International Journal of Safety and Security Engineering
Vol. 15, No. 11, November, 2025, pp. 2247-2259
Journal homepage: http://iieta.org/journals/ijsse

A Visual Cryptography Framework with Tuned Cipher Block Chaining and Quantum Key Distribution–Assisted Encryption for Securing Thermal Facial Biometrics in Anti-Doping Applications

K. Komathi*, D. Kavitha

Department of Computer Applications, St Peter's Institute of Higher Education and Research, Chennai 600054, India

Corresponding Author Email: komathikumarofficial@gmail.com

https://doi.org/10.18280/ijsse.151106

Received: 12 October 2025
Revised: 13 November 2025
Accepted: 24 November 2025
Available online: 30 November 2025

Keywords:
Visual Cryptography, thermal imaging, Cipher Block Chaining, Quantum Key Distribution, dope test

ABSTRACT

In this paper, Visual Cryptography (VC) is applied to the thermal images of players acquired in the sports field. The objective of VC is to protect players' information during a dope test done through thermal image analysis. VC transfers the thermal image in secured channel. The thermal image biomarker for a dope test is elevated skin temperature, asymmetrical heat patterns, excessive muscle heat retention, and abnormal recovery thermal signature. However, a major problem is the prevention of thermal images from the data breach, such as privacy violations, and the manipulation of doping assessments. To address the above problems, the player's thermal image is applied with VC with a quantum key algorithm and secures the player's identity. In the proposed method, the tampered thermal image is identified through the abnormal heat distribution in the player's face in the image. Initially, the thermal image is pre-processed using the Adaptive Histogram Equalization (AHE) and denoised using the Gaussian filter. Next, the image is divided into two secret shares, followed by the encryption and decryption process using the proposed Tuned Cipher Block Chaining with Quantum Key Distribution (TCBCQD) technique. The number of shares is decided by the TCBCQD technique. The number of shares is the tuning method in the proposed TCBCQD technique. Cryptographic-based access is done by the anti-doping agencies. The original image is deciphered after combining both the shares, which are available from the higher authorities. The image quality and security metrics were obtained. The proposed TCBCQD technique reconstructs the image with an accuracy rate of 98% and outperforms the existing methodologies.

1. INTRODUCTION

Cryptography has a wide range of applications, in areas such as secure online voting, document verification and validation, medical image security, banking and account transactions, biometric security, scanning QR codes, and image stenography [1, 2]. The usage of digital platforms and applications has increased tremendously in the last decade due to their adaptable and flexible nature [3]. Despite this growth, the integrity of the secure transmission over the internet is still under threat. Due to the increase in cybercrime, safe data transmission is incredibly challenging. Many researchers develop new algorithms for data security and secure data transmission. Traditional cryptographic technique transfers the text data across a secure channel using symmetric and asymmetric keys. Recently, data transfer has been performed using stenography, where the text is embedded into an image. However, security threats such as man-in the middle attack phishing attacks still occur. Distributed Denial of Service (DDoS), eavesdropping, ransomware attacks, and data breaches have emphasized the need of secure transmission model [4, 5].

Encryption is the key process in the cryptographic techniques and protects the integrity of the message. Recently, social applications utilize an end-to-end encryption process and perform safe communication. The symmetric encryption relies on public keys, whereas the asymmetric encryption uses both public and private keys. Symmetric encryption has major problems, such as the key distribution problem, key compromise, and lack of scalability. The above problems are addressed through asymmetric encryption, which requires high computational cost and is vulnerable to cyberattacks. The Visual Cryptography (VC) algorithm solves the security threat by splitting the image into 'n' components for sharing. Even if any of the shares are tampered the attacker cannot be able to view any single clue. The original message is retrieved when shared images are stacked together. This technique has low-complex mathematical calculations and reduces the hardware resource computational cost. During the decryption process, the quality of the encrypted image is low due to the unnecessary pixel expansions [6, 7]. The quality of the decrypted text is affected by the decryption technique. So, it is mandatory to select the optimal steps while decrypting the encrypted shares.

Cryptography maintains the Electronic Health Record (EHR) of patients in the medical field. Symmetric

cryptography algorithms such as Advanced Encryption Standard (AES), Data Encryption Standard (DES), and Triple DES (3DES) are used during the file transfer, messaging, smartcards, and disk encryption [8, 9]. Asymmetric algorithms such as Rivest-Shamir-Adleman (RSA), Elliptic Curve Cryptography (ECC), and Digital Signature Algorithm (DSA) are used in different fields such as email security, key exchange, certificate authorities, Secure Shell (SSH), cryptocurrency wallets, and blockchain security [10]. Recently, hybrid cryptography and quantum cryptography have sought the attention of many researchers because of their functionality and adaptability. The hybrid cryptography combines symmetric and asymmetric keys and guarantees secure communication over the cloud network. The process of bitcoin transaction uses block chaining [11]. Cryptography technique performs less during a security breach. Therefore, the VC has been used due to its adaptability. Table 1 shows the existing secure systems in anti-doping.

1.1 Problem statement

VC is used in secure image transmission [12]. However, the major problem is in the decryption process, while reconstructing the original image [13]. This issue is merely based on the inefficiencies in pixel expansion, which especially occurs in color images, and is addressed by many researchers [14]. For gray-scale and black-and-white images, the interpolation of the pixels is the problem [15]. VC has a simple decryption process and is prone to vulnerability [16]. An alternate method is required for the prevention of image distortion and loss of image quality during the reconstruction phase. Frequently, the anti-doping agencies and sports federation exchanges the testing reports across the different regions. These images are prone to breach and manipulation attacks. Attack occurs during the transmission of the image [17]. RGB images are acquired at sports venues and transmitted to multiple anti-doping authorities for analysis and verification. During the image transfer, vulnerabilities such as unauthorized access, partial data leakage, and tampering are not adequately addressed by conventional single-key encryption methods. In the proposed TCBCQD framework, VC is combined with QKD-assisted encryption. TCBCQB prevents information disclosure from individual shares, ensures secure key exchange, and maintains image integrity during reconstruction.

Table 1. Existing secure systems in anti-doping

Attacks	Method	RGB Biomarkers Targeted	Consequences	World Anti-Doping Agency (WADA) /Anti-Doping Administration & Management System (ADAMS) Gap	Tuned Cipher Block Chaining with Quantum Key Distribution (TCBCQD)+Visual Cryptography (VC) Solutions
Hotspot Manipulation	Pixel editing to normalize skin flushing	Vascular dilation, skin flushing (steroids, stimulants)	False negative: Conceals physiological stress indicators	CoC forms track samples, not pixels	**Number of Pixels Change Rate (NPCR) > 99.6%**: Single-pixel tampering breaks reconstruction
Asymmetry Alteration	Mirror/flip one facial side	Facial asymmetry from injection sites, swelling	Masks unilateral doping effects (local injections)	Images as opaque files in ADAMS	**VC Shares**: Partial reconstruction reveals inconsistencies
Gradient Smoothing	Gaussian blur on sweat/texture patterns	Sweat distribution, skin texture changes	Hides endurance enhancer signatures (sweat suppression)	No pixel-level integrity checks	**98% Pixel Accuracy**: Detects smoothing artifacts
Recovery Signature Erase	Skin tone/color normalization	Skin tone recovery patterns post-exercise	Conceals recovery drug use (skin healing acceleration)	ABP lacks RGB image modules	**Quantum Key Binding**: Session-specific validation
Identity Swap	Face replacement with a clean athlete	Visible face identity swap	False positive: Wrong athlete flagged for doping	ADAMS identity at the file level only	**Dual VC Shares**: Both required for reconstruction
Noise Injection	Add compression artifacts, sensor noise	Cover changes with JPEG artifacts	Undetectable "natural" alterations	No forensic image standards	**Preprocessing Pipeline**: Verifies baseline image profile
Metadata Forgery	Alter EXIF timestamps, camera data	Prove the image taken during a legitimate test	Breaks temporal chain-of-custody	CoC forms are vulnerable to digital forgery	**Quantum Key Distribution (QKD) Session Keys**: Cryptographic timestamp > metadata

1.2 Research gap analysis

Digital communication and cryptography play a vital role in internet technologies during the transfer of image/data/signal [18]. Cryptography is applied in different fields such as banking, biometrics, scanning QR codes, online transactions, and maintaining medical records [19]. Image transmission plays a vital role in sport analytics and is more prone to attacks. Image transmission lacks in image quality, such as pixel distortion, loss of image details with respect to the environmental conditions, and introduces noise and errors [20-23]. The Anti-doping test is a crucial situation in every player's life [24]. During image transfer, authentication and tampering of the image need to be prevented. Moreover, image analytics plays a major role in the dope test. Limitations of Conventional Cryptographic Techniques are the key compromises, scalability, computational overhead, and post-quantum vulnerability. Then the limitations of VC are pixel expansion, loss of visual quality during reconstruction, share management complexity, and susceptibility to noise in image-based applications.

