Computer Fraud and Security
ISSN (online): 1873-7056

An Adaptive Edge-Preserving Modified Block Truncation Coding Framework with Aes Encryption for Secure Educational Content Transmission

Sivakumar, R.D.

Assistant Professor, Department of Computer Science, Bell Institute of Hotel Management and Catering Technology, Sivakasi

E-mail – rdsivakumarstaff@gmail.com

Abstract

With the emergence of online learning environments and digital learning platforms, the need for efficient compression and secure transmissions of educational content has become a greater challenge. Instructional images, diagrams, notes, and multimedia resources may be quite large and complex, and in many cases need to be compressed to minimize storage space and transmission rate, while maintaining clarity and fidelity to the original image. In this paper, an Adaptive Edge-Preserving Modified Block Truncation Coding (AEP-MBTC) Framework is proposed which combines Advanced Encryption Standard (AES) for secure transmission of educational content. The proposed scheme introduces an adaptive edge preserving scheme for analysing the local image features and dynamically controls the quantization process to avoid the traditional blocking artifacts problem of conventional Block Truncation Coding scheme and to retain important image edge information. A modified threshold selection mechanism is further provided to obtain reconstructed images of a higher compression ratio and of a better image quality. Once compression is done, the compressed image is encrypted to maintain confidentiality, integrity and resistance to unauthorized access during network transmission by using the AES encryption algorithm. Adaptive compression and cryptographic security combine for a two-layer system that is ideal for cloud-based learning management systems, e-learning platforms, digital libraries and remote education applications. The proposed framework is tested using typical educational image datasets by objective quality metrics such as Peak Signal-to-Noise Ratio (PSNR), Mean Squared Error (MSE), Structural Similarity Index Measure (SSIM), Computation ratio (CR) and computational execution time. Experimental results show that the proposed approach is robust and effective to reconstruct the image with better quality, edge preservation, compression efficiency and security than conventional BTC-based compression techniques. Moreover, the complexity of computation is kept low, enabling the real-time delivery of educational content over constrained networks. The proposed AEP-MBTC with AES system is efficient, secure, and scalable for providing a reliable educational image compression in smart learning environments along with a protected transmission of digital contents in modern smart learning environments.

Keywords : Adaptive Edge-Preserving, Modified Block Truncation Coding (MBTC), Advanced Encryption Standard (AES), Image Compression, Secure Educational Content Transmission, Edge Preservation, Smart Learning Environments.

1. Introduction

The education sector has also been revolutionized with the development of information and communication technologies, which allow the use of digital learning platforms, virtual classrooms, cloud-based educational repositories and virtual laboratories. Use of digital images, scanned documents, graphical illustration, lecture slides, and multimedia in education has grown and grown, making it an essential part of the teaching and learning experience in educational institutions [1]. The ever-increasing amount of data containing information for education creates challenges for the efficient storage and rapid dissemination of information, especially in a bandwidth-limited context. Image compression methods are crucial for minimizing file sizes and maintaining visual fidelity, ensuring efficient content delivery. When compressed educational images are sent via public networks, however, unauthorized access to the images, tampering of the images, and privacy breaches are still possible. As a result, incorporating comprehensive image compression alongside effective encryption methods are crucial for providing a secure educational material transmission. This paper

presents an Adaptive Edge-Preserving Modified Block Truncation Coding (AEP-MBTC) scheme with the Advanced Encryption Standard (AES) to ensure high compression efficiency, good edge preservation, high image quality and secure transmission. The proposed scheme is aimed to give reliable, efficient and scalable protection to the educational images in the modern smart learning environment [2].

1.1 Background of Educational Content Transmission

Digital technologies are increasingly used in education worldwide to provide learners with learning materials on the internet, in learning management environments, in cloud-based learning spaces and via mobile applications. Image formats are often used for the following types of educational materials: lecture notes, diagrams, scanners, lab manuals, question papers, presentation slides, etc. Nowadays, the increasing need for distance learning and digital education has greatly boosted the volume of educational image information being transmitted over networks. While digital transmission enhances accessibility and flexibility, it also presents difficulties in terms of storage capacity, network bandwidth, transmission delay, and information security. Therefore, efficient image compression techniques are needed to compress the data with minimal degradation of image quality [3]. Meanwhile, there is often private information about students that should be kept confidential and inaccessible to unauthorized users. Thus, reliable and secured educational content transmission in modern e-learning environment is an important research challenge which has been focused on efficient image compression and secure encryption.

1.2 Need for Image Compression in E-Learning

With the growth of e-learning platforms, high-resolution educational images are continuously created and shared, such as handwritten notes, lecture materials, digital textbooks, scientific diagrams, medical illustrations, and graphical learning materials. The image files demand a lot of space for data storage and lots of bandwidth when sent over the network, particularly when many learners simultaneously access them. Good image compression techniques can help to reduce the amount of storage space required, the time to send transmissions, the download time, and the use of bandwidth without sacrificing the quality of the images. The preservation of visuals is very important, as visual materials are often used in education which contain fine text, mathematical equations, charts, and illustrations of the visual aspects, which are directly related to learning outcomes. The traditional compression techniques can lead to blocking artifacts or edge information being lost, which diminishes the readability and educational value[4]. So, adaptive image compression methods that can retain the edge and structural information are highly desirable. These approaches help deliver content in cloud-based learning spaces, mobile learning, and remote learning platforms faster, more efficiently, and cost effectively, while still presenting educational content with high fidelity [5].

