IoT CCTV Video Security Optimization Using Selective Encryption and Compression

Kawalpreet Kaur[1], Amanpreet Kaur[2]*, Yonis Gulzar[3]*, Vidhyotma Gandhi[4], Mohammad Shuaib Mir[5], Arjumand Bano Soomro[6]

Chitkara University Institute of Engineering and Technology, Chitkara University, Punjab, India[1, 2]
Department of Management Information Systems-College of Business Administration, King Faisal University,
Al-Ahsa 31982, Saudi Arabia[3, 5, 6]
Gyancity Research Labs, Gurugram, Haryana, India[4]

***Abstract*—Data security and privacy are critical concerns when integrating Closed-Circuit Television (CCTV) cameras with the Internet of Things (IoT). To enhance security, IoT data must be encrypted before transmission and storage. However, to minimize overheads related to storage space, computational time, and transmission energy, data can be compressed prior to encryption. H.264/AVC (Advanced Video Coding) offers a balanced solution for video compression by addressing processing demands, video quality, and compression efficiency. Encryption is vital for safeguarding data security, yet the integrity of IoT data may sometimes be compromised. Ineffective data selection can lead to inefficiencies and potential security risks, highlighting the importance of addressing CCTV video data security carefully. This study proposes an algorithm that integrates compression with selective encryption techniques to reduce computational overhead while ensuring access to critical information for real-time analysis. By employing frame intervals, the algorithm enhances efficiency without compromising security. The execution details and merits of the proposed approach are analyzed, demonstrating its effectiveness in safeguarding the privacy and integrity of IoT CCTV video data. Results reveal superior performance in terms of compression efficiency and encryption/decryption times, with an average encryption time of 0.00171 seconds for a 128-bit key, enabling fast processing suitable for real-time applications. The decryption time matches the encryption time, confirming the method's viability for practical IoT CCTV implementations. Metrics such as correlation coefficient, bitrate overhead, and histogram analysis further validate the approach's robustness against statistical attacks.**

***Keywords*—Closed-Circuit Television (CCTV); decryption; encryption; internet of things (IoT); security**

I. Introduction

amanpreet.kaur@chitkara.edu.in (A.K)There has been a noticeable advancement in video surveillance systems with the blend of IoT and CCTV systems. Remote monitoring and real-time analytics are one of the major benefits of this integration. Besides the positive aspects, the crucial problem here is to fortify the security of IoT-based CCTV video surveillance systems [1],[2]. The proliferation of IoT devices, specifically CCTV cameras has led to the tremendous rise in IoT generated data. A lot of security issues have been caused by large volume of generated data. The most crucial issues are unauthorized access, breach of privacy, and data leaks that affect the confidentiality of IoT data [3],[4]. Maintaining data integrity is essential to tackle these security related issues. After data integrity, another important aspect of data security is confidentiality, as information captured by CCTV cameras is highly sensitive. To maintain confidentiality, and to provide unauthorized access, reliable communication methods, and optimized encryption and decryption methods are highly required [5],[6],[7]. The security issues raised by the combination of IoT and CCTV need constant research and preventive strategies to overcome increasing security issues.

Video data has been secured using conventional encryption methods such as DES (Data Encryption Standard), RSA (Rivest–Shamir–Adleman), and AES (Advanced Encryption Standard). The purpose of these encryption techniques is to shield data by making it unintelligible to those lacking the decryption key. Encrypting whole video streams or files can protect them from unauthorized access. However, there are several limitations to this encryption method, especially when it comes to transmission latency and processing overhead. The primary issue encountered by CCTV systems is the storage and bandwidth demands related to video data. Modern HD (high definition) cameras produce substantial volumes of video data, requiring the implementation of compression methods to decrease file sizes for effective storage and transmission. The compression techniques H.264 and H.265 are two established standards for video data compression due to their ability to substantially decrease the size of video files without compromising the video quality. The use of compression and encryption to strengthen video surveillance system security has been the subject of a great deal of research. Most of the early work centered on full encryption techniques, that is applying conventional cryptographic algorithms to video streams, such as AES or RSA. However, the enormous computational cost of encrypting full video was a considerable challenge, especially for real-time applications like CCTV systems.

