSF and was accomplished under Grant Number W911NF-21-1-0264 and 2018611 respectively.

Yashas Hariprasad and S.S. Iyengar are with the Knight Foundation School of Computing and Information Sciences, Florida International University, Miami, FL, 33199, Email: yhari001@fiu.edu, iyengar@cs.fiu.edu

Naveen Kumar Chaudhary is with National Forensics Sciences University, Gandhinagar, India, 382007, Email: naveen.chaudhary@nfsu.ac.in

preserving the confidentiality of the key established between communicating parties [6]. Also, the detection relies on other principles, such as the non-orthogonality of states or the monogamy of entanglement. These principles are essential for ensuring security. Even if an attacker manages to replicate a single photon's quantum state (quantum cloning), the no-cloning theorem asserts that an unknown quantum state cannot be perfectly duplicated [7], thus ensuring the integrity and security of the transmitted key.

In this paper, we propose a hybrid quantum encryption framework fused with traditional secure transmission for sensitive videos. We create a robust and secure system that guarantees the confidentiality, integrity, and authenticity of video data during transmission by fusing the advantages of these two technologies which provide a greater degree of security against eavesdropping, interception, and manipulation of videos. More importantly, a pseudorandom key is generated which will be used during the encryption operation on the plain video frame. The encrypted video frames and the key image will be transmitted using Transport Layer Security (TLS) encrypted Hypertext Transfer Protocol (HTTP) over the internet network [38] to ensure robust transmission of the video files.

The reliance on quantum properties ensures that any attempt to intercept or clone quantum information would introduce detectable errors, alerting legitimate parties. Nonetheless, quantum encryption holds significant promise for securing video data in the face of modern threats.

Summary of our contribution:

- We propose a novel video encryption framework utilizing GQIR quantum image representation. The process involves conducting a row-wise XOR operation on a bit-by-bit basis to ensure confidentiality and authenticity.
- To ensure a highly resilient and secure transmission of the video files and to safeguard the integrity and confidentiality of the transmitted video data, we employ SSL-encrypted HTTP over the internet network.
- We conduct extensive experimental simulations to demonstrate the capability of plain image frame encryption showing that our model achieves best performance.
- To validate the superior performance, we present a detailed statistical analysis and comparison in terms of Information Entropy, Histogram Analysis, and Correlation Coefficient.

Organization of the paper: In Section 2, we present the related research that pertains to Quantum Image/Video Encryption Techniques. In Section 3, we describe the fundamental concepts underpinning our work. Section 4 introduces our novel innovative approach in 4 phases. The experimental setup and results followed by the statistical analysis are presented in Section 5. We also discuss how our results compare with existing state-of-the-art techniques across a variety of metrics. Finally, in Section 6, we conclude our work.

II. Related Works

The increased usage of video transmission via the Internet has created worries regarding the security and integrity of video transmissions. Data transmission has been made secure by using conventional encryption techniques like symmetric and asymmetric encryption. However, as computational power and algorithmic approaches improve, the risk of cryptographic attacks increases. Researchers and industry professionals are investigating and creating new encryption solutions to overcome these issues and guarantee the security and integrity of video feeds. The following related papers published in IEEE TCE enumerates algorithms that have major limitations and our work strategically provides novel and better encryption solutions and this is the focus of this paper.

A novel algorithm was proposed by Dang et al. [39] that combines Discrete Wavelet Transform (DWT) for image compression and Data Encryption Standard (DES) for fortified image encryption, specifically targeting security vulnerabilities pervasive in internet multimedia applications. By synergizing the principles of joint source coding and cryptographic coding, this algorithm not only bolsters security but also optimizes transmission rates. Employing techniques such as packetization encryption and wavelet-embedded zerotree coding (EZW), it ensures both data integrity and confidentiality throughout transmission. Crucially, DES is applied subsequent to EZW, effectively mitigating the risk of plaintext attacks, thereby enhancing security during both compression and encryption processes. Notably, the algorithm provides users a spectrum of options to tailor security enhancements to their specific needs. Users can opt for different wavelet filters, including the creation of custom filters as recommended in Part II of the JPEG 2000 standard, or they can leverage wavelet packet decomposition instead of octave-based decomposition. Additionally, users retain the flexibility to implement various algorithms for transposition operations in the subbands and can substitute DES with other robust encryption algorithms for further fortification of the compressed bit stream.

Sudharsanan [40] presents a novel encryption algorithm tailored specifically for JPEG images, operating directly on quantized Discrete Cosine Transform (DCT) coefficients within the JPEG domain. This innovative approach eliminates the need for conversion back to the spatial domain, ensuring encryption can be performed without loss of data. By splitting the monochrome image into 8×8 non-overlapping blocks and applying an 8×8 DCT to each block followed by scalar quantization, the algorithm quantizes the coefficients using a designated matrix. These quantized coefficients are then transformed into a one-dimensional vector through zig-zag scanning and fed into an entropy coder, which can utilize either Huffman or arithmetic coding. The resulting encrypted shares, stored in JPEG format, maintain compatibility with mainstream imaging applications, facilitating seamless integration into existing workflows while ensuring lossless decryption and retrieval of the original JPEG data. The decryption process involves reconstructing the quantized coefficients from the encrypted shares using a bit-wise XOR operation. Each block's shares are generated from the quantized coefficients, and two entropy encoders produce the final JPEG share images. Remarkably, the algorithm's hardware complexity primarily hinges on the need for a robust random number generator, which is increasingly prevalent in modern processor imple-

mentations. Moreover, the additional entropy encoder incurs a minimal cost, and while the bit decision process is described as serial, parallelization is straightforward.

Chiaraluce et al. [41] introduces a cutting-edge encryption algorithm specifically designed for securing video data, overcoming previous challenges associated with processing time and security. Unlike conventional methods that often compromise either processing speed or security levels, this algorithm achieves superior security measures without significant increases in processing time. Central to its innovation is the utilization of three distinct chaotic functions (CM1, CM2, and CM3), with the latter being one-dimensional and derived from the sum of two real numbers, a departure from prior approaches which typically relied on a single function. The authors present the significance of the initial states and control parameters for these chaotic functions, emphasizing their crucial role in generating the chaotic mask essential for encrypting the video data. With a focus on ensuring robust security, the algorithm incorporates various checks and adjustments, such as preventing divergence risks and ensuring parameter ranges, to guarantee the integrity and effectiveness of the encryption process. By summing the real numbers produced by the chaotic functions and applying further scaling operations, the algorithm generates encryption sequences essential for securing the video data. Robust against potential occurrences of zero sequences, the algorithm maintains a high level of security while accommodating frequent key changes to mitigate periodicity risks.

Singh et al. [42] propose a novel encryption technique tailored for color images, leveraging a 3D chaotic map to generate cipher images closely resembling the originals. The algorithm demonstrates robust chaotic behavior, validated through rigorous randomness assessments including the National Institute of Standards and Technology (NIST) test suite and Lyapunov exponent analysis. The contributions of their work are threefold: firstly, they introduce a new 3D chaotic map-based encryption algorithm for color images, showcasing its superior chaotic behavior through empirical testing. Secondly, they incorporate a lossy compression scheme to compress the cipher image without necessitating knowledge of a secret key, thus enhancing compression efficiency without compromising security. Lastly, they employ a customized Residual Dense Spatial Network (RDSN) to efficiently reconstruct images and address challenges in constrained super-resolution tasks, offering a comprehensive solution for image encryption and reconstruction. The proposed SIELNet algorithm emphasizes encryption before compression to bolster security. It utilizes a newly devised 3D chaotic map to encrypt color images, prioritizing data authenticity and trustworthiness. The cipher image is then compressed via downsampling and transmitted to the receiver for decryption. Finally, reconstruction is facilitated using the customized RDSN, ensuring efficient restoration of the original images. The algorithm safeguards image integrity during transmission and also enables efficient reconstruction at the receiver's end.

Mao et al. [43] introduces a covert communication method harnessing the time modulation of online video bullet comments, a popular feature on various online video platforms. By exploiting the absolute and relative time attributes of bullet comments, the proposed method embeds index values of loaded bullet comments and encrypted characters to convey secret messages. The sender converts secret information into encrypted characters, seamlessly integrating them into the sequence of normal bullet comments according to modulated timeframes. These loaded bullet comments are then uploaded to the corresponding video, while the receiver, upon extracting the bullet comments sequence, utilizes time information to decipher the index of loaded bullet comments and extract the encrypted characters, ultimately revealing the concealed message. To bolster communication security, the paper employs the Chaotic Encryption (CE) Algorithm to encrypt key data, ensuring symmetric encryption using shared seeds between sender and receiver. A notable contribution of this work lies in its analysis of the characteristics of bullet comments in online videos, identifying their suitability as a covert communication channel. By leveraging the time attributes of bullet comments, the proposed method achieves a double index of secret information, enhancing security and robustness. Furthermore, the paper presents an evaluation method based on the characteristics of secure communication on social media, highlighting the advantages of the proposed method over existing approaches. Through a systematic process divided into sending and receiving stages, this method offers a practical and effective means of covert communication in online video platforms, demonstrating its potential for secure information transmission in real-world scenarios.