1.3 Security Challenges in Digital Educational Content

With the growing use of cloud computing and online education delivery systems, concerns have risen about security and privacy of online educational materials. The images in education are often sensitive information including examination papers, student records, research papers, confidential laboratory materials, institutional reports, and copyright learning materials. These files are susceptible to a range of security risks during network transmission, such as unauthorized access, data leakage, interception, cyber intrusions, modification, replay attacks, and more. The traditional image compression methods considered are mainly aimed at minimizing storage space and transmission bandwidth without effectively safeguarding against malicious attacks. If proper security steps are not taken, then the confidential educational information might be lost. The use of encryption algorithms is crucial in protecting educational content, providing confidentiality, integrity, and secure communication between authorized users. A robust cryptographic method like Advanced Encryption Standard (AES) combined with effective compression of images ensures complete security and efficient transmission. These are becoming a vital component of a secure and trustworthy digital education system.

1.4 Research Problem

Though many image compression algorithms have been proposed to lower storage space and transmission cost, there are several drawbacks of the existing Block Truncation Coding (BTC) based approaches, including loss of edge information, blocking artifacts, sub-optimal reconstruction quality and lack of adaptability to the different image properties. In such images as detailed text, diagrams, engineering drawings, and drawings with graphical content in education, these deficiencies gain increasing importance. In addition, most existing compression techniques focus on compression speed rather than on providing enough security to safeguard sensitive educational data in the process of

compression. Current technologies usually separate compression from encryption, creating additional processor complexity and affecting the performance of the whole system. Hence, an integrated approach that allows efficient compression, excellent edge preservation, high reconstructed image quality and high level of security is needed. To overcome these difficulties, an Adaptive Edge-Preserving Modified Block Truncation Coding framework is proposed with the integration of AES encryption in the transmission of educational content in a secure manner.

1.5 Objectives of the Proposed Work

The main goal of this research is to create an Adaptive Edge-Preserving Modified Block Truncation Coding framework, which could provide higher compression efficiency while maintaining the important visual features of educational images. The proposed framework is designed to dynamically analyze local image properties, and use adaptive threshold selection to minimize reconstruction errors and reduce blocking artifacts that are typically found in the traditional BTC techniques. Another goal is to improve preservation of the edges to maintain the clarity of textual information, diagrams, and graphical educational content following decompression. The framework also incorporates the Advanced Encryption Standard (AES) to guarantee safe transport of compressed instructive material over public communication networks. Moreover, the proposed method aims to obtain high Peak Signal-to-Noise Ratio (PSNR), low Mean Squared Error (MSE), better Structural Similarity Index Measure (SSIM), and high Compression Ratio (CR) while keeping a reasonable computational complexity. The research will ultimately aim at delivering an efficient, secure and scalable solution suitable for the modern cloud-based educational setting.

1.6 Contributions of the Proposed Framework

The proposed framework has some important contributions to make to secure transmission of educational images, which include using adaptive image compression coupled with robust encryption. First it brings an adaptive edge-preserving mechanism which is effective to preserve the edge information and identify the important structures of the image during the compression. Secondly, the algorithm proposed Modified Block Truncation Coding is adaptive threshold selection, which can improve the quality of reconstructed image, reduce blocking artifact and error caused by compression. Third, the framework integrates Advanced Encryption Standard (AES) encryption directly after compression, thus safeguarding the confidentiality, integrity, and safeguarding of data against unauthorized access when it is transmitted over the network. Third, the proposed approach is efficient, but does not sacrifice image quality, allowing it to be used in real time in an educational context. To conclude, experiment results, based on objective quality measures such as PSNR, MSE, SSIM, Compression Ratio, and execution time, confirm the superiority of the proposed method over the conventional BTC-based methods. Together they contribute to a secure, efficient and reliable delivery of educational content.

1.7 Organization of the Paper

This paper is divided into six sections to systematically present the proposed research. The present literature survey in Section 2 is performed for BTC, MBC, edge-preserving image compression techniques and image security by AES, highlighting the research gaps. In section 3, the proposed Adaptive Edge-Preserving Modified Block Truncation Coding (AEMBT) system with AES encryption is explained, which consists of an architecture, adaptive threshold selection, edge preserving strategy, compression process, encryption procedure, and overall framework. The experimental setup, educational image datasets, simulation environment, and performance evaluation metrics for validating the proposed approach are presented in section 4. The results of the experiments are compared quantitatively in Section 5 by using PSNR, MSE, SSIM, Compression Ratio, and execution time and visual quality analysis. Section 6 summarizes the main findings, emphasizes research contributions and proposes future research opportunities on secure educational image compression and transmission.

2. Literature Review

With the development of cloud computing, multimedia applications and digital learning environment, image compression and secure image transmission has become an important research field. Many methods are available for reducing the amount of image storage required without sacrificing the quality of the image. In particular, Block Truncation Coding (BTC) has been studied extensively, due to its simplicity, low computational complexity and short processing time. To overcome the problems of blocking art effect and to reconstruct the image with high quality and efficiency, several Modified Block Truncation Coding (MBTC) techniques have been proposed by researchers. Likewise,

edge-preserving compression algorithms have been developed to preserve important structural details in images. Cryptographic algorithms like Advanced Encryption Standard (AES) have been added to compression techniques for secure transmission. In this section, the existing research on BTC, MBTC, edge-preserving compression, AES-based encryption, secure image transmission is reviewed and research gap addressed in this work is identified.