The main contributions of the proposed work:

In prior studies, VC, Cipher Block Chaining (CBC), and QKD have been used independently. The novelty of the

proposed TCBCQD method is the tuned integration of (i) VC-based multi-share generation for thermal facial biometrics, (ii) CBC-based block-level encryption applied to VC shares, and (iii) QKD-generated keys to strengthen authentication and resistance to key compromise. TCBCQD architecture secures thermal images during transmission. Simultaneously, addresses the other problems such as identity privacy, tamper resistance, and reconstruction quality.

1. To design a VC-based framework for thermal facial biomarker based antidoping tests. VC preserves data integrity and supports a robust cryptographic chain of custody for biometric samples, and limits unnecessary exposure of athletes' identities by ensuring that authorized authorities reconstruct the original thermal facial image from encrypted shares.
2. To preprocess the acquired thermal image, Adaptive Histogram Equalization (AHE) is proposed, which avoids image distortion. To enhance the pixel quality of thermal image Gaussian filters are proposed.
3. To strengthen and improve the security level of the proposed model, the CBC method is combined with the Quantum Key Distribution (QKD) algorithm. The shares of the VC are encrypted and decrypted using the proposed TCBCQD technique.
4. To estimate the quality of the reconstructed thermal image, statistical parameters such as Peak Signal to Noise Ratio (PSNR), Structure Similarity Index Measure (SSIM), accuracy rate, Number of Pixels Change Rate (NPCR), and Unified Average Changed Intensity (UACI) are obtained.

This research article is partitioned into five different sections. Section 1 provides a brief introduction to VC. A detailed literature survey of VC is discussed in Section 2. Section 3 describes the overall flow of the proposed methodology. The experimental analysis with appropriate justifications is discussed in Sections 4 and 5. Finally, the conclusion is in Section 6.

2. LITERATURE SURVEY

Cryptography algorithms such as RSA and AES are used for encrypting messages. Later, advanced cryptographic algorithms such as hash and SHA algorithms were used in encryption.

2.1 Visual Cryptography

The traditional cryptographic techniques have complex mathematical calculations for transferring data securely over the network. Image transfer requires high time and space complexity. To transfer an image, a simple technique for encrypting images using 'n' shares is used. VC technique can be performed on the RGB-color channels, thermal images, and gray scaled image for encryption. The gray-scaled image is securely transmitted using the AES algorithm [25]. Hash functions, secret keys, and symmetric algorithms are combined randomly for the encryption of the image. The VC technique transforms the gray-scale image into a binary image using a half-toning process [26]. In this technique, the images are broken down into a series of dots initially and finally reproduced by the continuous dot patterns. For the received image, PSNR is used for the prediction of the noise level. It compares the quality of the reconstructed image with the original transmitted gray scale image with PSNR values, which range between 30 – 34 dB. The Cheating Prevention – Visual Cryptographic (CP – VC) method analyzes pixel attacks using the polynomial interpolation technique at the reconstruction phase. The above algorithm is applied in the USC-SIPI database, which comprises monochrome images, color images, and multispectral images [27]. The method detects the cheating attacks with an accuracy rate of 97% with 3% false positive rate. The random images from the Columbia Object Image Library (COIL) dataset are selected and encrypted using the XOR operation. Gray-scale images are selected from the Extended Yale Face Database (EYFD) and encrypted using the Progressive Visual Cryptography (PVC) method by Ibrahim et al. [28]. The pixel variations are observed by calculating the PSNR value, which ranges between 31 and 32 dB, and the SSIM value is around 0.85.

2.2 Applications of Visual Cryptography

The VC is applied in the medical field for securing medical images such as X-rays, CT scans, and X-ray images. The NIH Chest X-ray database is encrypted using a reversible data hiding-based VC technique by Ahmad et al. [29]. The recovered image has a PSNR value ranging between 35 and 45 dB. The color cryptography is combined with the stenography technique to encrypt the 500 images chosen from the COCO dataset [30]. The PSNR range between the original and stenographic image is nearly 35-37 dB. To improve the security, shares are encrypted at multiple layers in the images of the MIT CBCL Face Database. The Multi-Secret Sharing Visual Cryptography (MSS-VCS) technique encrypts the ImageNet dataset with an accuracy rate of 96% [31]. RGB images are applied with VC, and the decrypted images have distortion, pixel expansion, and noise intervention. The RGB images are replaced with thermal images. Thermal images have high image quality with less noise intervention at the reconstruction phase. VC secures the thermal images better than RGB images. Still, the vulnerability is a major problem need to be addressed. Researchers have explored many combination algorithms and techniques to solve the above problem [32]. The image attacks are prevented by integrating VC with advanced encryption techniques such as AES, DES, and hash values. The combination method strengthens the security and has limitations such as space and time complexity [33]. The use of quantum computing with VC has paved the new dimension to cryptographic. Security threats are tackled by the quantum-resistant encryption algorithms that compress and scramble the images [34].

With reference to the above literature survey, hybrid cryptographic algorithms provide secure communication irrespective of different applications such as medical, military, banks, security, and monitoring. The significant parameters, such as complexity, scalability, and resources, need to be addressed. Table 2 shows the methods in the proposed system to solve the existing problems.

3. PROPOSED SYSTEM

Thermal images provide body temperature and cannot be tampered with easily. The image is divided into two shares, which can be varied up to 'n' shares depending on the application areas. Each share is unique and doesn't expose even a minute detail regarding the original thermal image.

Once the shares are divided, they are transformed to the receiver side through the cryptographic encryption and decryption process. The traditional cryptographic techniques are very complex and require ticket verification from a third party. The TCBCQD framework proposed model has less computational complexity, prevents security threats, and visual distortion due to the pixel expansion and interpolation. The proposed TCBCQD framework is a hybrid method. TCBCQD is a quantum-assisted security model. QKD is simulated at the algorithmic level and generates a shared secret key, and classical AES in CBC mode is used for efficient block-level encryption of VC shares. QKD evaluates the security impact of quantum-resistant key generation within a classical communication environment. The QKD-generated secret key is pre-shared securely between the sender and the authorized anti-doping agency through an offline or trusted initialization phase. The key is not transmitted over the public channel. Secure storage is within trusted anti-doping authority infrastructure and prevents cryptographic threat models.

Table 2. Proposed TCBCQD+Visual Cryptography (VC) solves the existing problems

Problems	Biometric/Thermal Impact	Tuned Cipher Block Chaining with Quantum Key Distribution (TCBCQD)+Visual Cryptography (VC) Solution
Pixel Expansion	Distorts thermal gradients, doping biomarkers	**Thermal-Optimized VC** + Adaptive Histogram Equalization (AHE) preprocessing minimizes expansion impact
Key Management	Chain-of-custody breach risk	**Quantum Key Distribution** eliminates third-party vulnerabilities
Computational Overhead	Field deployment delays	**Tuned CBC Mode** reduces overhead vs. stacked ciphers
Tamper Sensitivity	Falsified doping results	**High Number of Pixels Change Rate (NPCR)/Unified Average Changed Intensity (UACI)** ensures single-block detection
Identity Leakage	World Anti-Doping Agency (WADA) anonymization violation	**Visual Cryptography (VC) Shares** reveal no identity individually
Noise Amplification	Lost temperature biomarkers	**AHE+Gaussian Preprocessing** enhances SNR before encryption
Modal Degradation	Muscle heat retention markers lost	**Thermal-Specific Pipeline** preserves low-frequency data
Chain-of-Custody	Anti-Doping Administration & Management System (ADAMS) integration gap	**Quantum Keys + VC Binding** proves unaltered transit