Aribilola et al. [44] presents 'SecureCam', an innovative security application designed for mobile camera videos, which integrates selective detection and protection mechanisms using encryption. The selective detection module employs a novel low-computational unsupervised learning algorithm called Motion-Fusion (MF), enhancing the precision of motion detection in mobile camera videos. Subsequently, the detected video segments undergo selective encryption (SE) using the lightweight Chacha20 cipher, originally proposed for IoT devices. By selectively encrypting focused moving objects within the video stream, SecureCam ensures robust content protection while maintaining efficient processing capabilities suitable for real-time applications. The evaluation of SecureCam demonstrates its high accuracy in selective detection and protection of video content, showcasing its potential as an integral component of the Internet of Multimedia Things (IoMT) environment. Encryption using the Chacha20 algorithm provides a secure mechanism for safeguarding segmented video parts, with keys and nonces securely stored in hardware wallets to prevent unauthorized access. The paper elucidates the cryptographic operations involved in Chacha20 encryption, emphasizing its resistance to attacks due to its comprehensive round structure comprising arithmetic operations like integer addition modulo, bitwise exclusive OR, and N-bit left rotation. SecureCam thus represents a promising solution for enhancing security in mobile camera videos, offering a blend of precision motion detection and efficient content encryption to address contemporary privacy concerns in multimedia applications.

Mehraj et al. [45] introduce a robust and blind watermarking framework for cultural images (RBWCI), focusing

on ownership verification and copyright protection using the discrete cosine transform (DCT) domain. RBWCI employs a novel embedding approach based on the energy contraction property of the DCT transform, ensuring high robustness while preserving image quality even under various hybrid attacks. The watermark is embedded in the Cb and Cr channels of the YCbCr color model, exploiting the difference between preselected mid-frequency coefficients. To enhance watermark security, a double-layer encryption scheme involving chaotic and deoxyribonucleic acid (DNA) encryption is implemented. RBWCI operates as a blind watermarking technique, eliminating the need for an actual watermark or cover image during extraction, and exhibits resilience against hybrid attacks compared to state-of-the-art methods. The proposed authentication-based watermarking framework, RBWCI, undergoes three main steps: watermark preparation, embedding, and extraction. Host images in the RGB color space are converted to YCbCr, with the Cb and Cr channels used for watermark embedding. Each channel is divided into blocks, and a two-dimensional DCT is applied to each block. Mid-frequency coefficients are then selected, and their differences are adjusted based on specific watermark bits before applying inverse DCT to revert modified blocks to the spatial domain. Finally, the watermarked Cb and Cr channels are combined with the unchanged Y channel to reconstruct the watermarked image, demonstrating the effectiveness of RBWCI in cultural image authentication and copyright protection.

However, the proposed classical computing-based encryption schemes are susceptible to attacks due to their vulnerability to efficient factorization algorithms. Quantum encryption is one such field of study that shows promise for improved security. Quantum encryption techniques have the potential to provide higher security assurances since they make use of the laws of quantum physics. Multiple quantum encryption algorithmic methods have been proposed in the past for videos and images.

Yang et al. [9] propose a novel gray-level image encryption/decryption technique using double random-phase encoding and the quantum Fourier transform. The authors used a two-phase coding process as encryption keys in the Fourier transform and quantum image spatial domains. This was the first work to generalization of the double random-phase encoding method for quantum environments. A new quantum color image encryption algorithm based on a hyper-chaotic system was proposed by Tan et al. [10], in which the sequences generated by Chen's hyper-chaotic system are scrambled and diffused with three components of the original color image. This improved the slow processing speed of the classical image encryption algorithms and increased the security of private color images. To complete the encryption, the quantum Fourier transform was used sequentially. Sharma et al. [11] combine the discrete fractional Fourier transform (DFRFT) with the double random phase encoding technique in order to securely encrypt images. DFRFT is used to encrypt an image, and then the same is used in transform order to decrypt the image.

An innovative symmetric cryptography technique for digital video files was proposed by Kordov et al. [12] by combining two chaotic map forms. The authors assume that the video files are in raw video format and are made up of sequences of static pictures, and then apply the frame processing technique to encrypt the file. These assumptions are made in order to ensure that there is no compression or data loss during either the encryption or decryption operations. A novel quantum video encryption and decryption method on the basis of color information changes on each frame that encodes the video's content is presented by Yan et al. [13]. In order to increase the security of the video, the proposed technique offers a customizable operation to encrypt quantum video using a quantum measurement. The authors use a 10-frame video of the Tetris tile-matching puzzle game to simulate the proposed protocol. The video is changed into an incomprehensible collection of frames throughout the encrypting process and then by the use of revertible transformation during decryption the encrypted picture is restored to the original image.

Zhou et al. in [14] presented a quantum version of the generalized Arnold transform. They use the extended Arnold transform and the double random-phase encoding to create a unique quantum image encryption technique. The encryption algorithm's keys contain independent coefficients matrix parameters, iterative processes, and conventional binary sequences; as a result, the key space is large. The generalized Arnold transform scrambles the pixels, and the double random-phase operations encrypt the image's gray-level information. Hu et al. in [15] propose a novel quantum image encryption technique based on the modified flexible representation of quantum images. Arnold scrambling is the first step in the encryption process which disturbs the quantum picture information in the spatial domain. Quantum wavelet transforms are then used to decompose the scrambled quantum image into multiscale resolution in the frequency domain. The wavelet coefficients are then again encrypted in the frequency domain using Arnold scrambling. Then, the encrypted wavelet coefficients modify the pixel values of the fully rebuilt quantum pictures based on inverse quantum wavelet transformations.

Using Discrete Fractional Wavelet Transform (DFRWT) and quantum logical mapping, Li et al. [16] proposed a new picture encryption method. The method starts by using DFRWT to decompose several scales, then it shuffles high and low-frequency coefficients in the time-fractional-frequency domain to produce a scrambled picture. Through the use of an XOR operation and a pseudo-random sequence produced by quantum logical chaos, picture diffusion is achieved. To increase security, this method combines DFRWT-based decomposition, shuffles, and quantum logical chaos. Based on geometric transformation and intensity channel diffusion, a quantum color picture encryption technique was proposed [17]. The quantum image representation based on HSI color space (QIRHSI) was used as a carrier to first convert a plaintext picture into a quantum state form. The authors then used the generalized logistic was then used to create a pseudo-random sequence, with the pixel coordinates being permuted using several two-point swap operations. Following that, XOR, XNOR operations, and an intensity bit-plane cross-swap were used to alter the intensity values. The ciphertext picture was then obtained by performing a diffusion operation on the intensity bit-plane. Wang et al. [18] presented a novel encryption method for

quantum images based on double diffusions and the quantum wavelet transform (QWT). The proposed algorithm is a 2-step process where the input quantum picture underwent diffusion operation first, then the resultant quantum image underwent QWT to convert it to the frequency domain. A sensitive chaotic logistic map generates the encryption keys, ensuring the security of the system. The quantum image that underwent QWT transformation is subjected to the diffusion process.

Frequency-spatial domain iteration framework for the encryption and decryption of quantum images is proposed by Wang et al. [19]. The flexible representation for quantum images (FRQI) is used to represent the pictures. The positional information of the original photos is repeatedly scrambled by the encryption method using the Fibonacci and geometric transforms, while the color information is encoded using double random-phase encoding. Gong et al. [20] proposed a novel encryption technique based on quantum image XOR operations. The hyper-chaotic sequences produced by Chen's hyper-chaotic system are utilized to govern the control-NOT operation, which is used to encode gray-level information, to create the quantum picture XOR operations. In [21], a unique quantum picture encryption technique based on a quantum key image is proposed. The quantum key image's gray value contains the encryption keys, which are prepared using a cryptographic algorithm. Based on this quantum key picture, the plain image executes the XOR operations with it bit-by-bit.

He et al. [37] introduce OCPBP, a quantum image encryption algorithm leveraging superposition, entanglement, and quantum state instability for heightened security. OCPBP optimizes the quantum circuit and utilizes parity bit-plane permutation, reducing complexity and memory space while enhancing resistance to decryption attempts.

To address the limitations of purely quantum-based encryption, researchers have proposed hybrid frameworks that combine classical and quantum encryption techniques. Zhu et al. [5] proposed a hybrid encryption system for quantum-safe video conferencing coupled with blockchain. A combination of classical and quantum hybrid encryption schemes is built according to the secret level necessary for the video conference material after first embedding the quantum key distribution network in the classic network. Jose et al. [22] propose a hybrid encryption scheme that utilizes both classical symmetric encryption and quantum encryption which reduces communication overhead. The classical encryption techniques provide efficiency and robustness, while quantum encryption ensures enhanced security through key distribution using QKD. There are only a few studies that have looked into incorporating secure transmission into frameworks for quantum video encryption.

In contrast to the predominant focus in the literature on quantum cryptography, the proposed model introduces an innovative framework specifically designed for quantum video transmission. This framework not only tackles the distinct challenges inherent in video data but also puts forth a quantum-resistant encryption framework aimed at bolstering security. Experimental findings demonstrate that our approach surpasses existing quantum video encryption algorithms, paving the way for further empirical exploration and real-world implementation.