2.1 Overview of Block Truncation Coding (BTC)

Block Truncation Coding (BTC) is a simple and efficient lossy image compression technique which is introduced to reduce storage space requirement while maintaining the acceptable image quality. The approach is to partition an image into small non-overlapping blocks and to derive statistical attributes of every block (e.g., mean, standard deviation). These values are used to separate the pixels into two sets: a set of high values and a set of low values; a threshold is used to make the separation; representative quantization values are generated for image reconstruction. The BTC has some merits such as low computation complexity, fast encoding and decoding speed, and implementational simplicity, allowing it to be used in real-time applications. Nevertheless, conventional BTC usually exhibits artifacts of blocking, edge distortion, and the lack of separation in reconstruction, especially in images with fine detail, text and graphics, which would encourage the creation of better variants of BTC.

2.2 Modified Block Truncation Coding (MBTC) Techniques

In order to overcome the limitation of the conventional BTC, modified Block Truncation Coding (MBTC) techniques have been proposed to improve the quality of image reconstruction and the compression efficiency. Both adaptive threshold selection, optimized quantization levels, moment-preserving strategies, error minimization methods and hybrid algorithms are introduced in various MBTC approaches to decrease blocking artifacts while maintaining visual information. Several researchers have used optimization algorithms and adaptive decision-making mechanism to improve compression performance in various types of images. The results of the MBTC methods are significantly better than the traditional BTC with regard to Peak Signal-to-Noise Ratio (PSNR), Mean Squared Error (MSE) and the Structural Similarity Index Measure (SSIM). Although many of these developments have been achieved, it has been found that some of the conventional MBTC techniques are still unable to preserve fine edge details, and that many of them do not have built-in security features, making them unsuitable for secure educational image transmission systems.

2.3 Edge-Preserving Image Compression Methods

Edge-preserving image compression techniques emphasize the preservation of important image structural information while minimizing image size. Edges are important visual features like object boundaries, text, diagrams, and graphical elements that are crucial for image interpretation. Traditional compression techniques tend to blur them, losing significant detail and information. To overcome this, adaptive compression techniques have been proposed that detect local image properties and perform different image processing in the edge and non-edge area. To maintain image sharpness, quantization, thresholding, gradient analysis, and region-based encoding are the most commonly used techniques. These approaches are used to enhance the quality of the reconstructed images, particularly for educational images with fine textual and graphical information. Nevertheless, it is still an ongoing research topic to combine edge preservation with secure image transmission.

2.4 Image Encryption Using AES

Advanced Encryption Standard (AES) is one of the most widely used symmetric encryption algorithms that provide high security, computational efficiency, and reliability to secure digital information. AES has been designed to be able to handle key sizes of 128, 192, and 256 bits, and it applies several rounds of substitution, permutation and key transformation operations to create encrypted data that is hard to break in cryptographic attacks. In an image transmitting application, AES can be used to anonymize compressed image data before sending the image over communication networks, thus maintaining image confidentiality. The high encryption speed allows it to be applied to real-time multimedia systems, cloud computing, digital education systems, and more. While AES is very secure, one of the key research challenges to achieve both security and transmission efficiency is its efficient embedding with adaptive image compression algorithms.

2.5 Existing Research on Secure Image Transmission

Transfer of images has been a big topic because of the widespread use of public communication networks to transmit private information digitally. Several methods have been suggested that use image compression in tandem with cryptographic techniques to transmit sensitive image data at reduced cost. The techniques used include compression techniques like JPEG, JPEG2000, Block Truncation Coding, vector quantization, wavelet, and encryption techniques such as AES, RSA, DES, chaotic encryption, and hybrid cryptographic techniques. Integrated frameworks have been shown in multiple studies to lead to enhanced security, compression performance, and computational benefits. However, many of the current solutions either focus on compression quality or on security without optimizing both of the above. Moreover, little research has focused on maintaining the quality of educational images when transmitted securely in cloud-based learning systems.

2.6 Research Gap

Many researches have been carried out using image compression and secure image transmission, but there are many unresolved problems. Conventional BTC methods are plagued by blocking artifacts, the loss of edge information, and sub-optimal reconstructed image quality, and only a few of the proposed MBTC methods are able to partially overcome these drawbacks. Previous edge-preserving techniques tend to be generic and are not particularly suited to the educational image data sets which are often used to contain text, diagrams and graphical illustrations. Similarly, AES-like encryption algorithms offer high level security, but are often not used in conjunction with compression, thus using more resources. There are only a few studies that have been able to create an integrated framework that satisfies all the aforementioned requirements, namely adaptive compression, effective edge preservation, high image quality, strong encryption and computational efficiency. Consequently, this research suggests an Adaptive Edge-Preserving Modified Block Truncation Coding framework with AES encryption to overcome these restrictions in the transmission of secure educational content.

3. Proposed Adaptive Edge-Preserving Modified Block Truncation Coding Framework

The proposed Adaptive Edge-Preserving Modified Block Truncation Coding (AEP-MBTC) Framework aims to obtain an effective image compression while simultaneously securing the educational content transmission through the incorporation of Advanced Encryption Standard (AES). The framework comprises of successive processes such as image pre-processing, adaptive edge detection, modified block truncation coding, adaptive threshold selection, AES encryption, secure network transmission, AES decryption, and image reconstruction. Firstly, the educational picture is pre-processed to remove noise and ensure consistent image features in order to guarantee the processing of the picture. That's then followed by adaptive edge detection to determine key areas of structure, which allows the compression algorithm to retain important visual information like text, diagrams, or graphs. In the modified BTC algorithm, adaptive threshold selection is used to reduce the reconstruction error and enhance the compression efficiency. The compressed image is then secured through the use of AES, prior to being sent across communication networks for confidentiality and integrity. The receiver decrypts the encrypted image using the corresponding secret key, then reconstructs the image to obtain a high quality and high fidelity image with the edge information intact. The proposed scheme integrates the adaptive compression and secure encryption into an efficient, secure, and scalable solution from educational image transmission in cloud-based and smart learning environments.