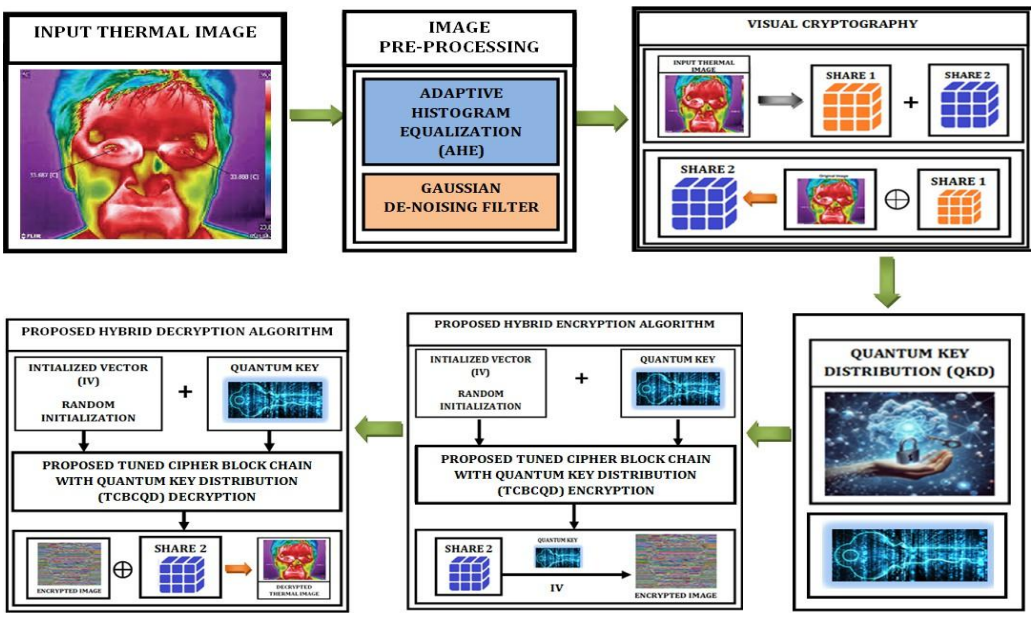


Figure 1. Overall architecture of the proposed Tuned Cipher Block Chaining with Quantum Key Distribution (TCBCQD) method

3.1 Workflow

The overall architecture of the proposed model is depicted in Figure 1. The input thermal image of size 224 × 224 is of 3-dimensional data and saved as an array of blocks. A multidimensional data array in image processing needs more space and time complexity. To overcome this problem, n-dimensional data is scaled up to the range of '0' to '255' using the unit8 operation in MATLAB. A total of 150 images is collected from the Kaggle sports dataset for different sports such as cricket, hockey, golf, and athletics [22]. The 100 images are used for training the TCBCQD proposed model, and 50 images are used for testing. Thermal images are generated using the Pix2Pix image augmentation method. The noise in the image degrades the image quality, normalized by using the AHE and then denoised using the Gaussian filter.

A thermal image has three color channels, such as Red, Green, and Blue. The respective pixel values are calculated in n-dimensional array space. In a thermal image, the extremely hot regions are denoted in red color, the extremely cool regions are denoted in blue color, and the moderate region represents the green, as shown in Figure 2. The corresponding histogram of the thermal image is shown in Figure 3. The input thermal images are applied with proposed algorithms such as AHE and

Gaussian filters. The AHE method equalizes the unevenly distributed pixels and improves the quality of the image. The presence of noise in the image is due to the environmental temperature, lighting condition and device calibration noise. The unwanted pixels are filtered using the Gaussian filter. The thermal image is enhanced for the encryption process. The pixel variations between the original and pre-processed images are observed through histograms and plotted in Figure 4. From histogram analysis, pixels are distributed evenly in the pre-processed image rather than the original image.

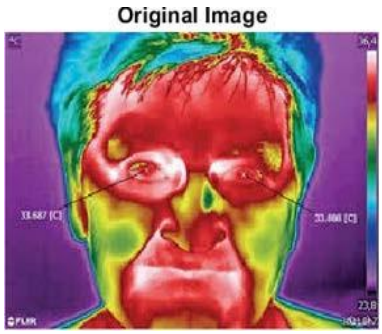


Figure 2. Input thermal image

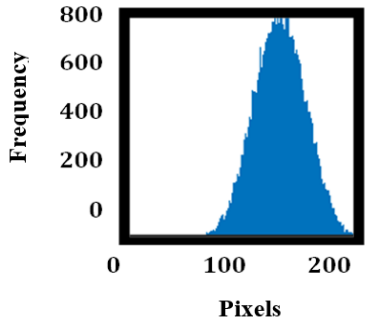


Figure 3. Histogram of thermal image

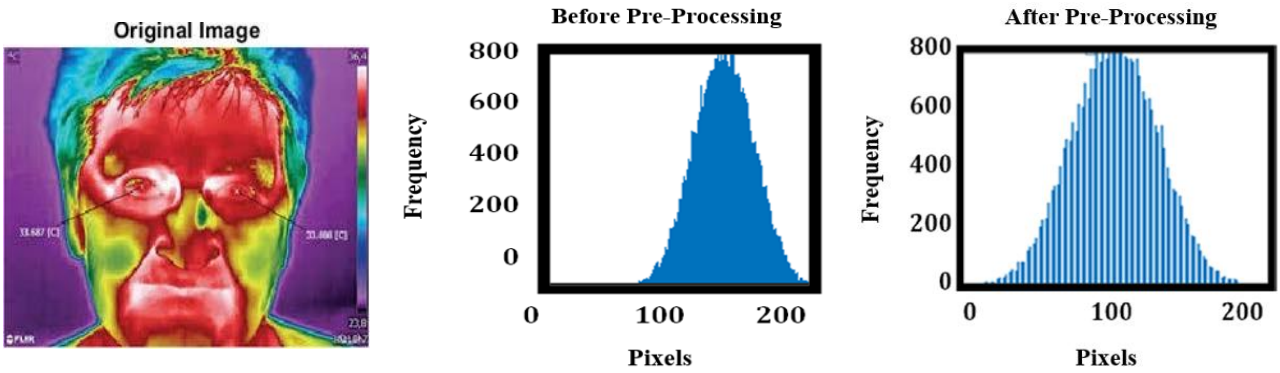


Figure 4. Histogram comparison of thermal image before and after the pre-processing step

In the proposed method, each pixel of the image is reconstructed of 8-bit size by the XOR operation and stored in Share 2 as an array matrix as in Eq. (1).

$$\text{Share 2}=\text{ORIGINAL IMAGE} \oplus \text{Share 1} \quad (1)$$

Share 1 is a randomly initialized 8-bit array matrix similar to the input thermal image size, and it is scaled between the values 0 – 255. Share 2 is a zero matrix, which is initialized similarly to the size of the input image. Next, Share 2 value is assigned by using the bitwise XOR operation between the original image and Share 1. To improve the security, a secret key is proposed in this paper using the QKD method. The traditional QKD algorithm is utilized and generates a random key of size equal to the input image. In order to reduce the calculation complexity, the values of the quantum key matrix are summed up to three-digit values and initialized as the secret key in the main code. The CBC operation takes place with two predominant factors, such as the Initialization Vector (IV) and the quantum key. In each block, the corresponding image block is encrypted using the quantum key and randomly initializes the vector. The series of blocks is interconnected by the chaining process; the current block is encrypted using the previous encrypted block. Since the first block has no prior block, the IV is considered as the previous block.

3.2 Encryption and decryption: Tuned Cipher Block Chaining with Quantum Key Distribution

CBC interlinks the ‘n’ number of blocks of thermal image and ensures the security while transferring it to the receiver. Each image pixels are calculated with a bitwise XOR operation with the previous ciphertext blocks and IV. IV and Quantum keys are the prerequisite factors in the proposed TCBCQD method. However, the initial cipher block does not have any previous cipher text block to perform the XOR operation. In order to address this problem, a randomly initialized vector of size equal to the input thermal image is generated.

The input thermal image and Share 1 are subjected to the XOR operation. The bitwise XOR operation is performed for each color channel exclusively, and the values are stored in Share 2. IV is specific and randomly generated for each cipher block during the encryption process. This prevents the pattern discovery and provides secure communication. The workflow of the proposed encryption model is shown in Figure 5. IV is initialized as the previous block, and the CBC encryption process is carried out as in Figure 5 using the AES. This proposed model contains 128-bit blocks based on the input thermal image size of 224 × 224 pixels. The input thermal image is divided into 3,134 blocks of 128 bits. Each pixel comprises 8 bits, with 16 pixels per block. The obtained resultant matrix is subjected to an XOR operation with the respective quantum key. The final encrypted matrix values are stored in block 1. This matrix is used for chaining the subsequent block 2. This process is continued for ‘n’ number of blocks to link all the initialized blocks with image shares as shown in Figures 6 and 7. The shares are represented by random pixels of noise, which don’t disclose any information.