Selective encryption has come out as a highly promising approach to tackle these issues. Studies showed that substantial computational reductions can be attained without compromising the security of a video by selectively encrypting the most crucial or sensitive portions of a video. Early researchers, such as Meyer and Gadegast (1995) introduced progressive selective encryption methods for MPEG video streams. Those methods focused on encrypting only the I-frames (intra-coded frames) while allowing P-frames (predicted frames) and B-frames (bi-directional frames) to remain

*Corresponding Author, Email ID: ygulzar@kfu.edu.sa (Y.G.), amanpreet.kaur@chitkara.edu.in (A.K) unencrypted. While this technique decreased the computing burden, it also led to the potential vulnerability of the unencrypted sections of the video to attacks. The research has expanded upon these principles by investigating methods to strengthen selective encryption by enhancing sensitive content detection in video streams.

Although selective encryption methods have shown excellent results, there are still certain issues and challenges in maintaining the security and effectiveness of CCTV systems. One of the major issues is computational overhead. Implementing complete encryption of CCTV videos using standard cryptographic methods is computationally complex, leading to performance issues in real-time systems, particularly those with low processing resources. Another major issue is the storage and bandwidth limitations of CCTV devices. Videos obtained by high-resolution surveillance systems require considerable storage capacity and bandwidth, thereby requiring the implementation of compression methods. Nevertheless, combining compression and encryption presents additional issues in preserving the security and integrity of CCTV video. The efficiency of selective encryption techniques is also a major issue among all as most of the selective encryption techniques cannot provide a secure and efficient solution. When only a selected piece of a CCTV video is encrypted, it can expose the other portions to attack, particularly in situations where unencrypted data might be used to deduce critical information.

Therefore, the objective of the study is to strenghten the security of CCTV video surveillance systems by boosting data integrity. Therefore, this study presents substantial results and highlights the importance of security in IoT based CCTV video monitoring systems. Providing users with reliable data and practical solutions to protect the safety and durability of their digital data is the primary goal [8],[9]. To better understand the complex aspects of this security problem, research is being done on data integrity, confidentiality, and the dynamic management of cyber threats. Robust security measures are necessary to counter possible risks including illegal access, data breaches, and privacy infringements, as this increase in data often contains sensitive information [10],[11].

This paper is structured as follows. First the introduction is defined, then "Related Work" reviews the existing literary works."Proposed Scheme" is the next section that addresses the suggested approach. The experimental findings are presented in "Experimental Results and Discussion," which also illustrates the system's suggested output. Lastly, we covered the conclusion in the last section.

II. Related Work

Gbashi et al. [12] proposed a novel, lightweight encryption technique for video frames that makes use of the ChaCha20 algorithm and a hybrid chaotic system. While 2D chaotic systems expand key space, the chaos system is used to produce encryption and seed keys. The encryption algorithm is effective against statistical attacks as shown in the results. The suggested approach is efficient in statistical measures and encryption effectiveness. Still, there is a need to apply this method to high-quality videos to reduce complexity so that it can be used in real time applications.

To further improve the encryption technique, Cheng et al. [13] proposed a selective video encryption method that relies on the integration of four-dimensional hyperchaotic systems and a video coding algorithm. This scheme works in two modes. One for the small encrypted data and less security required and the other for the large amount of encrypted data and sufficient real time security. According to the author's findings, this scheme is better than other existing video encryption methods in performance and encryption efficiency. But still, this method lacks real time implementation as all the results are proved by theoretical analysis only.

Lee and Park [14] discussed the importance of machine learning in the continuous growth of CCTV video surveillance systems. The efficiency of surveillance systems is enhanced by using cloud based video monitoring systems, but privacy and security issues become major concerns. Therefore, for processing CCTV video data, blockchain based method is proposed that not only ensures privacy but also synchronizes large volumes of video data. The proposed method supports the delta update function and is durable against attacks by encrypting transmitted data and thus suitable for intelligent video surveillance systems as it reduces the bandwidth required for transmission. But for real time implementation, more accurate video analysis will be required.