III. Preliminary Concepts

A. Quantum Image Representation

Digital images are encoded and represented utilizing quantum computing concepts and methods, which are referred to as quantum image representation (QIR). It investigates new ways to represent and interpret visual information by taking advantage of the special qualities of quantum systems. Digital images are commonly represented in traditional computers as grids of pixels, with each pixel including information about color or intensity. The visual data is, however, encoded into quantum states or quantum circuits in QIR. This encoding enables the manipulation and analysis of visual information through the use of quantum phenomena like superposition and entanglement. A digital image can be internally represented in a quantum processor using a variety of methods such as Flexible Representation of Quantum mages (FRQI) [23], Generalized Quantum Image Representation (GQIR) [24], Multi-Channel Representation for Quantum Images (MCQI) [25], Novel Enhanced Quantum Representation (NEQR) [26], Quantum log-Polar Image (QUALPI) [33], Flexible Representation for Quantum Color Image (FRQCI) [34] and so on. In our paper, we choose GQIR for our procedure because according to [27], GQIR is quite similar to the representation of a classical image and can represent a quantum image of any size, hence, it is simpler for researchers to comprehend and implement a conventional image processing technique into a quantum system.

To depict a $H \times W$ picture, GQIR employs $h = \lceil log_2\ H \rceil$ qubits for the Y-coordinate and $w = \lceil log_2\ W \rceil$ qubits for the X-coordinate. Color and location information are both stored in normalized quantum states $|0\rangle$ and $|1\rangle$ respectively. Consequently, a GQIR picture is represented as shown in equation 1.

$$|I\rangle = \frac{1}{\sqrt{2}^{h+w}} \left(\sum_{Y=0}^{H-1} \sum_{X=0}^{W-1} \otimes_{i=0}^{q-1} |C_{YX}\rangle\, |YX\rangle \right) \tag{1}$$

Where q is the color depth, h, and w are represented as equations 2 and 3.

$$h = \begin{cases} \lceil log_2\ H \rceil & H > 1 \\ 1 & H = 1 \end{cases} \tag{2}$$

$$w = \begin{cases} \lceil log_2\ W \rceil & W > 1 \\ 1 & W = 1 \end{cases} \tag{3}$$

$|YX\rangle = |Y\rangle\, |X\rangle = |y_{h-1}y_{h-2}\dots y_0\rangle\ \ |x_{w-1}x_{w-2}\dots w_0\rangle$ $y_0, x_0 \in \{0,1\}$ is the location information.

$|C_{YX}\rangle = \left| C^0_{YX} C^1_{YX} \dots C^{q-1}_{YX} \right\rangle$, $C^i_{YX} \in \{0,1\}$ is the color information.

In order to portray a $H \times W$ picture with gray range 2^q it requires $h + w + q$ qubits. GQIR is capable of depicting not just grayscale images but also colored ones, when q is equal to 2, an image is typically binary; when it is equal to 8, it is grayscale; and when it is equal to 24, it is a color image since q, the color depth is a variable.

B. Secure Sockets Layer Protocol

Secure Sockets Layer (SSL), is a cryptographic protocol used to secure data transmission over a computer network. It was developed by Netscape Communications Corporation [30]. SSL provides an encrypted connection between a user's web browser and a web server, preventing unauthorized access to sensitive information such as login credentials, credit card details, and personal data. SSL functions by combining asymmetric and symmetric encryption algorithms. Initially, the browser and server exchange digital certificates to verify each other's validity through a handshake process. After this handshake, all data communicated between the browser and server is encrypted, making it extremely unlikely for eavesdroppers to intercept or understand the information.

IV. Proposed Method

In this section, we propose our novel video encryption and transmission framework. The technique is presented in 4 Phases: 1. Key Generation; 2. Video Preprocessing; 3. Quantum Encryption; 4. Quantum Transmission.

A. Phase 1: Key Generation

We use a pseudorandom number generator to generate a key sequence where the length of the key is the same as the size of the video frame. Key K is generated as follows: Generate a random number series ranging from 0 to 255 for each pixel mapping to the size of the video frame and then convert these random numbers to a series of binary digits $\{0, 1\}$ such that $K = \{a_0, a_1, \ldots, a_{qk-1}\}$ where:

$$k = H * W \tag{4}$$

Figure 1 shows an example of this stream generation for a 1×3 grayscale picture and its representation in GQIR.

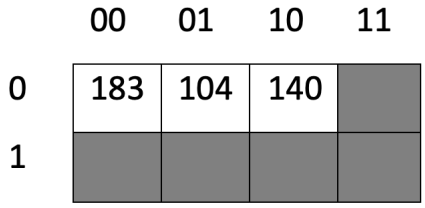


Fig. 1. Example of key series generation

Consider the example, $H = 1$, $W = 3$, This will give us $h = 1$ and $w = \lceil log_2\ 3 \rceil = 2$. Therefore, the 1×3 picture will be put into 2×4 box. Since we are considering only the gray value, only $Y = 0$ and $X = 00, 01, 10$ will be used.

Now using these values, we obtain the key:
$K = \{101101110110100010001100\}$.

Once we obtain the series, we model this to a 2D image into a quantum computer using GQIR method which will be our Key Image used for encryption. Every row of the key will use $H \times q$ bits from K as its gray value as shown in Figure 2.

Initially all the qubits $h + w + q$ is set to $|0\rangle$ and this state is represented as shown in equation 5

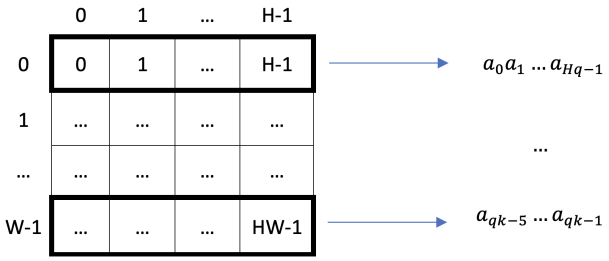


Fig. 2. Quantum Representation of Encryption Key

$$|\psi\rangle_0 = |0\rangle^{\otimes h+w+q} \tag{5}$$

A blank $2^h \times 2^w$ box is constructed using q identity gates (I) and $h+w$ Hadamard gates (H). The quantum operation of this is represented as U_1. This will transform the initial state $|\psi\rangle_0\ to\ |\psi\rangle_1$ which is an intermediate state.

$$U_1 = I^{\otimes q} \otimes H^{\otimes h+w} \tag{6}$$

$$\begin{aligned} |\psi\rangle_1 &= U_1\left(|\psi\rangle_0\right) \\ &= \left(I\,|0\rangle\right)^{\otimes q} \otimes \left(H\,|0\rangle\right)^{\otimes h+w} \end{aligned} \tag{7}$$

$$\begin{aligned} |\psi\rangle_1 &= \frac{1}{\sqrt{2^{h+w}}}\,|0\rangle^{\otimes q} \otimes \sum_{i=0}^{2^{h+w}-1} |i\rangle \\ &= \frac{1}{\sqrt{2^{h+w}}} \sum_{Y=0}^{2^h-1} \sum_{X=0}^{2^w-1} |0\rangle^{\otimes q}\,|YX\rangle \end{aligned} \tag{8}$$

The pixels' gray values are set for each pixel. The pictorial representation is shown in Figure 2. We can see that the key values are mapped to each row in the $H \times W$ picture. In order to store values for each pixel the quantum equations are as follows:

$$U_2 = \left(I \otimes \sum_{ji \neq YX} |ji\rangle\,\langle ji|\right) + \Omega_{YX} \otimes |YX\rangle\,\langle YX| \tag{9}$$

where Ω_{YX} is a quantum operation that modifies the value of the pixel (Y, X) from $|0\rangle^{\otimes q}$ to the value from key series K which is represented in Figure 2. Ω^i_{YX} will set the value of the ith qubit of pixel (YX)'s key information.

$$\Omega_{YX} = \otimes_{i=0}^{q-1} \Omega^i_{YX} \tag{10}$$

$$\Omega^i_{YX} :\ |0\rangle \rightarrow \left|0 \oplus K^i_{YX}\right\rangle \tag{11}$$

The XOR operation is denoted by $\oplus$ and the CNOT gate with $(h + w)$ control bits will work as follows: when $K^i_{YX} = 1$ then $\Omega^i_{YX} :\ |0\rangle \rightarrow \left|0 \oplus K^i_{YX}\right\rangle$. Else, $\Omega^i_{YX} :\ |0\rangle \rightarrow |0\rangle$ which will not do anything on the quantum state. Applying $U_2\ on\ |\psi\rangle_1$

$$
\begin{aligned}
U_2\left(|\psi\rangle_1\right) = & \ U_2\left(\frac{1}{\sqrt{2}^{h+w}}\sum_{j=0}^{2^h-1}\sum_{i=0}^{2^w-1}|0\rangle^{\otimes q}|ji\rangle\right) \\
= & \frac{1}{\sqrt{2}^{h+w}}U_2\left(\sum_{ji\neq YX}|0\rangle^{\otimes q}|ji\rangle + |0\rangle^{\otimes q}|YX\rangle\right) \\
= & \frac{1}{\sqrt{2}^{h+w}}U_2\left(\sum_{ji\neq YX}|0\rangle^{\otimes q}|ji\rangle + |K_{YX}\rangle|YX\rangle\right)
\end{aligned} \tag{12}
$$