After the series of encryption processes, the final encrypted

block is obtained. This block is visually represented as noise grains, and the valid information contained in that block and not disclosed. Each share has distinct random patterns. This is an added advantage. In this paper, the share count is set to '2', so the input thermal image is divided into '2' shares. The original image is reconstructed with the necessary shares, quantum key, and ordered encrypted matrix. Therefore, it is not possible for the attackers to retrieve meaningful information from the communication channel. Similar to the encryption process, the CBC decryption process has a series of steps to retrieve the original input thermal image. Initially, the encrypted previous block is initialized as the IV. Each element of the encrypted matrix undergoes an XOR operation with the corresponding quantum key available between the sender and receiver. Next, the original XOR matrix is subjected to an XOR operation with the IV to recover the exact pixel of the input thermal image. The decryption process occurs in series manner, until the input thermal image is obtained. The decrypted image is identical to the original input thermal image and is shown in Figure 8. The performance of the proposed model is compared for visible, thermal, and gray-scaled images and shown in Figure 9. The input to the proposed model is varied, and the patterns of the encrypted image are analyzed. It is evident that the final encrypted image has unrecognizable pixels, which ensures security.

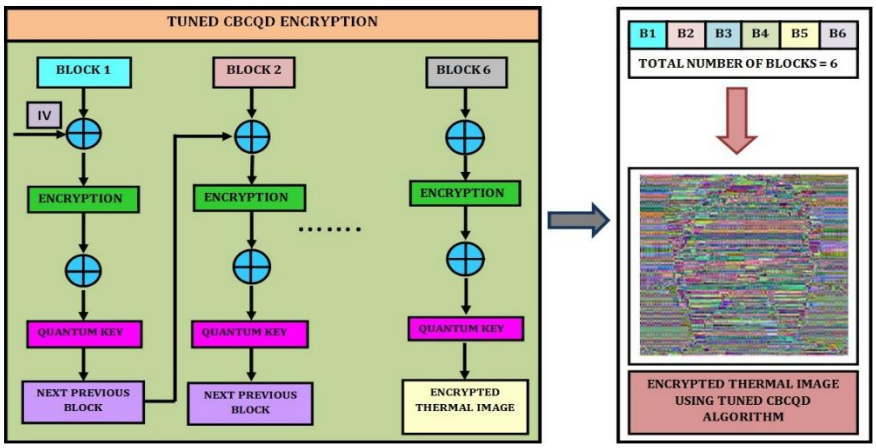


Figure 5. Encrypting thermal image using the proposed Tuned Cipher Block Chaining with Quantum Key Distribution (TCBCQD)

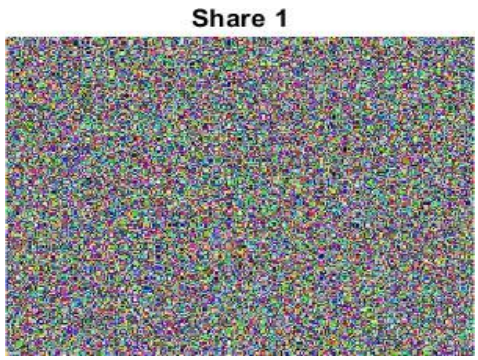


Figure 6. Visual Cryptography (VC) based generated Share 1

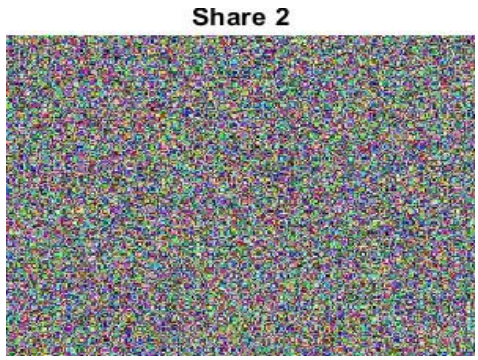


Figure 7. Visual Cryptography (VC) based generated Share 2

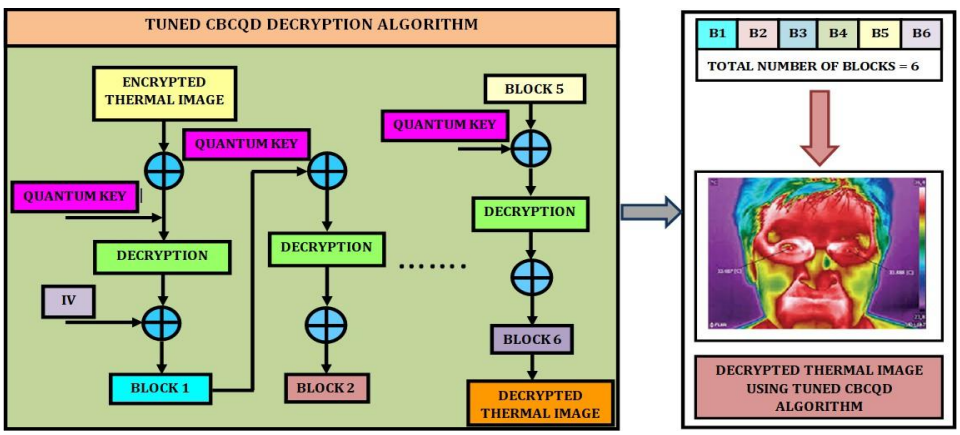


Figure 8. Decrypting thermal image using the proposed Tuned Cipher Block Chaining with Quantum Key Distribution (TCBCQD)

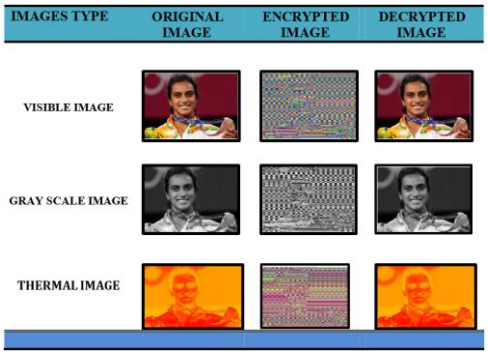


Figure 9. Performance comparison of different image types using the proposed Tuned Cipher Block Chaining with Quantum Key Distribution (TCBCQD)

4. EXPERIMENTAL RESULT ANALYSIS

4.1 Peak Signal to Noise Ratio

PSNR calculates the absolute difference in pixel intensities between the reconstructed image and original thermal image as in Eq. (2). It predicts the amount of the distortion level in the reconstructed image. This logarithmic unit of measurement is expressed in terms of decibels (dB). The high PSNR value indicates good image quality, and the low PSNR value indicates low image quality. For a good quality of image, the PSNR value is in the range of 30 to 50 dB.

$$PSNR = 11 * \log\left(\frac{MAM^2}{MSE}\right) \quad (2)$$

- *MAMMI* is the maximum possible pixel value (255 for an 8-bit image) of the input image.
- *MSE* is the Mean Squared Error between the original and distorted images.

4.2 Mean Square Error

MSE is calculated by averaging the differences between pixel values of the original and the reconstructed images as in Eq. (3). The MSE value measures overall error in pixel values of the reconstructed image.

$$MSE = \left(\frac{1}{mn}\right) * sum\Big(from\ i = 0\ to\ m - 1, sum\Big(from\ j = 0\ to\ n - 1, \big(I(i,j) - K(i,j)\big)^2\Big)\Big) \quad (3)$$

where, $I(i, jj)$ and $K(i, jj)$ represent the pixel values at i[th] and j[th] position of the compressed and original image.

4.3 Structural Similarity Index

The SSIM measures the perceived similarity between the restructured image and the original thermal image, similar to how human eyes. This metric focuses on perceivable information from thermal images, such as luminance (brightness), contrast (variance), and structure (texture). The SSIM index ranges between the values '0' to '1'. The SSIM between the original image (x) and reconstructed image (y) is calculated using the formula as in Eq. (4).

$$SSIM(x,y) = \frac{(2 * mu_x * mu_y + C_1) * (2 * \sigma_{xy} + C_2)}{(mu_x^2 + mu_y^2 + C_1) * (\sigma_x^2 + \sigma_y^2 + C_2)} \quad (4)$$

- μ_x, μ_y is average intensities of x and y;
- σ_x^2, σ_y^2 are the variances of images x and y;
- σ_{xy} is the covariance between original (x) and reconstructed image (y);
- C_1, C_2 are small constants that avoid division by zero.