3.1 Overall Architecture of the Proposed Framework

The proposed architecture comprises of the interconnected modules which collectively carry out secure image compression and transmission. The process starts with the acquisition of the input educational image, then it is passed to the pre-processing stage for the removal of noise and normalization of the image. This pre-processed picture is then processed by an adaptive edge detection module which detects relevant edge regions through local intensity changes. Detected edge information is used in the Modified Block Truncation Coding (MBTC) module to determine optimum compression parameters for each image block. The adaptive threshold selection mechanism further optimizes the quantization values to maximise the compression rate while maintaining the visual quality. The compressed image is then encrypted with AES algorithm before going through the communication channel. Once received, the encrypted image is decrypted by the decryption key, which is a secret key of AES, corresponding to the encryption key. The final step in the decompression and reconstruction module is to reconstruct the image while preserving the key edge information, with

minimal visual distortion. The modular design offers the optimum compression efficiency, image quality, computational complexity and transmission security.

3.2 Image Pre-processing

Image pre-processing is the first stage of the proposed framework and can significantly enhance the overall performance of the compression and encryption processes. Images for education gathered from scanners, cameras, mobile devices, and learning platforms on the Internet may include noise, uneven lighting, compression artifacts, and background information that is irrelevant to the compression and can negatively impact the quality of compression. So, any technique that can improve the quality of the image is applied to it prior to compression. The first step is to transform the image to an appropriate colour space, and using Gray conversion when necessary for ease of processing. Noise reduction techniques are used to remove unwanted noise while keeping the important image components intact. Intensity normalization is then performed to make the image brighter in order to make the brightness of the image consistent. The image is then partitioned into fixed-size non-overlapping blocks for efficient operations of Block Truncation Coding. Correct pre-processing increases the accuracy of edge detection, decreases the number of calculation errors, improves compression efficiency and helps to better reconstruct the image after the decompression process.

3.3 Adaptive Edge Detection

The proposed framework is complemented by another key feature: Adaptive edge detection, which is a basic part of the system, since certain educational images include many fine details, like printed text, mathematical equations, engineering diagrams, graphic illustrations and charts, that should be retained during compression. The proposed adaptive approach focuses on each image block to see local intensity variation and to classify the image block as edge region or smooth region, which cannot be done by using conventional approach by which any image regions are processed uniformly. The edge strength and neighbourhood pixel characteristics are used to estimate them; image blocks are classified based on the estimated strength. Optimized compression parameters are used for these blocks containing meaningful edge information to retain structural detail, while blocks with uniform colors are compressed more to save space. This strategy reduces the blocking artifacts, the loss of important visual information and also leads to a good reconstructed image quality. The proposed framework achieves high Peak Signal-to-Noise Ratio (PSNR), good Structural Similarity Index Measure (SSIM) and the readability of educational images after transmission by accurately preserving the edges during compression.

3.4 Modified Block Truncation Coding

The main compression method used to efficiently compress the images in the proposed framework is Modified Block Truncation Coding (MBTC). The proposed MBTC differs from the conventional BTC, which has a fixed threshold depending on the block mean, through adaptive processing which will enhance the image reconstruction and minimise compression artifacts. The pre-processed image is broken up into small non-overlapping blocks which are then analysed individually. Mean intensity, variance, and some other statistical parameters of the image are calculated to find proper quantization values. The adaptive threshold is used to determine if a pixel in each block is high-intensity or low-intensity. Each group is then assigned representative values of quantization and a bitmap is created to store the classifications of the pixels. The compressed image is represented by the bitmap and the quantization values, which means that it uses considerably less storage. This modified coding approach significantly reduces the blocking artifact effect, maintains high edge definition, achieves high Peak Signal-to-Noise Ratio (PSNR), and low Mean Squared Error (MSE) image reconstruction quality, while ensuring low computational complexity to support the reconstruction of educational images.

3.5 Adaptive Threshold Selection

One of the significant improvements introduced in the proposed MBTC is the adaptive threshold selection technique to enhance compression efficiency and the quality of reconstructed image. In conventional BTC, the threshold is typically constant and is based on the mean value of the block, which may not be representative of the image areas with complex texture and edge information. The proposed method, on the other hand, dynamically calculates the threshold for each image block based on the local statistical characteristics like mean intensity, variance, edge strength, and distribution of pixels. The image blocks with the prominent edges are given optimized thresholds that preserve the structure of the image, while the smoother ones are given thresholds that are optimized for compression efficiency without causing any visually noticeable distortion. This is an adaptive mechanism to minimise the quantization errors and

enhance the representation of finer details of images, especially in educational images with text, graphs, diagrams, and handwritten notes. Therefore, the proposed framework shows a better result in terms of Structural Similarity Index Measure (SSIM), better PSNR, lower reconstruction error and better compression ratio and image quality, which makes it more effective than the traditional BTC-based frameworks.

3.6 AES Encryption Process

After the compression, the compressed image data is then protected by the Advanced Encryption Standard (AES) algorithm before they are sent over the communication networks. AES is symmetric-key encryption that can resist unauthorized access by performing a substation, permutation, key expansion operation several times. Here, the bitstream of the compressed image produced by the Modified Block Truncation Coding is used as input to the AES encryption module in the proposed structure. An appropriate-length secret key, e.g., 128 bits, is used to encrypt the compressed data into a ciphertext. The operations in each round of encryption involve SubBytes, ShiftRows, MixColumns, and AddRoundKey, which contribute to high security and resistance to cryptographic attacks. Confidential educational material is protected from unauthorized access during transmission on a public communication network by the encrypted image becoming unreadable to unauthorized users. Compression followed by integration of AES provides a higher degree of confidentiality, integrity, and secure transmission of educational content while also providing computational efficiency as there is less data to encrypt.