This equation only sets the value for its particular pixel and all the other pixel values need to be set. In order to do that, another quantum operation U_3 is formulated.

$$
U_3 = \prod_{Y=0}^{H-1}\prod_{X=0}^{W-1}U_{YX} \tag{13}
$$

Applying U_3 *on* $|\psi\rangle_1$: This will transform the intermediate state $|\psi\rangle_1$ *to* $|\psi\rangle_2$ which is a final state (Encryption Key).

$$
|\psi\rangle_2 = U_3\left(|\psi\rangle_1\right) \tag{14}
$$

$$
\begin{aligned}
A &= \sum_{Y=0}^{H-1}\sum_{X=0}^{W-1}\Omega_{YX}|0\rangle^{\otimes q}|YX\rangle \\
B &= \sum_{Y\in\{H,\ \ldots,2^h-1\} or X\in W,\ldots,2^w-1}\otimes_{i=0}^{q-1}|0\rangle|YX\rangle \\
&= \frac{1}{\sqrt{2}^{h+w}}(A+B)
\end{aligned} \tag{15}
$$

B. Phase 2: Video Preprocessing

To prepare the video file for encryption and transmission, it will go through preprocessing steps which will reduce the length of the video into manageable chunks that can be further used. The video is first divided into scenes, which are separate chunks that differ in time, place, or content. The scenes are separated into shots after they have been recognized. A shot is an uninterrupted series of frames that a single camera continuously records. Finally, each shot is broken down into individual frames, which are the individual images that make up the video. Figure 3 represents the preprocessing steps.

C. Phase 3: Quantum Encryption

After the video data has been preprocessed, the frames will be encrypted using our novel quantum encryption approach, ensuring the security and confidentiality of the video. The key that is generated in Stage 1 is used for encryption. The key and the plain image are represented as matrices of pixels, with each pixel having color information. The key and the plain video frame are aligned using their position information. The alignment process makes sure that throughout the XOR operation, relevant pixels are correctly matched. The color information of the images is then bit by bit row-wise XORed to obtain the encrypted video frame. The XOR process is performed row by row, which means that each pixel in a particular row of the plain video frame is XORed with the matching pixel in the row of the key. This procedure makes sure that the encryption is used uniformly over the whole frame. Figure 4 shows a pictorial representation of the encryption process. The key used during encryption is used to decrypt this encrypted video frame. The original plain video frame $|P\rangle$ may be retrieved by doing an XOR operation between the encrypted image $|E\rangle$ and the key $|K\rangle$ with the proper alignment.

The equations for this operation are as follows:

$$
\begin{aligned}
|P\rangle &= \frac{1}{\sqrt{2}^{h+w}}\sum_{X=0}^{W-1}\otimes_{i=0}^{q-1}\left|C^i_{YX}\right\rangle|YX\rangle \\
|K\rangle &= \frac{1}{\sqrt{2}^{h+w}}\sum_{X=0}^{W-1}\otimes_{i=0}^{q-1}\left|K^i_{YX}\right\rangle|YX\rangle
\end{aligned} \tag{16}
$$

$$
|P\rangle \oplus |K\rangle = |E\rangle \tag{17}
$$

$$
|E\rangle = \frac{1}{\sqrt{2}^{h+w}}\sum_{X=0}^{W-1}\otimes_{i=0}^{q-1}\left|C^i_{YX}\oplus K^i_{YX}\right\rangle|YX\rangle \tag{18}
$$

D. Phase 4: Secured Video Transmission

In the proposed framework, we implement SSL-encrypted HTTP transmission over the internet to securely send video data. This approach ensures authenticity between the browser and the website by initiating an SSL/TLS handshake and verifying the identity of both communicating parties [38]. SSL (Secure Sockets Layer) certificates play a crucial role in ensuring the integrity of the quantum-secured image frames. These certificates utilize hashing algorithms to verify and guarantee that video frames remain untampered during transmission.

The framework relies on the TLS (Transport Layer Security) handshake for video transmission. The TLS protocol specifies a cipher suite of algorithms that facilitate the exchange of session keys or ciphered keys for every session. It is capable of establishing relevant session keys even over an unencrypted channel by employing public key cryptography.

In our proposed work, the TLS handshake manages authentication, which involves a server asserting the identity of the client for end-to-end video frame communication. Subsequently, the secured frames are shared using public keys that are one-way encrypted. This means that any recipient with the corresponding public key can decrypt the ciphered keys using the server's private key. This process ensures the integrity and authenticity of the original sender who encrypted the video frame with their private key, thereby maintaining the security of the transmitted video data.

V. Experimental Simulation and Results

In this section, we present a comprehensive examination of the novel encryption algorithm that we have presented in this paper. Due to the current unavailability of standard quantum computers, we resort to classical computing resources to execute the simulations necessary for our study. The current approach to simulate on classical systems lays the groundwork

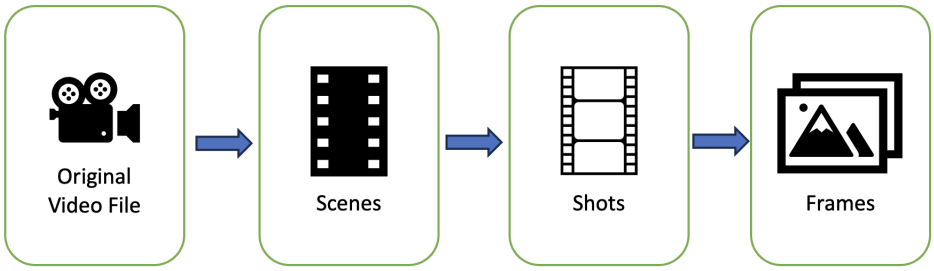


Fig. 3. Video to Frames Preprocessing

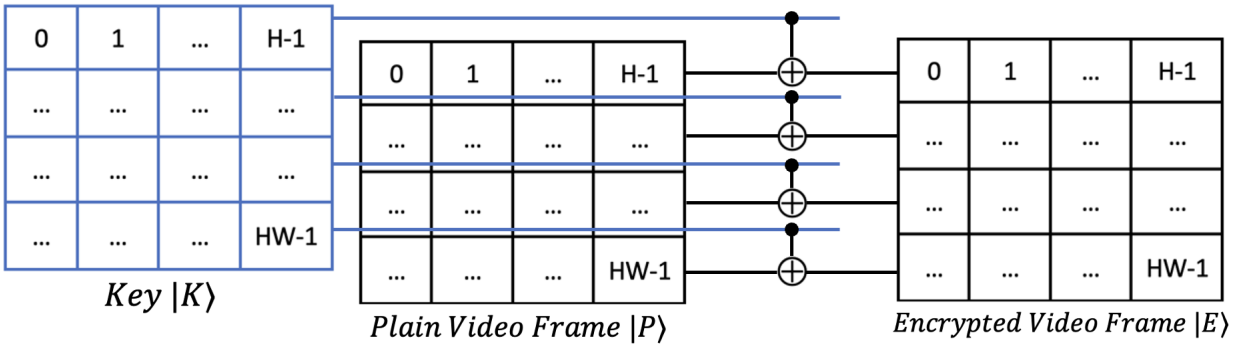


Fig. 4. Plain Video Frame and Key Encryption using CNOT gate

Fig. 5. (a) Shows the Plain Images of "Butterfly"; (b) Shows the Grayscale Plain Images of "Butterfly"; (c) Shows the Encrypted Images of "Butterfly"

for future advancements, offering a valuable interim solution while paving the way for seamless integration with quantum computers as they become more accessible. The core of our approach involves a Python script that plays a pivotal role in transforming quantum images into expansive matrices. These matrices serve as the canvas on which we simulate quantum phenomena, including intriguing aspects such as quantum entanglement and superposition. To emulate quantum operations, we utilize unitary matrices, thereby facilitating a classical interpretation of quantum processes. The crucial step in this process is the conversion of quantum information into a classical format. We achieve this by performing carefully chosen measurements on the quantum information, culminating in the extraction of probability distributions. This transformation from the quantum realm to the classical domain is pivotal in deciphering the encrypted content. The experiments are simulated on a single video frame for demonstration purposes, the methodology is designed to be applicable to a stream of image frames, thus encompassing full video files. The same encryption process used for the single frame in the study can be extended to video files, ensuring no visible or detectable information about the original frames is discernible

(a) Plain Image (b) Plain Image in Grayscale (c) Encrypted Image

Fig. 6. (a) Shows the Plain Images of "Peppers"; (b) Shows the Grayscale Plain Images of "Peppers"; (c) Shows the Encrypted Images of "Peppers"

post-encryption.

A. Experimental Setup

In this section, we detail the test images employed, our analytical approach, and the evaluation metrics applied in our research. Additionally, we offer a thorough validation of our experimental results through a comprehensive comparison of the statistical analysis outcomes. The experiments were conducted five times, and the average results were taken into account. These tests were carried out on an Apple MacBook Air equipped with 32 GB of RAM and an M2 processor.

Dataset: For our analysis, we have selected three prominent plain images, "Butterfly", "Peppers", and "Plane" each of size 512×512 pixels. These images serve as our benchmark for evaluating the effectiveness of our encryption algorithm using Python scripts.