The strength of the encryption algorithm is analyzed with metrics such as Number of Pixels Change Rate (NPCR) and Unified Average Changing Intensity (UACI). The pixel variations between the original and the encrypted image are compared using NPCR and calculated as in Eq. (5).

$$NPCR = \left(\frac{sum\Big(from\ i = 1\ to\ M, sum\big(from\ j = 1\ to\ N, D(i,j)\big)\Big)}{M * N}\right) * 100\% \quad (5)$$

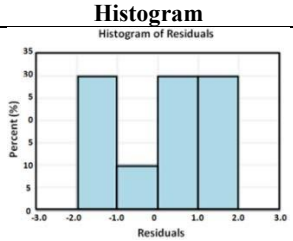
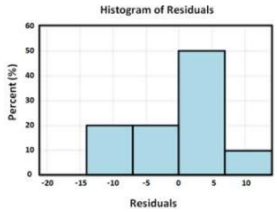
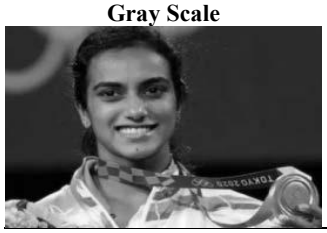
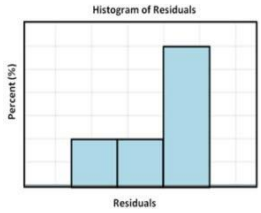
The dimensions of the images are represented as 'M' and 'N'. The binary function $D(i, jj)$ comprises the pixel values of the encrypted and original image. A higher NPCR value has a strong diffusion property and propagates even a small alteration in the input image. The average intensity change between the two encrypted images is computed.

The absolute difference between two images is compared and ensures the robustness of the encryption process. The performance of the proposed system is scrutinized by the above-mentioned metrics, and their corresponding results are tabulated in Table 3.

The thermal image has the highest PSNR value, i.e., 38.56 dB, when compared to the other images. PSNR is high, and minute details of the object are preserved effectively in thermal images. Gray-scale images have the second-highest PSNR value of 35.78 dB, and the visible image has 33.12 dB. The gray-scaled image has intensity values for the reconstructed image. RGB images have to be tracked on multiple channels, comparing the gray-scaled image. Even if one channel is affected, the entire reconstruction phase has high noise.

For the MSE metric, gray scale images have the lowest score of 15.92, and thermal image has moderate score of 18.25. The variation of this score is based on the structural information of the images. The gray-scale image has one channel, and three channels for the thermal and visible images. Though a thermal image has three channels, there is no loss of details in the image during the reconstruction or decryption process. In contrast, the visible images cannot be able to decrypt the images effectively without any loss. Therefore, the visible images have the highest MSE score of 20.48. Similarly, the SSIM value of thermal is high when compared to the visible and gray scale images. From Table 1, the SSIM values of thermal, gray scale, and visible are 0.910, 0.869, and 0.796, respectively.

Table 3. Performance analysis of the proposed method

Image Type	Histogram	PSNR (dB)	MSE	SSIM (0-1)
Thermal 		38.56	18.25	0.910
Visible 		33.12	20.48	0.796
Gray Scale 		35.78	15.92	0.869

Note: Peak Signal to Noise Ratio (PSNR); Mean Square Error (MSE); Structure Similarity Index Measure (SSIM).

Further, the proposed TCBCQD method is validated using metrics such as accuracy, precision, recall, and F1-score. Eq. (6) shows the accuracy calculation.

$$Accuracy = \frac{TP + TN}{TP + TN + FP + FN} \tag{6}$$

The precision identifies the true positives among all the positive predictions as in Eq. (7).

$$Precision = \frac{TP}{TP + FP} \tag{7}$$

Recall predicts the true positive values among the correctly predicted values as in Eq. (8).

$$Recall = \frac{TP}{TP + FN} \tag{8}$$

The precision and recall values are balanced by the F1-score. It is mathematically calculated as in Eq (9).

$$F1 - Score = 2 * \frac{Precision * Recall}{Precision + Recall} \tag{9}$$

A random selection of 5 different sets of facial images is selected for three different image data types. The precision is shown in Figure 10. Recall is shown in Figure 11, and F1-score is shown in Figure 12.

From these figures, it is observed that thermal images have better scores when compared to visible and gray-scale images. Thermal images retain low-frequency information in the images. Gray-scale images have scores equal to thermal images, slightly lower than thermal images. This is due to the pixel distortion and noise due to external interferences such as lighting conditions, fog, smoke, etc. It is evident that the thermal image has good PSNR, MSE, and SSIM values when compared to the gray-scale image and visible image.

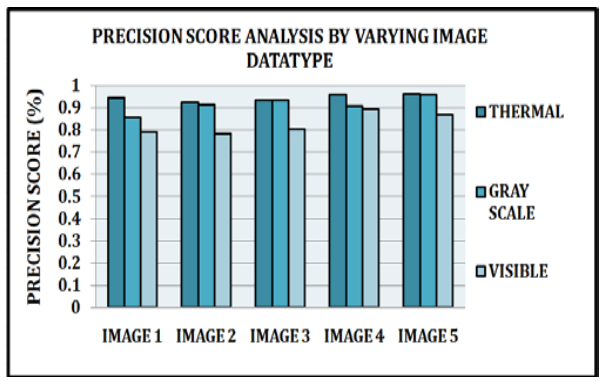


Figure 10. Precision score analysis of the proposed Tuned Cipher Block Chaining with Quantum Key Distribution (TCBCQD) model by varying image data type

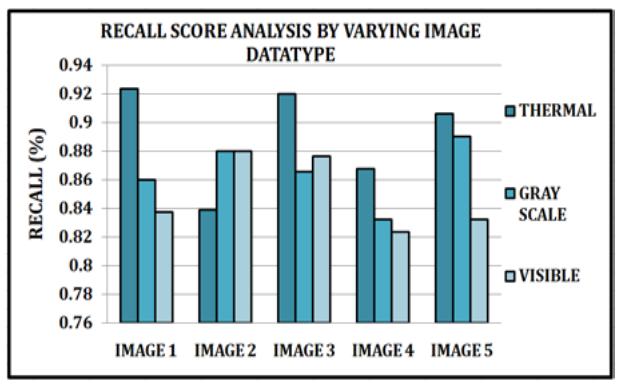


Figure 11. Recall score analysis of the proposed Tuned Cipher Block Chaining with Quantum Key Distribution (TCBCQD) model by varying image data type

In addition, the time complexity is measured for the proposed TCBCQD method. Gray-scale images have fewer structural parameters, and the time taken to decrypt the gray-scale image is less compared to the thermal image. However, it differs drastically from a visible image as every channel are consideration. The time taken to decrypt thermal, visible, and gray scale image using the proposed TCBCQD method is tabulated in Table 4.

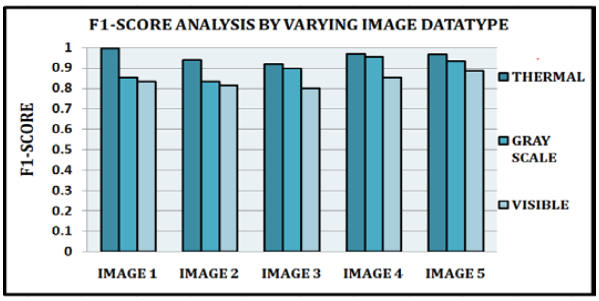


Figure 12. F1-score analysis of the proposed Tuned Cipher Block Chaining with Quantum Key Distribution (TCBCQD) model by varying image data type

Table 4. Time analysis for the encryption process

Algorithms	Image Datatype	Time in Seconds
Traditional ECC Encryption [16]	Visible	1.72
Traditional ECC Encryption [16]	Thermal	1.52
Traditional ECC Encryption [16]	Gray Scale	1.51
Traditional AES Encryption [18]	Visible	1.56
Traditional AES Encryption [18]	Thermal	1.67
Traditional AES Encryption [18]	Gray Scale	1.57
Proposed Tuned CBCQD Encryption	Visible	1.35
Proposed Tuned CBCQD Encryption	Thermal	1.18
Proposed Tuned CBCQD Encryption	Gray Scale	1.17

Note: Elliptic Curve Cryptography (ECC); Advanced Encryption Standard (AES); Tuned Cipher Block Chaining with Quantum Key Distribution (TCBCQD).