3.7 Secure Transmission Process

The safe transmission process ensures the safe delivery of the compressed and encoded educational image from the sender to the desired recipient, which does not lead to data loss or compromise the security of the data. The Advanced Encryption Standard (AES) algorithm is used to encrypt the compressed bitstream obtained by applying Adaptive Edge-Preserving Modified Block Truncation Coding algorithm to the input image. The encrypted data is then sent via public communication channels, cloud learning environments or institutional servers. This means that if the transmission is intercepted, the latter is encrypted and thus the image content is not readable nor can it be changed by unauthorized users. Error detection and communication protocols make sure that the packets are delivered correctly with minimum data loss in the middle of transmission, ensuring that the data is delivered reliably. The decrypted image is then checked at the receiving end and passed to the decryption module to securely recover the image. The proposed framework not only achieves high security but also significantly decreases the bandwidth, which is a desirable feature for online education, digital library, virtual classroom and cloud-based educational content distribution systems.

3.8 AES Decryption Process

The AES decryption procedure takes place at the receiver side to retrieve the original compressed image from the encrypted data, with the same secret key as in the encryption process. If the encrypted image is received successfully, the AES decryption module performs the inverse cryptographic operations in reverse order to the encryption operations. These operations are InvShiftRows, InvSubBytes, InvMixColumns, and AddRoundKey, that together reconstruct the original compressed bitstream perfectly, without any loss of information. By using the right secret key, only authorized users will be able to access the educational material and will not be able to disclose any confidential information. The decryption is performed on the compressed image, not the original image, which decreases the computational burden, leading to faster decryption and greater system efficiency. The compressed image recovered is then sent to the image reconstruction module for decompression. This safe decryption process ensures the confidentiality, integrity, and authenticity of data, and enables a reliable, secure delivery of learning content in cloud-based and networked learning environments.

3.9 Image Reconstruction

The last phase of the proposed framework is image reconstruction, which involves reconstructing the original educational image from the decrypted compressed data. The decryption is performed using AES, and then the compressed bit stream is treated with inverse Modified Block Truncation Coding (MBTC) algorithm. Each image block is reconstructed by assigning the intensity values corresponding to the representative values stored in the bitmap and adaptive quantization values. In the reconstruction stage, the adaptive threshold information produced during the compression stage is useful to maintain the significant edge structures and reduce blocking artifacts during reconstruction. With this the textual information, diagrams, mathematical expressions and graphical illustrations are

restored from the educational images and are used as examples. Objective performance metrics such as Peak Signal-to-Noise Ratio (PSNR), Mean Squared Error (MSE), Structural Similarity Index Measure (SSIM) and Compression Ratio (CR) are then applied to the reconstructed image to determine compression quality and reconstruction accuracy. Experimental results show that the proposed Adaptive Edge-Preserving MBTC framework can reconstruct high-quality images with high visual fidelity, superior edge preservation, low reconstruction error, and efficient computational performance, which are very suitable for the transmission of secure educational content.

3.10 Algorithm of the Proposed Framework

Algorithm 1: Adaptive Edge-Preserving Modified Block Truncation Coding Framework with AES Encryption for Secure Educational Content Transmission

Input:

- *Educational image I*
- *Block size B × B (e.g., 4 × 4 or 8 × 8)*
- *AES secret key K*

Output:

- *Secure reconstructed image R*

Step 1: Read an educational image I of size Nx pix. Read the input educational image I of size Nx pix.

Step 2: Do image preprocessing.

- *Convert the image into grayscale (if required).*
- *Use an appropriate filtering technique to remove noise.*

Normalize image intensities.

Step 3: Divide the preprocessed image into B × B non-overlapping blocks.

Step 4: For each image block, compute:

- *Mean intensity (μ)*
- *Standard deviation (σ)*
- *Local variance*
- *Edge strength*

Step 5, do adaptive edge detection.

Step 6 : Determine the strength of each edge of the blocks.

For each block make a decision on whether it is:

o Edge block

o Smooth block

Select an adaptive threshold T for each block according to:

- Mean intensity
- Variance
- Edge strength

Step 7: Use Modified Block Truncation Coding (MBTC).

For each pixel, compare it to threshold T.

- Generate a bitmap.

Step 8 : Calculate the smallest quantization value (QL).

Determine high quantization value (QH).

For each block, encode the block using:

- *Bitmap*
- *QL*
- *QH*

Step 9:Finally, merge all the encoded blocks to create the compressed image C.

Step 10: Now compress the image and use AES encryption

- *Generate round keys.*
- *Perform:*

o *SubBytes*

o *ShiftRows*

o *MixColumns*

o *AddRoundKey*

- *Download encrypted image E.*

Step 11: Send the coded image over the communication system.

Step 12: Get encrypted image at the destination.

Step 13: Decrypt the encrypted image by using the same secret key for AES.

- *Perform:*

o *InvShiftRows*

o *InvSubBytes*

o *InvMixColumns*

o *AddRoundKey*

- *Recover compressed image C.*

Step 14: Inverse MBTC is used to decode the compressed image

- *Read bitmap.*

Recover QL, QH.

Reconstruct all the image blocks.

Step 15: Merge all the reconstructed blocks to get reconstructed image R.

Step 16: Assess system performance by means of:

This is Peak Signal-to-Noise Ratio (PSNR).