Furthermore, the same process would be applied to a stream of image frames (Video File). The encrypted images based on the grayscale images that we have generated, corresponding to these plain images are presented in Figure 5 and 6. No visible or detectable information about the original photographs may be seen in these encrypted images. This is evidence of the capability of our encryption method.

B. Statistical Modeling and a Comparison of Performance

Statistical modeling is a valuable tool for evaluating the performance and security of image/video encryption techniques. We focus on three crucial statistical metrics in this research: information entropy, correlation coefficient analysis, and histogram analysis. Information Entropy, which measures the randomness and unpredictability of an encrypted image, sheds light on how strong a cryptographic technique is. Higher entropy levels suggest greater security, by making it extremely difficult for an attacker to identify patterns or learn information about the original image from the encrypted counterpart. On the other hand, correlation coefficient analysis explores the interdependence of pixel values within the encrypted image. Less predictability and more security are indicated by a lower correlation coefficient. The third technique, histogram analysis, provides a thorough analysis of pixel value distribution in encrypted images. Histograms that are evenly spaced demonstrate the method's effectiveness at masking the features of the underlying image. When pixel value distributions are erratic, histogram analysis helps identify possible vulnerabilities that may result.

1) Information Entropy: Information entropy, denoted as $H(X)$, quantifies the amount of uncertainty or randomness in a random variable X representing the set of the gray level [28]. Stronger encryption is indicated by a larger entropy number, which also suggests a higher level of unpredictability and the distribution of gray values to be more uniform. The following formula is used to define the information entropy of a discrete random variable with probability mass function $p(x)$:

$$H\left(X\right) = \ - \sum_{j=0}^{2^K-1} p(x)_j log_2 p(x)_j \tag{19}$$

In the context of image encryption, the probability distribution function, denoted as $p(x)_j$, estimates the possibility of coming across a certain symbol x_j. An 8-bit information entropy value is what a perfect encryption method should provide [29]. Real information sources seldom send fully random signals, hence in reality, the entropy of the source is typically less than this ideal number.

The information entropy values for the original images and their matching encrypted equivalents are shown in Table I. The information entropy values of all encrypted images closely resemble the 8-bit ideal value, which is a notable finding from Table I. This is significant proof that the proposed novel encryption technique successfully defends against entropy-based attacks by converting the original, meaningful images into almost random representations. It supports the idea that the encryption process strengthens the pictures' randomness and cryptographic robustness, making it difficult for unauthorized parties to extract valuable information from the encrypted data.

2) Histogram Analysis: Another fundamental statistical method for analyzing the distribution of pixel values inside a picture is histogram analysis. It aids in assessing how well an

Information Entropy H(X)	Images		
	Butterfly	Peppers	Plane
Plain Image	6.954241	7.571214	6.535651
Encrypted Image (Wang et.al [21])	-	7.99382	7.997785
Encrypted Image (He et.al [37])	-	7.99827	-
Encrypted Image (Khorrampanah et.al [46])	-	7.99829	-
Encrypted Image (Hosny et.al [47])	-	7.99821	-
Encrypted Image (Our Method)	**7.999262**	**7.99944**	**7.999249**

TABLE I
INFORMATION ENTROPY OF PLAIN IMAGE AND ENCRYPTED IMAGE COMPARISON

encryption technique can mask the details of the original image when it comes to image encryption. The encrypted image has a wide and consistent range of pixel values, which makes it difficult for an attacker to extract useful information.

Figure 8 presents the histograms for both the original images and their corresponding encrypted equivalents. These histograms are essential tools for determining how pixel values are distributed within the images and for assessing the efficacy and security of the proposed novel encryption technique. This homogeneity acts as a strong barrier against attacks based on histograms and indicates the successful concealing of intrinsic image properties. It provides a degree of pixel value distribution uniformity that defends against unauthorized extraction of information from the encrypted images, reaffirming its robustness in preserving image confidentiality. We can observe that the histograms of different plain images exhibit noticeable differences, highlighting the unique pixel value distributions inherent to each image. In contrast, the histograms of their corresponding encrypted images show uniformity and similarity. This phenomenon underscores the encryption algorithm's effectiveness.

3) Correlation Coefficient: Correlation coefficient analysis is a statistical method used to quantify the degree of linear relationship or correlation between two variables. In the context of image encryption, it is used to determine the degree of similarity or correlation between neighboring pixels within an image. A lower correlation coefficient denotes increased encryption security and signifies that pixel values are less predictable.

Mathematically, the Pearson Correlation Coefficient denoted as CCr is used to measure the linear correlation between two variables X and Y:

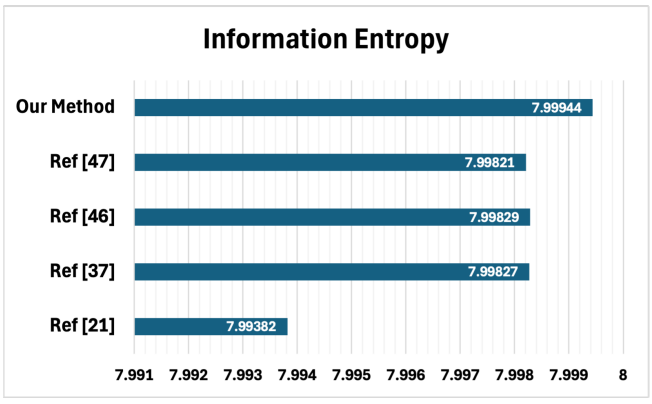


Fig. 7. Information Entropy H(X) of Encrypted Peppers Image comparison

$$CC_r = \frac{\sum_{i=1}^{N}(A)(B)}{\sqrt{\sum_{i=1}^{N}(A)^2}\sqrt{\sum_{i=1}^{N}(B)^2}} \tag{20}$$

Where:
$A = (X_i - \bar{X})$ and $B = (Y_i - \bar{Y})$
N = Total number of data points (in this case, pixels in the image)
X_i and Y_i are the pixel values at positions i in two adjacent pixels
$\bar{X}$ and $\bar{Y}$ are the mean pixel values of the entire image.

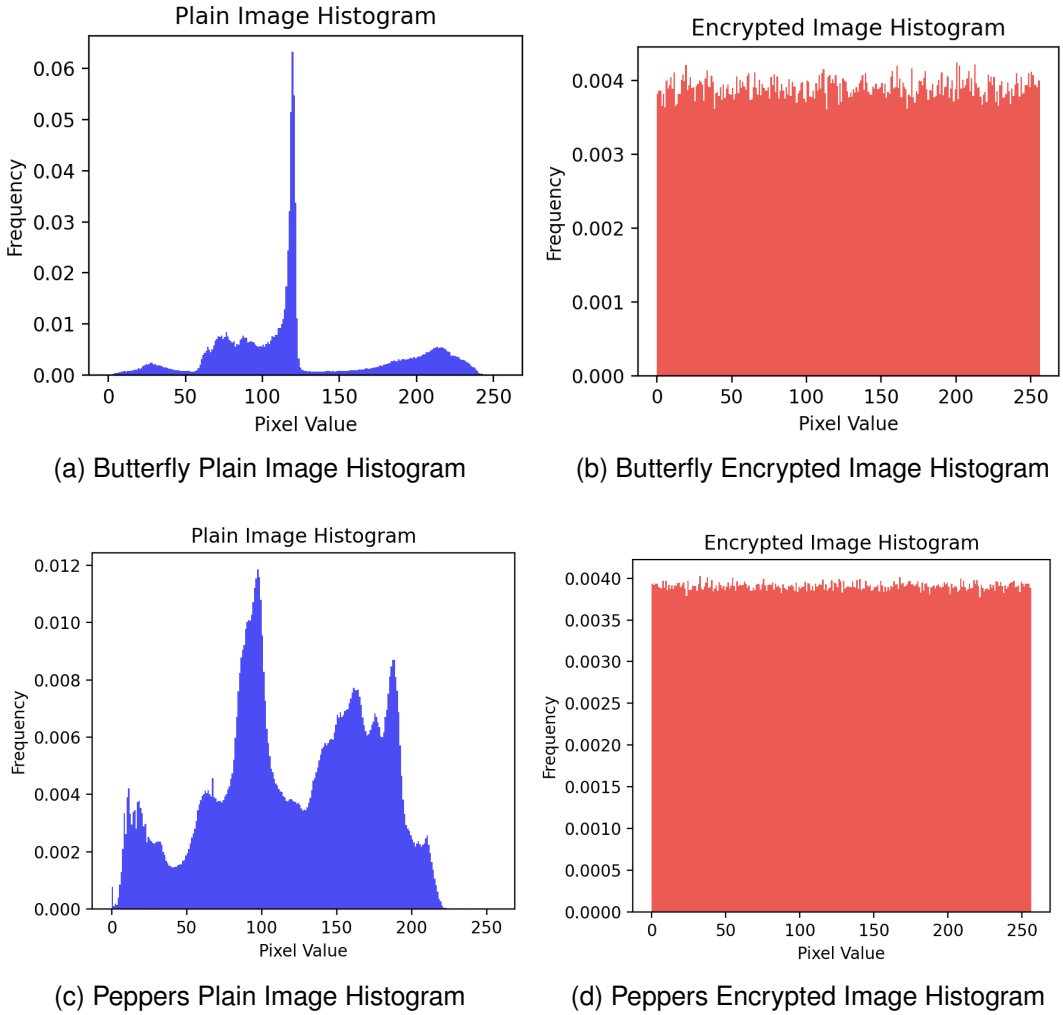
A correlation coefficient CCr close to 1 indicates that there is a strong positive linear relationship, meaning adjacent pixels in the image are highly correlated. A correlation coefficient close to -1 indicates that there is a strong negative linear relationship. A correlation coefficient close to 0 signifies that there is little to no linear relationship, indicating reduced predictability between pixel values.