To provide reliable security for multimedia data, El-Shafai et al. [15] proposed a 3DV compression-encryption system for IoT wireless networks. This scheme employs compression and a robust encryption algorithm using symmetric keys. The proposed scheme demonstrated several advantages, including easy implementation, high key sensitivity, efficient encryption for video and image data, and resistance against various network attacks. Simulation results confirm its efficiency against different attacks, making it suitable for securing IoT multimedia applications. But still, there is a need to test this method on different IoT networks and also for real time multimedia applications.

To improve the security and privacy of CCTV surveillance systems Sivalakshmi et al. [16] suggest an approach that combines the Privacy Region Mask Separation method and an adaptive silhouette-blur scheme. These techniques help to identify sensitive regions in video frames while ensuring the privacy of video data. To further enhance the privacy protection process, an optimized version of the Coati optimization is integrated with these techniques. To further improve data storage and access, H.264/AVC standard is used for video encoding. This method performs better than RSA and ECC if talking about encryption, decryption speed, and quality preservation, but did not apply to real time data.

A new method has been proposed by Yu and Kim [17] to overcome the limitations of the traditional Region of Interest (ROI) encryption process in high-efficiency video coding (HEVC)/H.265. Encryption is applied to wider areas using traditional methods that result in the inefficiency of resources. Therefore, specific coding units are encrypted in the proposed method to improve encryption speed and reduce computation. But this method is limited to specific coding standards, and not applied to real world data.

To improve data security, the effectiveness of the selective encryption method is evaluated and processing overhead is reduced. The effect of selective encryption on data security, integrity, and accessibility is quantified. The literature review with contributions and limitations is depicted in Table I. The main aim of this paper is to optimize security and performance by analyzing encryption algorithms when applied to certain video segments. The findings will contribute in the comprehension of the efficiency of selective encryption in securing confidential data and optimizing computational capacity.

TABLE I LITERATURE REVIEW WITH CONTRIBUTIONS AND LIMITATIONS

References	Techniques	Contributions	Limitations
[12]	ChaCha20 algorithm and a hybrid chaotic system	• Effective against statistical attacks	• Not applicable in real time applications.
[13]	Selective video encryption method	• Performance and encryption efficiency	• Not applicable in real time applications.
[14]	Blockchain based method	• Suitable for intelligent video surveillance systems as it reduces the bandwidth required for transmission	• Not applicable in real time applications, • More accurate video analysis will be required
[15]	3DV compression-encryption system	• Easy implementation, • High key sensitivity, • Efficient encryption for video and image data, and • Resistance against various network attacks	• Not tested this method on different IoT networks and • Not tested for real time multimedia applications.
[18]	H.266/VVC (Versatile Video Coding) with a layered multiple tree structure	• Enhanced Compression Efficiency • Low Latency Streaming • Bandwidth Reduction	• Increased Computational Requirements • Scalability Challenges • Trade-offs in Quality and Efficiency
[16]	Privacy Region Mask Separation method, an adaptive silhouette-blur scheme, and Improved Coati Optimization Algorithm with H.264/AVC standard	• Enhanced Privacy Protection • Optimized Performance • Efficient Video Encoding and Storage • Improved Encryption and Decryption Speed • Higher Image Quality	• Lack of Real-Time Data Validation • Limited Scope of Video Scenarios • Computational Complexity • Restricted Focus on Privacy Regions
[17]	Coding Unit (CU)-Based Encryption, Region of Interest (ROI) Detection using YOLOv4, and HEVC/H.265 Video Encoding	• Selective Encryption for Improved Efficiency • Enhanced Privacy Protection Improved Video Quality Reduction in Encryption Time and Resources	• Limited to Specific Video Coding Standards • Increased Complexity in Real-Time Scenarios • Limited Testing on Real-World Data

III. METHODOLOGY

The proposed methodology addresses data security and privacy concerns in CCTV surveillance systems. The main goal is to strengthen CCTV security by using selective encryption methods. Fig. 1 depicts the flowchart for the cryptography process. This method encrypts specific parts of the video, protecting sensitive information and maintaining access to critical data for real-time analysis. The methodology is designed to optimize computational overhead and ensure the safety of user data. The steps for methodology are given below and the compression and selective encryption process for IoT CCTV video data is depicted in Fig. 2.

A. *Data Preparation*

A dataset of CCTV footage was collected from an 1800 square feet area, including indoor and outdoor cameras, with different lighting conditions and camera angles to reflect real-world surveillance scenarios.