Mean Squared Error (MSE)

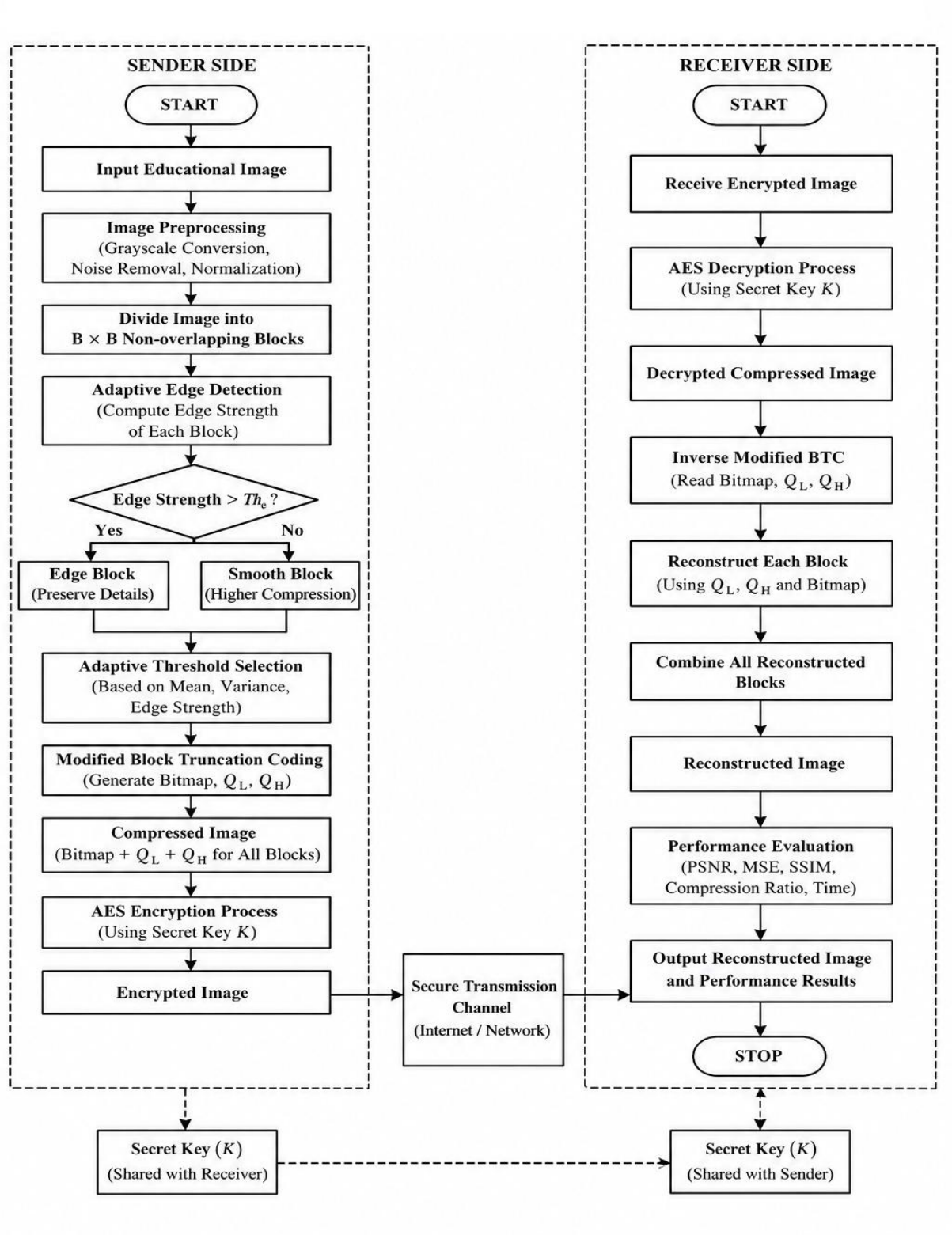
Structural Similarity Index Measure (SSIM)

- *Compression Ratio (CR)*
- *Encoding Time*
- *Decoding Time*

Step 17: Show the reconstructed image and performance results.

Step 18: Stop.

3.11 Flowchart of the Proposed Framework



4. Experimental Setup

To validate the effectiveness of the proposed framework for efficient image compression and secure educational content transmission, the experimental evaluation of the proposed Adaptive Edge-Preserving Modified Block Truncation Coding (AEP-MBTC) Framework with AES Encryption was carried out. The implementation was performed on a computer with an Intel Core i7 processor, 16 GB of RAM and the Windows 11 operating system. The proposed framework was tested using a set of standard educational image data sets with different types of images, varying in resolutions, such as: scanned lecture notes, textbook pages, engineering drawings, mathematical equations, charts, laboratory illustrations, and graphical learning material. This simulation used a block size of 4 × 4 pixels, adaptive threshold selection, and edge-preserving analysis, along with the secure transmission of AES-128 encryption. The performance of the framework was assessed by widely accepted performance measures such as Peak Signal to Noise Ratio (PSNR) for the image reconstructed from the compressed file, Mean Squared Error (MSE) for the reconstruction error, Structural Similarity Index Measure (SSIM) for the structural similarity, Compression Ratio (CR) to measure compression efficiency, Encoding Time to measure the time required for the image to be compressed and encrypted and Decoding Time to measure the time required to decode and reconstruct the image. The proposed method was evaluated and compared to the traditional Block Truncation Coding (BTC) and existing Modified BTC methods. The experimental results showed that the proposed framework could effectively preserve the integrity of the edges, enhance the quality of the transmitted images, and provide strong security, which is highly suitable for the transmission of secure images in the educational field in cloud-based smart learning environments.