A lower correlation coefficient in the encrypted image is the desired outcome because it shows that the encryption process has introduced randomness and unpredictability, making it challenging for an attacker to identify any information about the original image by examining the relationships between adjacent pixels.

We can observe this in Table II and III, which reveal differences in the correlation patterns between neighboring pixels. A strong association exists between neighboring pixels in the original image space in all directions—horizontally, vertically, and diagonally. Strong correlations like this suggest that the plaintext pictures are rather predictable, which might present a weakness for attackers looking to use these patterns to gather information. The reduction in size to 250 x 250 is aimed at focusing on the outcome of the calculation of Correlation Coefficients and the analysis of Histograms as this helps in highlighting results more clearly.

Conversely, a transition becomes apparent for the encrypted images. Regardless of the orientation, the correlation coefficients between neighboring pixels in the encrypted image constantly display weakness. This highlights the encryption algorithm's accomplishment of successfully obscuring the patterns that were originally visible in the plain image. In addition to strengthening image security, this decreased pixel correlation also serves as an effective disincentive against any attempts to decrypt the encrypted data by examining nearby pixel correlations.

Figure 8 illustrates the distribution patterns of two neighboring pixels within both the original image and its encrypted counterpart.



(a) Butterfly Plain Image Histogram (b) Butterfly Encrypted Image Histogram

(c) Peppers Plain Image Histogram (d) Peppers Encrypted Image Histogram

Fig. 8. (a) and (c) Show the Histograms for Plain Images of "Butterfly" and "Peppers" Respectively; (b) and (d) Show the Histograms for Encrypted Images of "Butterfly" and "Peppers" Respectively.

Plain Image (Our Method)	Horizontal Correlation	Vertical Correlation	Diagonal Correlation
Butterfly	0.977897	0.981830	0.966332
Peppers	0.972767	0.970884	0.947142
Plane	0.962669	0.961037	0.928884

TABLE II
CORRELATION COEFFICIENTS IN HORIZONTAL, VERTICAL AND DIAGONAL DIRECTION FOR PLAIN IMAGES

We can observe that the plain image generally displays a considerable similarity between these correlations in the context of neighboring pixel correlations, hence a considerable cluster of data points emerges around a 45-degree diagonal line, as seen in Figure 8 (a), (c), and (e). However, the correlation between neighboring pixels in the encrypted image must go toward zero in order for an encryption technique to be regarded as efficient. As a result, we can observe that all data points are evenly distributed within the rectangle, showing little to no association.

C. Threat Model and Validation

Threat Model: The threat model encompasses a range of sophisticated attacks targeting encrypted communication systems. Adversaries may employ network eavesdropping to intercept sensitive information exchanged between parties, including encryption keys or encrypted messages. Brute-force attacks involve systematically trying various combinations to decrypt encrypted content, exploiting weaknesses in encryption algorithms or key spaces. Side-channel attacks exploit information leaked during the encryption process, such as power consumption or timing data, to infer sensitive information about the encryption key or encrypted message. Cryptanalysis involves analyzing encrypted messages to uncover patterns or weaknesses in encryption algorithms, aiming to decipher content without knowledge of the encryption key.

Validation: In the face of a comprehensive threat model encompassing network eavesdropping, brute-force attacks, side-channel attacks, cryptanalysis, and quantum attacks, the

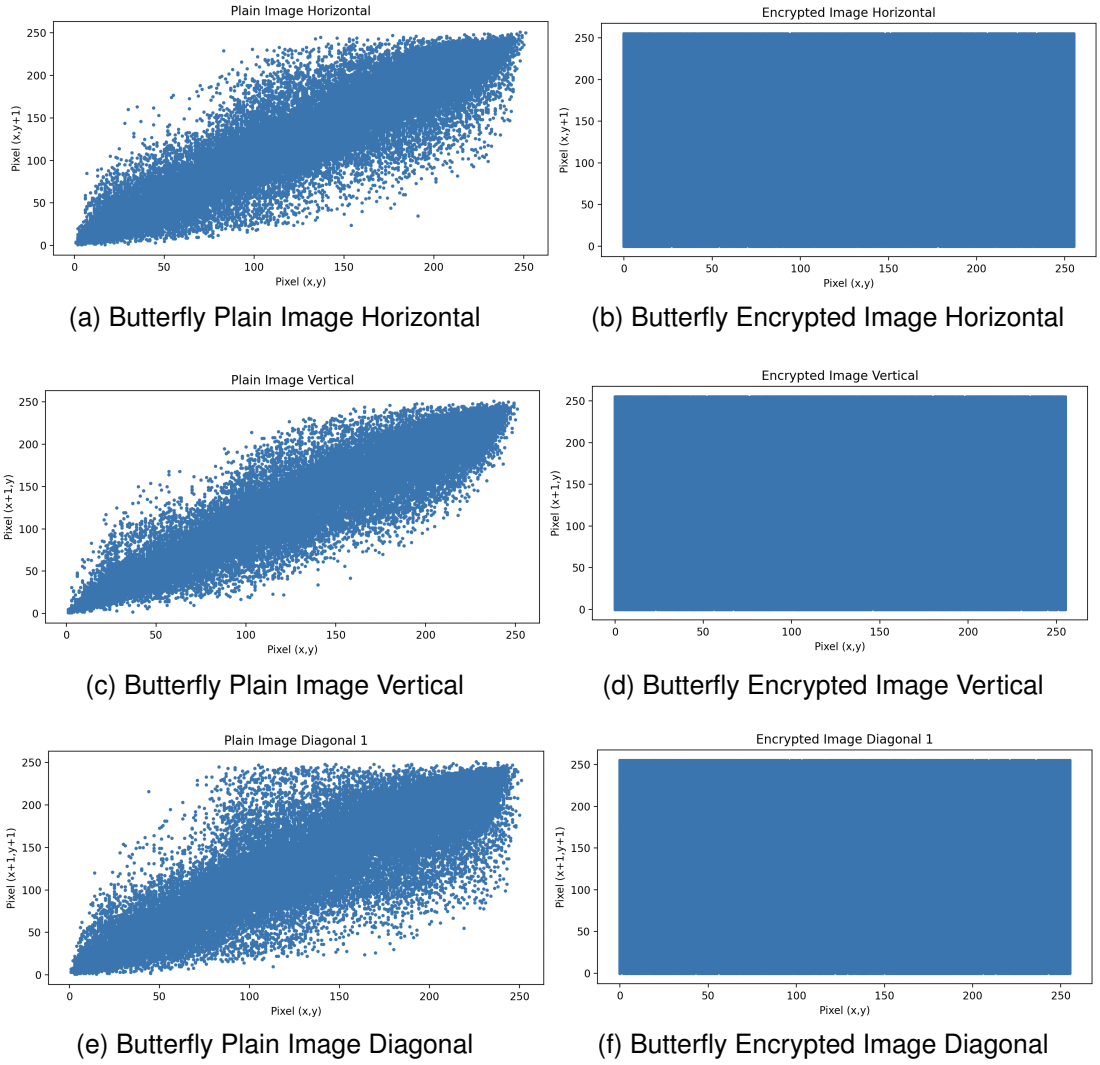


Fig. 9. (a), (c), (e) Represent the Correlation Coefficient distribution for Horizontal, Vertical, and Diagonal direction for the Butterfly Plain Image, and (b), (d), (f) Represent the Correlation Coefficient distribution for Horizontal, Vertical, and Diagonal direction for Butterfly Encrypted Image

method of Quantum Image Encryption utilizing GQIR and row-wise XOR operation emerges as a robust defense mechanism. By integrating GQIR, the encryption scheme gains immunity against potential quantum attacks, effectively safeguarding encrypted images from adversaries equipped with quantum computing capabilities. This resilience ensures that even with access to advanced resources, adversaries cannot efficiently decrypt the images, maintaining the confidentiality of the communication.

This strategy thwarts brute-force attacks by creating a vast and unpredictable key space, making it exceedingly difficult for attackers to guess or exhaustively search for the correct key. The encryption operation enhances the overall security posture by making it difficult for adversaries to decipher the encrypted images without possessing the quantum encryption key. Together, these measures effectively mitigate risks associated with network eavesdropping, brute-force attempts, and cryptanalysis, fortifying the encryption scheme against a myriad of potential threats.

Moreover, the implementation of secure key exchange protocols further bolsters the integrity of communication channels. These protocols ensure that encryption keys are exchanged securely, minimizing the risk of interception or manipulation by adversaries. By enhancing the integrity of communication channels, the overall security of the system is strengthened, complementing the robust encryption mechanisms in place. In essence, the combination of Quantum Image Encryption utilizing GQIR, pseudorandom number generation, row-wise XOR operation, and secure key exchange protocols form a comprehensive defense strategy against a diverse range of threats, ensuring the confidentiality and integrity of sensitive information in communication channels.