Table 5. Time analysis for the decryption process

Algorithms	Image Datatype	Time in Seconds
Traditional ECC Decryption [16]	Visible	0.48
Traditional ECC Decryption [16]	Thermal	0.45
Traditional ECC Decryption [16]	Gray Scale	0.46
Traditional AES Decryption [18]	Visible	0.44
Traditional AES Decryption [18]	Thermal	0.41
Traditional AES Decryption [18]	Gray Scale	0.40
Proposed Tuned CBCQD Decryption	Visible	0.33
Proposed Tuned CBCQD Decryption	Thermal	0.25
Proposed Tuned CBCQD Decryption	Gray Scale	0.25

Note: Elliptic Curve Cryptography (ECC); Advanced Encryption Standard (AES); Tuned Cipher Block Chaining with Quantum Key Distribution (TCBCQD).

Comparing Table 4 and Table 5, it is observed that the encryption process consumes more time than the decryption process. The encryption process includes complex steps such as randomization and transformation of the pixels into corresponding shares. Whereas the decryption process is simple, which stacks the shares together to retrieve the decrypted image. During encryption and decryption, the visible image has the highest execution time because of the 3 color channels. More data needs to be processed for 8-bit per channel and a total of 24-bit depth data. Therefore, the visible images have a higher execution time than the thermal and gray scale.

4.4 Ablation study

Initially, the proposed TCBCQD model is validated with a thermal image. The robustness of the thermal image is compared with the visible image and gray scale image. In addition, the number of shares is tuned to find any changes in the overall performance of the proposed TCBCQD model. This study helps in error diagnosis, optimization, and trade of analysis. Additionally, the proposed TCBCQD model is compared with the existing traditional VC techniques.

Table 6. Comparing the accuracy rate of the algorithms by tuning the shares of Visual Cryptography (VC)

Algorithms	Image Datatype	Share 2 Accuracy (%)	Share 4 Accuracy (%)
Traditional ECC [16]	Visible	87	85
Traditional ECC [16]	Thermal	90	89.8
Traditional ECC [16]	Gray Scale	92.4	93
Traditional AES [18]	Visible	88	84
Traditional AES [18]	Thermal	91.5	90
Traditional AES [18]	Gray Scale	92	92
Proposed Tuned CBCQD	Visible	92	91.5
Proposed Tuned CBCQD	Thermal	97.5	95.9
Proposed Tuned CBCQD	Gray Scale	96	95.6

Note: Elliptic Curve Cryptography (ECC); Advanced Encryption Standard (AES); Tuned Cipher Block Chaining with Quantum Key Distribution (TCBCQD).

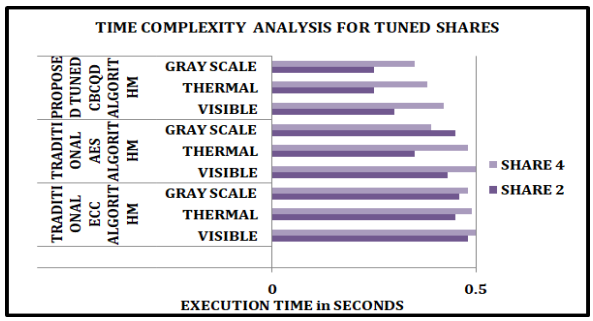


Figure 13. Time complexity analysis of the models by tuning shares

It is observed that the accuracy rate of Share 2 and Share 4 is nearly close enough, as shown in Table 6. Since there is no major deviation in the accuracy rate between the two shares, Share 2 is selected to avoid unnecessary complexities. The time taken to encrypt and decrypt using the proposed TCBCQD method is plotted as a bar chart in Figure 13. To validate the proposed TCBCQD model's performance, it is

compared with the existing ECC [16] and AES [18] algorithms. From the bar chart, it is witnessed that the proposed model takes less execution time of 0.3534s approximately. Secondly, the gray-scale images are executed in 0.3576s approximately. Finally, the gray-scale image has the highest execution time of around 0.505s. Comparing Share 2 and Share 4, Share 2 has the lowest execution time due to fewer computational processes. Hence, Share 2 is selected for this proposed TCBCQD method. Table 7 shows the statistical comparison of the TCBCQD proposed and the existing methodologies.

The overall accuracy rate of the proposed TCBCQD method is compared with the existing method and shown in Figure 14. The traditional ECC algorithms have an accuracy rate ranging between 89% to 90% for all three types of images. Similarly, the traditional AES algorithm ranges between 85% to 90% approximately. The TCBCQD proposed algorithm achieves an accuracy rate ranging closely between 94% to 98%. The accuracy rate of ECC and AES is low, compared to the VC, because of high noise signals. This is justified through the SSIM values and shown in Figure 15. MSE is shown in Figure 16. PSNR is shown in Figure 17. The low PSNR value indicates the presence of annoying signals due to environmental lighting conditions and pixel distortions.

Table 7. Statistical comparison of the proposed and the existing methodologies

Cryptography Algorithms	Image Type	PSNR	MSE	SSIM	Accuracy (%)
Traditional ECC Algorithm [16]	Thermal	33.12	15.92	0.765	89.5
Traditional ECC Algorithm [16]	Visible	33.02	16.45	0.825	86.6
Traditional ECC Algorithm [16]	Gray Scale	32.08	14.34	0.899	85.7
Traditional AES Algorithm [18]	Thermal	35.67	20.48	0.841	90.5
Traditional AES Algorithm [18]	Visible	34.25	19.76	0.675	85.4
Traditional AES Algorithm [18]	Gray Scale	36.34	17.63	0.897	89.8
Proposed Tuned CBCQD Algorithm	Thermal	40.56	13.04	0.986	97.6
Proposed Tuned CBCQD Algorithm	Visible	36.76	14.63	0.867	93.5
Proposed Tuned CBCQD Algorithm	Gray Scale	39.87	13.67	0.902	94.3

Note: Peak Signal to Noise Ratio (PSNR); Structure Similarity Index Measure (SSIM); Mean Square Error (MSE); Elliptic Curve Cryptography (ECC); Advanced Encryption Standard (AES); Tuned Cipher Block Chaining with Quantum Key Distribution (TCBCQD).

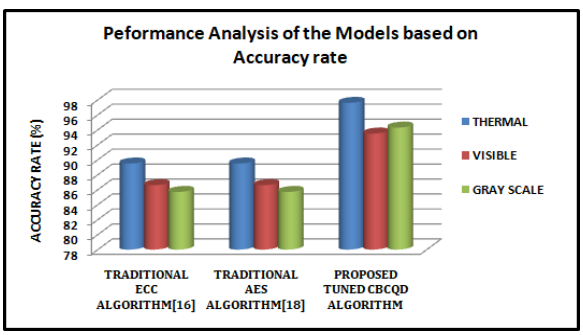


Figure 14. Performance analysis of the models based on the accuracy rate

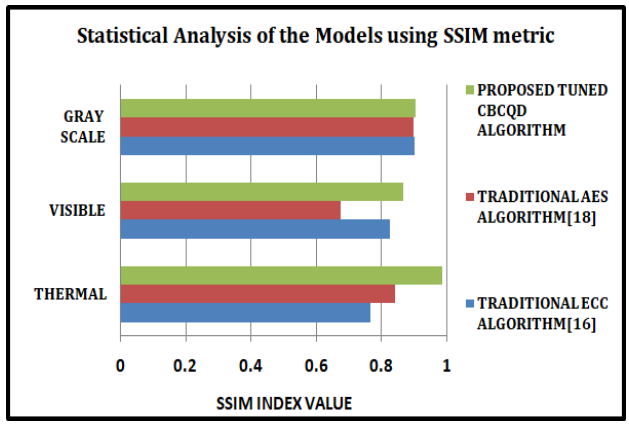


Figure 15. Statistical measure of the models using the Structure Similarity Index Measure (SSIM) metric

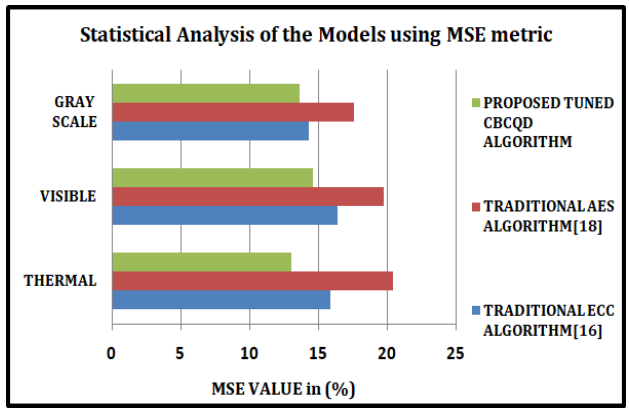


Figure 16. Statistical measure of the models using the Mean Square Error (MSE) metric