The captured CCTV videos have different sizes, resolutions, lengths, frame counts, and frame rates to meet real world needs.

1) Compression using H.264/AVC (Advanced video coding): CCTV video was compressed using the H.264/AVC video compression standard, a widely adopted standard for video compression.

High compression efficiency is achieved with H.264/AVC as both spatial (within a single frame) and temporal (between successive frames) redundancies are removed, reducing file size while maintaining quality.

Bitrate, one of the crucial compression parameters, was varied to balance compression level and video quality. Lower bitrates were used to minimize storage space while maintaining sufficient quality for real-time surveillance needs.

B. *Dynamic Key Management*

Develop a dynamic key management system that generates and manages encryption keys. These keys should be unique to each encrypted portion, ensuring adaptability to changing security requirements and user preferences. The dynamic nature of key management enhances the overall security posture of the system.

C. *Selective Encryption Technique*

The Selective Encryption Technique is used to encrypt only the determined video frames. Unlike traditional methods that encrypt the entire stream, this approach strategically targets specific elements based on frame interval, reducing the computational burden and preserving critical information for real-time analysis.

The AES-256 (Advanced Encryption Standard) algorithm was used for encryption as it balances security and computational efficiency.

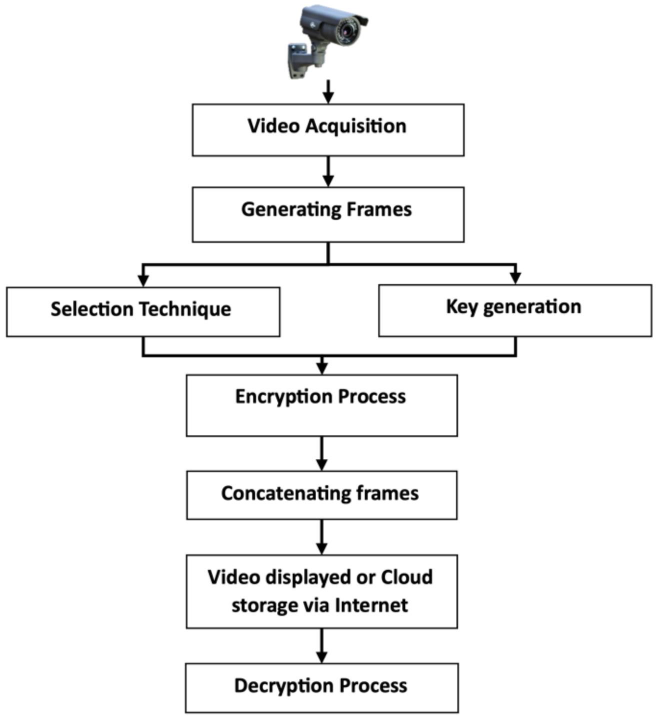


Fig. 1. Cryptography process.

D. Performance Evaluation

The system was evaluated based on the following metrics to assess both video quality and encryption performance:

1) *Entropy*: This metric measures how much disorder or information is present in the image. Higher entropy means more pixel complexity, whereas more regular patterns are an indication of lower entropy.

2) *Correlation analysis*: The correlation coefficient describes the relationships between adjacent video frames and the distribution of pixels. The lack of association between frames indicates that there is no pattern at all, making statistical cryptanalysis impossible.

3) *Bit rate overhead analysis*: The bit rate overhead measures the variation in bit rate before and after encryption. This demonstrates how well the encryption method reduces file size.

4) *Encryption efficiency*: The time taken for both the compression and selective encryption processes was measured to ensure the method is feasible for real-time CCTV applications.

5) *Decryption efficiency*: The time taken for decryption processes was measured to ensure the method is quickly and easily retrieves encrypted video footage and well suited for real-time CCTV applications.

6) *Histogram analysis*: Using the pixel distribution in each frame, the histogram analysis describes the visual relationships between the original and encrypted frames. Typically, cryptanalysts use the distribution of pixels to carry out statistical attacks.