D. Future Work

Future investigations into enhancing the framework for quantum-safe video transmission could significantly benefit from a focused examination of scalability on a larger scale. This research direction is crucial for ensuring that the system can efficiently handle increasing data volumes and user

TABLE III
COMPARISON OF CORRELATION COEFFICIENTS IN HORIZONTAL, VERTICAL, AND DIAGONAL DIRECTION FOR ENCRYPTED IMAGES

Encrypted Image	Method	Horizontal Correlation	Vertical Correlation	Diagonal Correlation
Butterfly	Our Method	**0.002840**	**-0.002244**	**0.001953**
Peppers	Our Method	**-0.000193**	**-0.002015**	**-0.001263**
	Wang et.al [21]	0.014839	- 0.116362	- 0.002251
	He et.al [37]	0.0009	0.0005	0.0009
	Khorrampanah et.al [46]	0.0003	0.0012	- 0.0012
	Hosny et.al [47]	- 0.0145	0.0071	0.0200
Plane	Our Method	**-0.000836**	0.005059	**-0.000385**
	Gong et.al [20]	- 0.0064	**0.0043**	0.0266
	Wang et.al [21]	0.005333	- 0.122520	0.018075

demands without compromising security or performance. Furthermore, we plan to study the impacts on throughput and performance overhead for the proposed framework. Additionally, the development and refinement of more advanced quantum-resistant algorithms are imperative to proactively mitigate the evolving threats posed by quantum computing advancements. By prioritizing these areas, researchers can pave the way for more secure, efficient, and future-proof encryption technologies, ensuring that video transmission remains protected against the most cutting-edge cybersecurity threats.

VI. CONCLUSION

In this article, we introduce an innovative hybrid quantum video encryption and transmission framework that merges quantum encryption with traditional secure transmission methods to meet the growing need for secure video communication.

By harnessing the capabilities of quantum computing alongside the reliability of secure SSL transmission, this framework offers a powerful defense against eavesdropping, interception, and tampering with video data. Through the generation of pseudorandom encryption keys and the implementation of secure transmission protocols, it guarantees the confidentiality, integrity, and authenticity of video content, addressing the evolving challenges of an increasingly digital landscape.

This framework provides robust protection against unauthorized interception and manipulation, ensuring the security of video data as compared to all the existing work in the literature. We demonstrate the effectiveness of our approach through simulations conducted on a plain image frame, supported by statistical analysis that confirms its efficacy and feasibility (ranges from 10-15 % compared to the existing methods).

ACKNOWLEDGMENT

We extend our heartfelt gratitude to the Editor-in-Chief, Guest Editors, and diligent reviewers for their invaluable feedback, which significantly enhanced the clarity and coherence of this paper's content.

This research was sponsored by the Army Research Office and the NSF, and was accomplished under Grant Number W911NF-21-1-0264 and 2018611. The views and conclusions contained in this document are those of the authors and should not be interpreted as representing the official policies, either expressed or implied, of the Army Research Office or the U.S. Government. The U.S. Government is authorized to reproduce and distribute reprints for Government purposes notwithstanding any copyright notation herein.

REFERENCES

[1] Thabit, Fursan, Ozgu Can, Asia Othman Aljahdali, Ghaleb H. Al-Gaphari, and Hoda A. Alkhzaimi. "A Comprehensive Literature Survey of Cryptography Algorithms for Improving the IoT Security." Internet of Things (2023): 100759.

[2] Hariprasad, Yashas, K. J. Latesh Kumar, L. Suraj, and S. S. Iyengar. "Boundary-Based Fake Face Anomaly Detection in Videos Using Recurrent Neural Networks." In Proceedings of SAI Intelligent Systems Conference, pp. 155-169. Cham: Springer International Publishing, 2022.

[3] Mohseni, Masoud, Peter Read, Hartmut Neven, Sergio Boixo, Vasil Denchev, Ryan Babbush, Austin Fowler, Vadim Smelyanskiy, and John Martinis. "Commercialize quantum technologies in five years." Nature 543, no. 7644 (2017): 171-174.

[4] Thejas, G. S., Yashas Hariprasad, S. S. Iyengar, N. R. Sunitha, Prajwal Badrinath, and Shasank Chennupati. "An extension of Synthetic Minority Oversampling Technique based on Kalman filter for imbalanced datasets." Machine Learning with Applications 8 (2022): 100267.

[5] Zhu, Dexin, Jun Zheng, Hu Zhou, Jianan Wu, Nianfeng Li, and Lijun Song. "A hybrid encryption scheme for quantum secure video conferencing combined with blockchain." Mathematics 10, no. 17 (2022): 3037.

[6] Gisin, Nicolas, Grégoire Ribordy, Wolfgang Tittel, and Hugo Zbinden. "Quantum cryptography." Reviews of modern physics 74, no. 1 (2002): 145.

[7] Wootters, William K., and Wojciech H. Zurek. "The no-cloning theorem." Physics Today 62, no. 2 (2009): 76-77.

[8] Scarani, Valerio, Helle Bechmann-Pasquinucci, Nicolas J. Cerf, Miloslav Dušek, Norbert Lütkenhaus, and Momtchil Peev. "The security of practical quantum key distribution." Reviews of modern physics 81, no. 3 (2009): 1301.

[9] Yang, Yu-Guang, Juan Xia, Xin Jia, and Hua Zhang. "Novel image encryption/decryption based on quantum Fourier transform and double phase encoding." Quantum information processing 12 (2013): 3477-3493.

[10] Tan, Ru-Chao, Tong Lei, Qing-Min Zhao, Li-Hua Gong, and Zhi-Hong Zhou. "Quantum color image encryption algorithm based on a hyper-chaotic system and quantum Fourier transform." International Journal of Theoretical Physics 55 (2016): 5368-5384.

[11] Sharma, Deepak. "Robust technique for image encryption and decryption using discrete fractional Fourier transform with random phase masking." Procedia Technology 10 (2013): 707-714.

[12] Kordov, Krasimir, and Georgi Dimitrov. "A new symmetric digital video encryption model." Cybernetics and Information Technologies 21, no. 1 (2021): 50-61.

[13] Yan, Fei, Abdullah M. Iliyasu, Salvador E. Venegas-Andraca, and Huamin Yang. "Video encryption and decryption on quantum computers." International Journal of Theoretical Physics 54 (2015): 2893-2904.

[14] Zhou, Nan Run, Tian Xiang Hua, Li Hua Gong, Dong Ju Pei, and Qing Hong Liao. "Quantum image encryption based on generalized Arnold transform and double random-phase encoding." Quantum Information Processing 14 (2015): 1193-1213.

[15] Hu, Wen-Wen, Ri-Gui Zhou, Jia Luo, She-Xiang Jiang, and Gao-Feng Luo. "Quantum image encryption algorithm based on Arnold scrambling and wavelet transforms." Quantum Information Processing 19 (2020): 1-29.

[16] Li, Chunmeng, and Xiaozhong Yang. "An image encryption algorithm based on discrete fractional wavelet transform and quantum chaos." Optik 260 (2022): 169042.

[17] PSong, Xianhua, Guanglong Chen, and Ahmed A. Abd El-Latif. "Quantum color image encryption scheme based on geometric transformation and intensity channel diffusion." Mathematics 10, no. 17 (2022): 3038.

[18] Wang, Shen, Xianhua Song, and Xiamu Niu. "A novel encryption algorithm for quantum images based on quantum wavelet transform and diffusion." In Intelligent Data analysis and its Applications, Volume II: Proceeding of the First Euro-China Conference on Intelligent Data Analysis and Applications, June 13-15, 2014, Shenzhen, China, pp. 243-250. Springer International Publishing, 2014.

[19] Wang, Han, Jian Wang, Ya-Cong Geng, Yan Song, and Ji-Qiang Liu. "Quantum image encryption based on iterative framework of frequency-spatial domain transforms." International Journal of Theoretical Physics 56 (2017): 3029-3049.

[20] Gong, Li-Hua, Xiang-Tao He, Shan Cheng, Tian-Xiang Hua, and Nan-Run Zhou. "Quantum image encryption algorithm based on quantum image XOR operations." International Journal of Theoretical Physics 55 (2016): 3234-3250.

[21] Wang, Jian, Ya-Cong Geng, Lei Han, and Ji-Qiang Liu. "Quantum image encryption algorithm based on quantum key image." International Journal of Theoretical Physics 58 (2019): 308-322.

[22] Jose, M. Victor, and V. Seenivasagam. "An Enhanced Opass With Modified Elliptic Curve Cryptography-Based User Authentication Scheme For Grid Computing." Life Science Journal 10, no. 3 (2013).

[23] Le, Phuc Q., Abdullahi M. Iliyasu, Fangyan Dong, and Kaoru Hirota. "A flexible representation and invertible transformations for images on quantum computers." New Advances in Intelligent Signal Processing (2011): 179-202.

[24] Jiang, Nan, and Luo Wang. "Quantum image scaling using nearest neighbor interpolation." Quantum Information Processing 14 (2015): 1559-1571.