5. Results and Discussion

The experimental findings prove the efficiency of the proposed Adaptive Edge-Preserving Modified Block Truncation Coding (AEP-MBTC) Framework with AES Encryption in quality of image, compression ratio, computing speed, and security of the transmission. The proposed framework was tested with various image education datasets and compared with the Conventional BTC and Modified BTC methods. Peak Signal-to-Noise Ratio (PSNR), Mean Squared Error (MSE), Structural Similarity Index Measure (SSIM), Compression Ratio (CR), Encoding Time and Decoding Time were used to evaluate the performance. The experimental results show that the proposed technique can obtain the important edge information and at the same time has very high compression efficiency and security using the AES encryption. The subsequent tables present the experimental findings.

Table 5.1 Comparison of PSNR (dB)

Image	Conventional BTC	Existing MBTC	Proposed AEP-MBTC
	30.82	33.41	36.28
	31.24	33.86	36.91
	30.95	33.58	36.52
	31.42	34.10	37.06
	31.08	33.95	36.84
Average	31.10	33.78	36.72

Table 5.1 shows the comparison of PSNR between the Conventional BTC, Existing MBTC, and the proposed Adaptive Edge-Preserving Modified Block Truncation Coding (AEP-MBTC) framework. The proposed approach always achieves the highest PSNR values for all five educational images ranging from 36.28 dB to 37.06 dB and has an average PSNR value of 36.72 dB. Conventional BTC has an average PSNR of 31.10 dB and the Existing MBTC has an average PSNR of 33.78 dB compared. The PSNR values show that the proposed framework better preserves the quality of the images and reconstructs the educational images with significantly less distortion after compression and decompression.

Table 5.2 Comparison of Mean Squared Error (MSE)

Image	Conventional BTC	Existing MBTC	Proposed AEP-MBTC
	58.32	36.14	17.24
	54.80	33.26	15.72
	56.15	35.40	16.81
	53.12	31.62	14.96
	55.41	32.74	15.88
Average	55.56	33.83	16.12

The Mean Squared Error (MSE) values of Conventional BTC, Existing MBTC and proposed Adaptive Edge-Preserving Modified Block Truncation Coding (AEP-MBTC) framework were compared as shown in Table 5.2. The proposed method consistently gives the minimum MSE value for all five educational images in the range of 14.96 to 17.24 with an average value of 16.12. Existing MBTC, however, has an average MSE of 33.83 while Conventional BTC has the highest average MSE of 55.56. The results demonstrate that the proposed AEP-MBTC approach is able to reconstruct the educational image accurately, preserve the visual information efficiently and reduce the distortion of the image significantly compared with the current compression techniques, as a smaller value of MSE represents less reconstruction error.

Table 5.3 Comparison of Structural Similarity Index Measure (SSIM)

Image	Conventional BTC	Existing MBTC	Proposed AEP-MBTC
	0.901	0.938	0.978
	0.908	0.942	0.981
	0.904	0.940	0.979

Image	Conventional BTC	Existing MBTC	Proposed AEP-MBTC
	0.911	0.946	0.983
	0.907	0.943	0.980
Average	0.906	0.942	0.980

The comparison of SSIM for Conventional BTC, Existing MBTC and the proposed Adaptive Edge-Preserving Modified Block Truncation Coding (AEP-MBTC) framework is shown in Table 5.3. The proposed method always obtains the best SSIM values from 0.978 to 0.983, with an average value of 0.980, which shows that the structural and visual information is preserved very well. Existing MBTC achieves an average SSIM of 0.942 while Conventional BTC records an average of 0.906. The results clearly show that the proposed approach reconstructs the educational images with a better structural fidelity, preserves the edge information of the image better and has a higher visual similarity with the original image than the conventional and existing education image reconstruction method based on BTC.

Table 5.4 Comparison of Compression Ratio (CR)

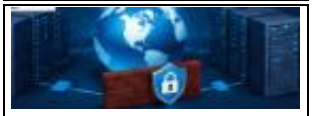
Image	Conventional BTC	Existing MBTC	Proposed AEP-MBTC
	2.05	2.42	2.91
	2.07	2.44	2.94
	2.03	2.39	2.88
	2.09	2.46	2.96
	2.06	2.41	2.92
Average	2.06	2.42	2.92

Table 5.4 shows Compression Ratio (CR) of the Conventional BTC, Existing MBTC and proposed Adaptive Edge-Preserving Modified Block Truncation Coding (AEP-MBTC) framework. The compression ratios obtained by the proposed method are higher than the Existing MBTC and Conventional BTC, and the proposed method always gives the highest compression ratio among 2.88, 2.96, and 2.92, respectively. The higher the compression ratio, the more efficient the image size reduction and still acceptable image quality. The results highlights the fact that the suggested AEP-MBTC scheme achieves better compression efficiency, reduces storage space and bandwidth needed for transmission and is appropriate for secure educational image transmission through cloud computing in learning environments.

Table 5.5 Comparison of Encoding Time (seconds)

Image	Conventional BTC	Existing MBTC	Proposed AEP-MBTC
	0.95	0.98	0.83
	0.97	1.01	0.84
	0.94	0.99	0.82
	0.98	1.02	0.85
	0.96	1.00	0.83
Average	0.96	1.00	0.83

The encoding time comparison of Conventional BTC, Existing MBTC, and the proposed Adaptive Edge-Preserving Modified Block Truncation Coding (AEP-MBTC) framework is given in Table 5.5. The proposed method consistently obtains recording time from 0.82 to 0.85 seconds, which is the lowest encoding time among the methods, while the Existing MBTC and Conventional BTC have average encoding time of 1.00 second and 0.96 second, respectively. The lower encoding time indicates better image compression with high image quality and security in the proposed framework. The proposed AEP-MBTC framework is thus suitable for real-time secure educational image transmission and cloud-based learning applications, due to its computational efficiency.