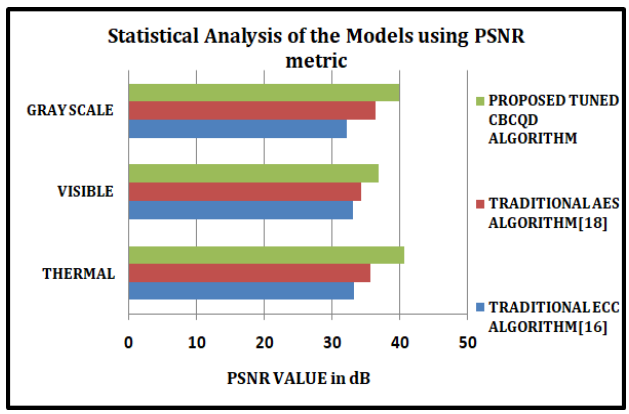


Figure 17. Statistical measure of the models using the Peak Signal to Noise Ratio (PSNR) metric

5. DISCUSSION

The accuracy rate of the proposed TCBCQD method surpasses that of the traditional algorithms, as shown in Table 6 and Figure 12. Thermal camera acquires all details of images, irrespective of environmental conditions such as smoke, fog, rain, low light, or ambience. So, thermal images have precise details with good image quality, which is mandatory for the effective decryption or reconstruction process. The traditional algorithms have a more complex process, which leads to high time and space complexity.

Security and integrity of traditional algorithms are compromised due to third-party key exchange. To overcome all these issues, the proposed TCBCQD method is tuned in such a way that it combines the quantum key and cipher block chaining concept with VC. Furthermore, ECC and AES algorithms are of with high computational overhead and utilization of resources, when comparing VC. However, the proposed TCBCQD method has a good accuracy rate because thermal image has less distortion. The proposed TCBCQD method utilizes the quantum key, and the security is strengthened to a higher level without compromising the time complexity. Therefore, the proposed TCBCQD method has a high accuracy rate of around 98%. Table 8 shows a comparison of the proposed TCBCQD and existing methods.

Table 9 shows tampering sensitivity analysis, and Table 10 shows Share-2 vs. Share-4: Proposed TCBCQD+VC analysis. Table 11 shows proposed method advantages (TCBCQD+VC Share-2).

Table 8. Comparison of Tuned Cipher Block Chaining with Quantum Key Distribution (TCBCQD) with the proposed and existing methods

Method	PSNR (dB)	SSIM	Reconstruction Accuracy (%)	Pixel Expansion Ratio	Computational Time (s)	NPCR (%)	UACI (%)
Traditional AES	28.4 ± 1.2	0.82 ± 0.03	89.2 ± 2.1	1.0x (no VC)	3.45 ± 0.23	99.2 ± 0.4	33.1 ± 0.8
Traditional ECC	27.8 ± 1.5	0.79 ± 0.04	87.6 ± 2.4	1.0x (no VC)	4.12 ± 0.31	98.7 ± 0.5	32.8 ± 1.0
FSM-based VCS	32.1 ± 1.1	0.88 ± 0.02	92.4 ± 1.8	2.25x	1.89 ± 0.15	99.4 ± 0.3	33.5 ± 0.6
QR-based VCS	31.7 ± 1.3	0.86 ± 0.03	91.8 ± 2.0	2.0x	2.34 ± 0.18	99.1 ± 0.4	33.2 ± 0.7
Proposed TCBCQD	**35.8 ± 0.9**	**0.95 ± 0.01**	**98.1 ± 0.7**	**1.8x**	**1.67 ± 0.12**	**99.7 ± 0.2**	**34.2 ± 0.4**

Note: Peak Signal to Noise Ratio (PSNR); Structure Similarity Index Measure (SSIM); Number of Pixels Change Rate (NPCR); Unified Average Changed Intensity (UACI); Advanced Encryption Standard (AES); Visual Cryptography (VC); Elliptic Curve Cryptography (ECC); Tuned Cipher Block Chaining with Quantum Key Distribution (TCBCQD).

Table 9. Tampering sensitivity analysis

Tamper Type	Thermal Images			RGB Images		
	NPCR (%)	UACI (%)	Recon. Error (%)	NPCR (%)	UACI (%)	Recon. Error (%)
Single Pixel	**99.8**	**34.5**	**12.3**	98.9	33.1	8.7
1% Block	**99.7**	**34.1**	**15.8**	99.2	33.6	11.2
5% Block	**99.6**	**33.9**	**28.4**	99.1	33.4	19.6
Gradient Smooth	**99.9**	**34.7**	**22.1**	99.3	33.8	14.3

Note: Number of Pixels Change Rate (NPCR); Unified Average Changed Intensity (UACI).

Table 10. Share-2 vs. Share-4: Proposed TCBCQD+VC analysis

Aspect	Share-2 (Proposed Optimal)	Share-4 Configuration	Performance Impact
Pixel Distribution	Information is split across 2 independent shares	Distributed across 4 independent shares	Share-4: Higher pixel expansion (2.8x vs 1.8x)
Reconstruction Process	Simple stacking + TCBCQD decryption	Complex multi-share stacking + decryption	Share-4: Accumulated quantization noise, alignment errors
PSNR (dB)	35.8 ± 0.9	33.2 ± 1.2	-2.6 dB degradation in Share-4
SSIM	0.95 ± 0.01	0.89 ± 0.03	-0.06 drop due to interpolation complexity
Reconstruction Accuracy (%)	98.1 ± 0.7	94.3 ± 1.4	-3.8% from multi-channel distortion
Security (Theoretical)	High (both shares + quantum key required)	Higher redundancy	Share-2: Optimal practical security
Computational Overhead	1.67 ± 0.12s	2.45 ± 0.21s	+47% time increase in Share-4
NPCR/UACI	99.7% / 34.2%	99.5% / 33.8%	Share-2 superior tamper sensitivity

Note: Tuned Cipher Block Chaining with Quantum Key Distribution (TCBCQD); Visual Cryptography (VC); Peak Signal to Noise Ratio (PSNR); Structure Similarity Index Measure (SSIM); Number of Pixels Change Rate (NPCR); Unified Average Changed Intensity (UACI).

Table 11. Proposed method advantages (TCBCQD+VC Share-2)

Encryption Property	TCBCQD+VC Mechanism	Impact on Image Quality	Quantitative Evidence
CBC Diffusion Strength	Block chaining with quantum keys	Enhances VC share randomness	NPCR 99.7% vs AES 99.2%
Pixel Expansion Control	Tuned VC parameters (Share-2)	Reduces interpolation artifacts	1.8x vs Share-4 2.8x
Chaining Overhead	Optimized CBC mode	Minimizes reconstruction delay	45% faster than stacked ciphers
Thermal Optimization	AHE+Gaussian preprocessing	Preserves biomarker fidelity	PSNR +3.7 dB vs VC baselines

Note: Tuned Cipher Block Chaining with Quantum Key Distribution (TCBCQD); Visual Cryptography (VC); Number of Pixels Change Rate (NPCR); Advanced Encryption Standard (AES); Adaptive Histogram Equalization (AHE); Peak Signal to Noise Ratio (PSNR).

6. CONCLUSIONS

The VC is an ideal solution for achieving security without compromising the player's identity. Though the traditional VC algorithm has no key management scheme, there is a possibility of vulnerable attacks. To tackle this problem, the proposed TCBCQD method combines the CBC and quantum key distribution (QD) technique. Evaluating the different existing methodologies, it is identified that there is computational overhead in the cryptography process due to the distortion of images. Thermal images are acquired with the radiation emitted by the particular sports player, and if any malfunctions occur, it is easily spotted with the variations in the temperature range. The introduction of a shared quantum key ensures the authentication in the proposed TCBCQD method. Even if a single block is tampered; the attacker cannot be able to visualize the image content. The accuracy rate of the proposed TCBCQD method is 98% approximately. This proposed model provides a better image cryptographic solution and ensures security without any compromise. Therefore, authorized anti-doping agencies securely reconstruct and access the identity using the required VC shares and QKD-assisted keys. In future work, this research will be extended for EHR, medical images for transmission in hospital and to prevent data breaches.