[25] Sun, Bo, A. Iliyasu, Fei Yan, Fangyan Dong, and Kaoru Hirota. "An RGB multi-channel representation for images on quantum computers." J. Adv. Comput. Intell. Intell. Inform 17, no. 3 (2013).

[26] Zhang, Yi, Kai Lu, Yinghui Gao, and Mo Wang. "NEQR: a novel enhanced quantum representation of digital images." Quantum information processing 12 (2013): 2833-2860.

[27] Jiang, Nan, Xiaowei Lu, Hao Hu, Yijie Dang, and Yongquan Cai. "A novel quantum image compression method based on JPEG." International Journal of Theoretical Physics 57 (2018): 611-636.

[28] Wang, Xing-yuan, Feng Chen, and Tian Wang. "A new compound mode of confusion and diffusion for block encryption of image based on chaos." Communications in Nonlinear Science and Numerical Simulation 15, no. 9 (2010): 2479-2485.

[29] Chen, Jun-xin, Zhi-liang Zhu, Chong Fu, and Hai Yu. "A fast image encryption scheme with a novel pixel swapping-based confusion approach." Nonlinear Dynamics 77 (2014): 1191-1207.

[30] "SSL Protocol - Netscape", Accessed October 14, 2023. https://www.ibm.com/docs/en/ibm-http-server/9.0.5?topic=communications-secure-sockets-layer-ssl-protocol

[31] Abd EL-Latif, Ahmed A., Bassem Abd-El-Atty, and Salvador E. Venegas-Andraca. "Controlled alternate quantum walk-based pseudo-random number generator and its application to quantum color image encryption." Physica A: Statistical Mechanics and its Applications 547 (2020): 123869.

[32] Li, Hai-Sheng, Qingxin Zhu, Ming-Cui Li, and Hou Ian. "Multidimensional color image storage, retrieval, and compression based on quantum amplitudes and phases." Information Sciences 273 (2014): 212-232.

[33] Zhang, Yi, Kai Lu, Yinghui Gao, and Kai Xu. "A novel quantum representation for log-polar images." Quantum information processing 12 (2013): 3103-3126.

[34] Li, Panchi, Hong Xiao, and Binxu Li. "Quantum representation and watermark strategy for color images based on the controlled rotation of qubits." Quantum Information Processing 15, no. 11 (2016): 4415-4440.

[35] Kumar, KJ Latesh, Yashas Hariprasad, K. S. Ramesh, and Naveen Kumar Chaudhary. "AI Powered Correlation Technique to Detect Virtual Machine Attacks in Private Cloud Environment." In AI Embedded Assurance for Cyber Systems, pp. 183-199. Cham: Springer International Publishing, 2023.

[36] Miller, Jerry, Lawrence Egharevba, Yashas Hariprasad, Kumar KJ Latesh, and Naveen Kumar Chaudhary. "Cyber Security Attack Detection Framework for DODAG Control Message Flooding in an IoT Network." In International Conference on Information Security, Privacy and Digital Forensics, pp. 213-230. Singapore: Springer Nature Singapore, 2022.

[37] He, Jinwen, Hegui Zhu, and Xv Zhou. "Quantum image encryption algorithm via optimized quantum circuit and parity bit-plane permutation." Journal of Information Security and Applications 81 (2024): 103698.

[38] Kunkelmann, Thomas. "Applying encryption to video communication." In Proceedings of the Multimedia and Security Workshop at ACM Multimedia, vol. 98, pp. 41-47. 1998.

[39] P. P. Dang and P. M. Chau, "Image encryption for secure Internet multimedia applications," in IEEE Transactions on Consumer Electronics, vol. 46, no. 3, pp. 395-403, Aug. 2000, doi: 10.1109/30.883383.

[40] S. Sudharsanan, "Shared key encryption of JPEG color images," in IEEE Transactions on Consumer Electronics, vol. 51, no. 4, pp. 1204-1211, Nov. 2005, doi: 10.1109/TCE.2005.1561845.

[41] F. Chiaraluce, L. Ciccarelli, E. Gambi, P. Pierleoni and M. Reginelli, "A new chaotic algorithm for video encryption," in IEEE Transactions on Consumer Electronics, vol. 48, no. 4, pp. 838-844, Nov. 2002, doi: 10.1109/TCE.2003.1196410.

[42] K. N. Singh, N. Baranwal, O. P. Singh and A. K. Singh, "SIEL-Net: 3-D Chaotic-Map-Based Secure Image Encryption Using Customized Residual Dense Spatial Network," in IEEE Transactions on Consumer Electronics, vol. 69, no. 4, pp. 862-868, Nov. 2023, doi: 10.1109/TCE.2022.3227401.

[43] C. Mao, Z. Li, M. Zhang, Y. Zhang and X. Luo, "A Covert Communication Method Adapted to Social Media Based on Time Modulation of Bullet Comments," in IEEE Transactions on Consumer Electronics, vol. 69, no. 3, pp. 568-580, Aug. 2023, doi: 10.1109/TCE.2023.3277919.

[44] I. Aribilola, M. N. Asghar, N. Kanwal, M. Fleury and B. Lee, "SecureCam: Selective Detection and Encryption Enabled Application for Dynamic Camera Surveillance Videos," in IEEE Transactions on Consumer Electronics, vol. 69, no. 2, pp. 156-169, May 2023, doi: 10.1109/TCE.2022.3228679.

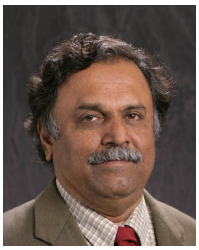
[45] S. Mehraj et al., "RBWCI: Robust and Blind Watermarking Framework for Cultural Images," in IEEE Transactions on Consumer Electronics, vol. 69, no. 2, pp. 128-139, May 2022, doi: 10.1109/TCE.2022.3217974.

[46] Khorrampanah, Mahsa, Monireh Houshmand, and Mohammad Mahdi Lotfi Heravi. "New method to encrypt RGB images using quantum computing." Optical And Quantum Electronics 54, no. 4 (2022): 245.

[47] Hosny, Khalid M., Sara T. Kamal, and Mohamed M. Darwish. "A color image encryption technique using block scrambling and chaos." Multimedia Tools and Applications 81, no. 1 (2022): 505-525.

Yashas Hariprasad is currently a Ph.D. candidate and holds the role of Graduate Research Assistant at Florida International University's (FIU) Knight Foundation School of Computing and Information Sciences (KFSCIS). He is actively involved in research conducted at the US Army-funded FINDS Digital Forensics Center of Excellence under the guidance of Dr. S. S. Iyengar. He possesses a strong foundation in Python, Machine Learning, Digital Forensics, and Cybersecurity. His collaborative efforts extend beyond his institution, as he has worked alongside researchers from various universities, including Poznan University of Technology in Poland, UNC-Chapel Hill, and SIT-India. Additionally, he has collaborated with industry experts as a Security Risk Analyst at VMware.

He has actively contributed to mentoring undergraduate and high-school students. His dedication and accomplishments in the field have earned him several awards, including an Appreciation medal from the Commander of DISA (Defense Information Systems Agency), a combat support agency within the United States Department of Defense. Outside of his research pursuits, he also took on leadership responsibilities by serving as the founding vice president of the Artificial Intelligence and Coding Club at FIU in 2022. Before embarking on his Ph.D. journey, he obtained a Bachelor of Engineering degree in Computer Science and Engineering from SIT, Tumkur, India, in 2020.



S.S. Iyengar is currently the Distinguished University Professor, Founding Director of the Discovery Lab and Director of the US Army funded Center of Excellence in Digital Forensics at FIU. He has been involved with research and education in high-performance intelligent systems, Data Science and Machine Learning Algorithms, Sensor Fusion, Data Mining, and Intelligent Systems. Since receiving his Ph.D. degree in 1974 from MSU, USA, he has directed over 65 Ph.D. students, many postdocs, and many research undergraduate students. He has published more than 600 research papers, has authored/co-authored and edited 32 books, and holds various patents. He has served on many scientific committees and panels worldwide and has served as the editor/guest editor of various IEEE and ACM journals.

His books are published by MIT Press, John Wiley and Sons, CRC Press, Prentice Hall, Springer Verlag, IEEE Computer Society Press, etc. More recently in Spring 2021, Dr. Iyengar in collaboration with HBCUs was awarded a $2.25M in funding for setting up a Digital Forensics Center of Excellence over a period of 5 years (2021-2026). He received an honorary Doctor of Science from Poznan University of Technology in Poland in May 2023. Dr. Iyengar is a Member of the European Academy of Sciences, a Life Fellow of the Institute of Electrical and Electronics Engineers (IEEE), a Fellow of the Association of Computing Machinery (ACM), a Fellow of the American Association for the Advancement of Science (AAAS), a Fellow of the Society for Design and Process Science (SDPS), and a Fellow of the American Institute for Medical and Biological Engineering (AIMBE).

x

Naveen Kumar Chaudhary Naveen Kumar Chaudhary has been a Professor of Cyber Security and Dean at National Forensic Sciences University, Gandhinagar, India, since 2019. He holds a Bachelor of Technology degree in Information Technology & Telecommunication Engineering and a Master of Engineering degree in Digital Communication.