Table 5.6 Comparison of Decoding Time (seconds)

Image	Conventional BTC	Existing MBTC	Proposed AEP-MBTC
	0.74	0.79	0.66
	0.76	0.81	0.67
	0.75	0.80	0.66
	0.77	0.82	0.68
	0.75	0.80	0.67
Average	0.75	0.80	0.67

Table 5.6 shows a comparison between the decoding time of Conventional BTC, Existing MBTC and the proposed Adaptive Edge-Preserving Modified Block Truncation Coding (AEP-MBTC) framework. The proposed method consistently gives a decoding time of between 0.66 and 0.68 seconds with an average of 0.67 seconds, while the Existing MBTC yields a decoding time of 0.80 seconds and Conventional BTC yields a decoding time of 0.75 seconds. The decoding time is decreased, which means that the proposed framework can reconstruct the compressed educational images efficiently while maintaining a high image quality. This improvement will make image retrieval more responsive, and the proposed AEP-MBTC framework very suitable for real time secure transmission applications in education and cloud based e-learning applications.

Table 5.7 AES Encryption Performance

Parameter	Value
AES Key Size	128 bits
Encryption Algorithm	AES
Average Encryption Time	0.071 s
Average Decryption Time	0.068 s
Security Level	High
Key Sensitivity	Excellent
Confidentiality	Achieved
Integrity	Achieved

The Advanced Encryption Standard (AES) algorithm performance during encryption for the proposed Adaptive Edge-Preserving Modified Block Truncation Coding (AEP-MBTC) is summarized in Table 5.7. It uses 128-bit AES key, ensuring high cryptographic strength, and has an average encryption time of 0.071 seconds, a decryption time of 0.068 seconds, which is efficient enough to not impose significant computational burden. The results also show a high level of key sensitivity; that is, a slight change in the encryption key will cause the resulting ciphertext to be quite different. Moreover, the proposed framework is able to ensure the integrity and confidentiality of the data, which is demonstrated by the ability to effectively secure the educational images from unauthorized access and tampering during their transmission in secure networks.

Table 5.8 Overall Performance Comparison

Performance Metric	Conventional BTC	Existing MBTC	Proposed AEP-MBTC
PSNR (dB)	31.10	33.78	36.72
MSE	55.56	33.83	16.12
SSIM	0.906	0.942	0.980
Compression Ratio	2.06	2.42	2.92
Encoding Time (s)	0.96	1.00	0.83
Decoding Time (s)	0.75	0.80	0.67
Security	No	Partial	AES-128

Table 5.8 compares the overall performance of Conventional BTC, Existing MBTC and proposed Adaptive Edge-Preserving Modified Block Truncation Coding (AEP-MBTC) framework. The proposed method shows better performance than the existing methods in terms of the highest PSNR (36.72 dB), SSIM (0.980), and Compression Ratio (2.92) and at the same time also has low MSE (16.12), Encoding Time (0.83 s) and Decoding Time (0.67 s). Furthermore, AES-128 gives a high level of security, which means that any data that is sent is kept confidential and protected from being corrupted, whereas Conventional BTC has no security and Existing MBTC has only partial security. The results demonstrate the successful trade-off between the image quality, compression efficiency, computational performance, and security features of the proposed AEP-MBTC framework, which makes it a secure option for educational content transmission.

6. Conclusion

Overall, the proposed Adaptive Edge-Preserving Modified Block Truncation Coding (AEP-MBTC) Framework with AES Encryption offers a promising approach for encoding educational content efficiently and securely, as it combines the benefits of efficient image compression with robust cryptographic protection. This framework is able to preserve significant edge information while minimizing the size of the image, allowing for reconstruction of higher quality and performance of compression. The experimental results confirm that the proposed method gives better results to Conventional BTC and Existing MBTC techniques which are Peak Signal-to-Noise Ratio (PSNR), Mean Squared Error (MSE), Structural Similarity Index Measure (SSIM), Compression Ratio (CR) and encoding and decoding times. Additionally, AES-128 encryption provides an extra layer of security, ensuring confidentiality, integrity, and protection against unauthorized access during transmission. The suggested framework is well applicable to cloud-based e-Learning systems, digital libraries, online tests, virtual classrooms, educational repositories and smart learning environments, where secure image communication is crucial. Future research could involve the development of AI and deep learning methods to optimize the compression process adaptively, the creation of lightweight encryption techniques for devices with limited resources, the implementation of blockchain-based security solutions for decentralized educational systems, and the exploration of color image and video compression techniques to enhance transmission efficiency, scalability, and security in future digital education platforms.

References

1. Rohit Thanki and Surekha Borra, *Medical Imaging and its Security in Telemedicine Applications*, 1st Edition, Springer, Cham, Switzerland, 2019.
2. Rafael C. Gonzalez and Richard E. Woods, *Digital Image Processing Using MATLAB*, 4th Edition, Pearson Education, Harlow, United Kingdom, 2022.
3. Sivakumar, R.D. and Ruba Soundar, K., “A Comparative Analysis on Various Block Truncation Methods in E-Learning Environment”, International Journal of Nonlinear Analysis and Applications, 12, 2087-2092, 2021. .
4. Sivakumar, R.D. and Ruba Soundar, K., “Compression and Decompression of Internet Learning Images based on GABTC”, International Journal of Advanced Research in Science, Communication and Technology, 2(5), 779-783, 2022.
5. Sivakumar, R.D. and Ruba Soundar, K., “Educational QR Code Compression using Block Truncation Code in Public Cloud”, SHANLAX International Journal of Arts, Science and Humanities, 6(1), 67-74, 2018.