REFERENCES

[1] Kalubandi, V.K.P., Vaddi, H., Ramineni, V., Loganathan, A. (2016). A novel image encryption algorithm using AES and Visual Cryptography. In 2016 2nd International Conference on Next Generation Computing Technologies (NGCT), Dehradun, India, pp. 808-813. https://doi.org/10.1109/NGCT.2016.7877521

[2] Khan, P.W., Byun, Y. (2020). A blockchain-based secure image encryption scheme for the industrial Internet of Things. Entropy, 22(2): 175. https://doi.org/10.3390/e22020175

[3] Shakhmetova, G., Barlybayev, A., Saukhanova, Z., Sharipbay, A., Raykul, S., Khassenov, A. (2024). Enhancing visual data security: A novel FSM-based image encryption and decryption methodology. Applied Sciences, 14(11): 4341. https://doi.org/10.3390/app14114341

[4] Hoobi, M.M. (2020). Efficient hybrid cryptography algorithm. Journal of Southwest Jiaotong University, 55(3): 1-9. https://doi.org/10.35741/issn.0258-2724.55.3.5

[5] Shareef, A.A.A., Yannawar, P.L., Qawy, A.A., Almusharref, M.G. (2022). Share and retrieve images securely using Blockchain technology. International Journal on Technical and Physical Problems of Engineering (IJTPE), 52(14): 207-211.

[6] Shakor, M.Y., Khaleel, M.I., Safran, M., Alfarhood, S., Zhu, M. (2024). Dynamic AES encryption and blockchain key management: A novel solution for cloud data security. IEEE Access, 12: 26334-26343. https://doi.org/10.1109/ACCESS.2024.3351119

[7] Hameedi, S.S., Bayat, O. (2022). Improving IoT data security and integrity using lightweight blockchain dynamic table. Applied Sciences, 12(18): 9377. https://doi.org/10.3390/app12189377

[8] Nwatuzie, G.A., Enyejo, L.A., Umeaku, C. (2025). Enhancing cloud data security using a hybrid encryption framework integrating AES, DES, and RC6 with file splitting and steganographic key management. International Journal of Innovative Science and Research Technology, 10(1): 2456-2165. https://doi.org/10.5281/zenodo.14792173

[9] Barik, K., Misra, S., Sanz, L.F., Chockalingam, S. (2024). Enhancing image data security using the APFB model. Connection Science, 36(1): 2379275. https://doi.org/10.1080/09540091.2024.2379275

[10] Lin, Y.R., Juan, J.S.T. (2023). RG-based (k, n)-threshold Visual Cryptography with abilities of OR and XOR Decryption. Engineering Proceedings, 55(1): 65. https://doi.org/10.3390/engproc2023055065

[11] Maragathavalli, P., Aravindhar, R.S., Keerthana, R., Harini, M., Sanjay Kumar, S. (2024). Securing digital evidence: Blockchain and AES-encryption for tamper-resistant data integrity in cybercrime investigations. International Education and Research Journal, 10(3): 169-172. https://doi.org/10.21276/IERJ24037421355530

[12] Taherdoost, H. (2023). Privacy and security of blockchain in healthcare: Applications, challenges, and future perspectives. Sci, 5(4): 41. https://doi.org/10.3390/sci5040041

[13] Ehuil, B.B., Chen, C., Wang, S., Guo, H., Liu, J. (2024). A secure mutual authentication protocol based on Visual Cryptography technique for IoT-Cloud. Chinese Journal of Electronics, 33(1): 43-57. https://doi.org/10.23919/cje.2022.00.339

[14] Khudair, J., Abd Ghan, K., Baharon, M.R.B. (2023). Comparative study in enhancing AES algorithm: Data encryption. Wasit Journal for Pure Sciences, 2(2): 316-339. https://doi.org/10.31185/wjps.100

[15] Su, Y., Wang, X. (2022). A robust visual image encryption scheme based on controlled quantum walks. Physica A: Statistical Mechanics and its Applications, 587: 126529. https://doi.org/10.1016/j.physa.2021.126529

[16] Karolin, M., Meyyappan, T. (2024). Visual Cryptography secret share creation techniques with multiple image encryption and decryption using Elliptic Curve Cryptography. IETE Journal of Research, 70(2): 1638-1645. https://doi.org/10.1080/03772063.2022.2142684

[17] Ren, L., Zhang, D. (2022). A QR code-based user-friendly Visual Cryptography scheme. Scientific Reports, 12(1): 7667. https://doi.org/10.1038/s41598-022-11871-9

[18] Chen, Y.H., Juan, J.S.T. (2022). XOR-Based (n, n) Visual Cryptography schemes for grayscale or color images with meaningful shares. Applied Sciences, 12(19): 10096. https://doi.org/10.3390/app121910096

[19] Cherbal, S., Zier, A., Hebal, S., Louail, L., Annane, B. (2024). Security in internet of things: A review on approaches based on blockchain, machine learning, cryptography, and quantum computing. The Journal of Supercomputing, 80(3): 3738-3816. https://doi.org/10.1007/s11227-023-05616-2

[20] Hwang, S.O., Waseem, H.M., Munir, N. (2024). Billiard quantum chaos: A pioneering image encryption scheme in the post-quantum era. IEEE Access, 12: 85150-85164. https://doi.org/10.1109/ACCESS.2024.3415083

[21] Nancy, V., Balakrishnan, G. (2021). Thermal image-

based object classification for guiding the visually impaired. The Computer Journal, 64(11): 1747-1759. https://doi.org/10.1093/comjnl/bxaa097
[22] Xie, H. (2025). Practice of wearable devices combined with deep learning algorithms in predicting athletic injury risk. Intelligent Decision Technologies,19(6): 4147-4164. https://doi.org/10.1177/1872498125138039
[23] Viret, M., Ohl, F. (2025). Managing ignorance to preserve anti-doping cosmology–The case of contamination. International Journal of Sport Policy and Politics, 17(1): 117-135. https://doi.org/10.1080/19406940.2024.2404205
[24] Tandon, S., Bowers, L.D., Fedoruk, M.N. (2015). Treating the elite athlete: Anti-doping information for the health professional. Missouri Medicine, 112(2): 122.
[25] Filleul, V., d'Arripe-Longueville, F., Garcia, M., Bimes, H., Meinadier, E., Maillot, J., Corrion, K. (2025). Anti-doping education interventions in athletic populations: A systematic review of their characteristics, outcomes and practical implications. International Review of Sport and Exercise Psychology, 18(2): 880-942. https://doi.org/10.1080/1750984X.2024.2306629
[26] Sang-Yong, L., Park, J.H., Yoon, J., Ji-Yong, L. (2023). A validation study of a deep learning-based doping drug text recognition system to ensure safe drug use among athletes. Healthcare, 11(12): 1769. https://doi.org/10.3390/healthcare11121769
[27] Read, D., Skinner, J., Smith, A.C., Lock, D., Stanic, M. (2024). The challenges of harmonising anti-doping policy implementation. Sport Management Review, 27(3): 365-386. https://doi.org/10.1080/14413523.2023.2288713
[28] Ibrahim, D., Sihwail, R., Arrifin, K.A.Z., Abuthawabeh, A., Mizher, M. (2023). A novel color Visual Cryptography approach based on Harris Hawks Optimization Algorithm. Symmetry, 15(7): 1305. https://doi.org/10.3390/sym15071305
[29] Ahmad, S., Hayat, M.F., Qureshi, M.A., Asef, S., Saleem, Y. (2021). Enhanced halftone-based secure and improved Visual Cryptography scheme for colour/binary Images. Multimedia Tools and Applications, 80(21): 32071-32090. https://doi.org/10.1007/s11042-021-11152-z
[30] Ti, Y.W., Chen, S.K., Wu, W.C. (2020). A new Visual Cryptography-based QR code system for medication administration. Mobile Information Systems, 2020(1): 8885242. https://doi.org/10.1155/2020/8885242
[31] Mondal, U.K., Pal, S., Dutta, A., Mandal, J.K. (2021). A new approach to enhance security of Visual Cryptography using steganography (VisUS). arXiv preprint arXiv:2103.09477. https://doi.org/10.48550/arXiv.2103.09477
[32] Rani, N., Sharma, S.R., Mishra, V. (2022). Grayscale and colored image encryption model using a novel fused magic cube. Nonlinear Dynamics, 108(2): 1773-1796. https://doi.org/10.1007/s11071-022-07276-y
[33] Rao, K.S., Sridhar, M. (2021). A novel image encryption using parity based Visual Cryptography. Network, 26(1): 135-142. https://doi.org/10.18280/isi.260115
[34] Bhat, M.N., Buradagunta, S., Rani, K.U. (2019). A novel approach to key management using Visual Cryptography. Ingénierie des Systèmes d'Information, 24(6): 627-632. https://doi.org/10.18280/isi.240610