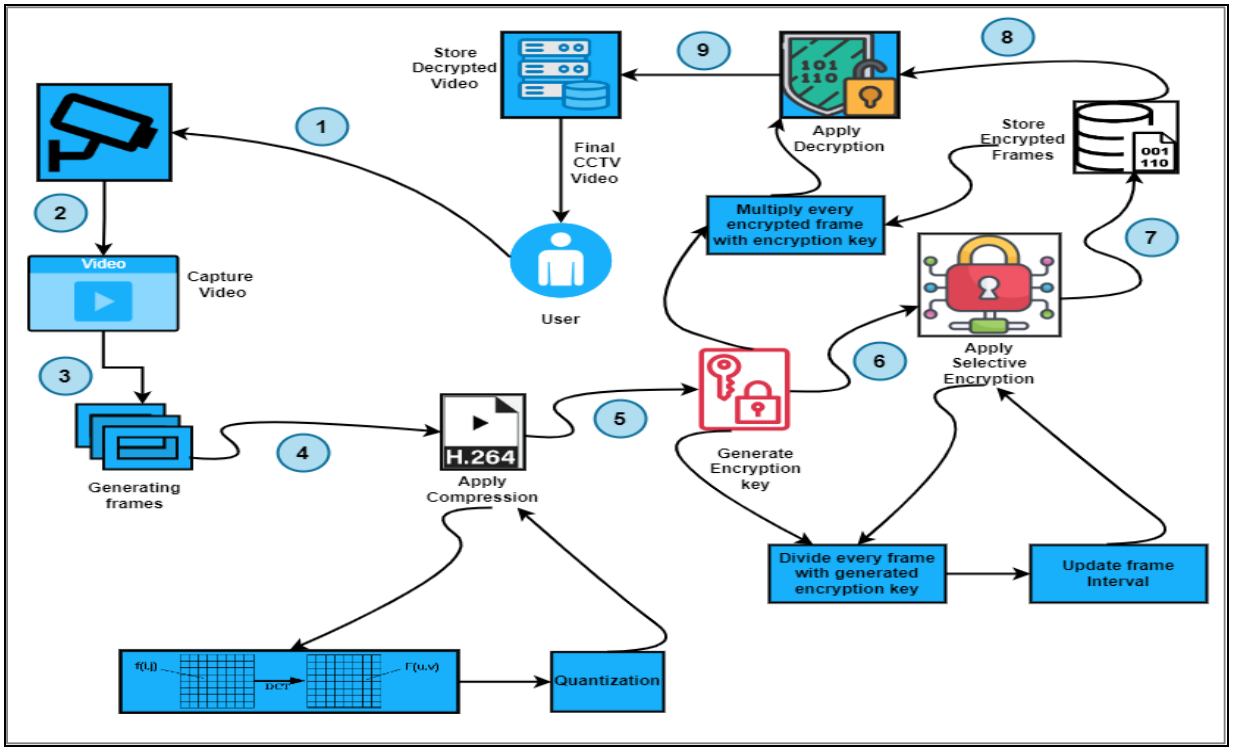


Fig. 2. Compression and selective encryption process for IoT CCTV video data.

IV. Proposed Algorithm

A systematic approach is applied to optimize data size and protect video data by using the proposed video encryption and compression algorithm. First, video frames are compressed to optimize their efficiency in terms of storage. Subsequently, the selected video data is encrypted with a randomly generated key to protect its confidentiality and integrity. The decryption process is carried out after encryption to retrieve the original content. The entire process is simplified as it enables the safe transfer and storage of video frames without additional decompression. Fig. 3 describes the flowchart for the proposed Algorithm 1.

Algorithm 1: Proposed Algorithm	
Step1: Read Original Video Frames	• O = {O1, O2, ..., On}
Step2: Initialize Variables	• x2 = 15 • x = frames per second (FPS)
Step 3: Compression Operation	For each frame Oi in O: • Compress every frame Oi by compression algorithm
Step 4: Encryption Key Generation	• Generate a random key matrix (K).
Step 5: Encryption Operation	For each frame Oi in O: • Calculate x1 = $int(current\frac{frame}{x} + 3)$ • Encryption operation: $Ei[x,y] = Oi[x,y]/K[x,y]$ • Update x2 = x2 + 15
Step 6: Create Encrypted Video Frames	• E = {E1, E2, ..., En}
Step 7: Decryption Operation	For each decrypted frame Di in D: • Decryption operation: $Di[x,y]=Ei[x,y]×K[x,y]$

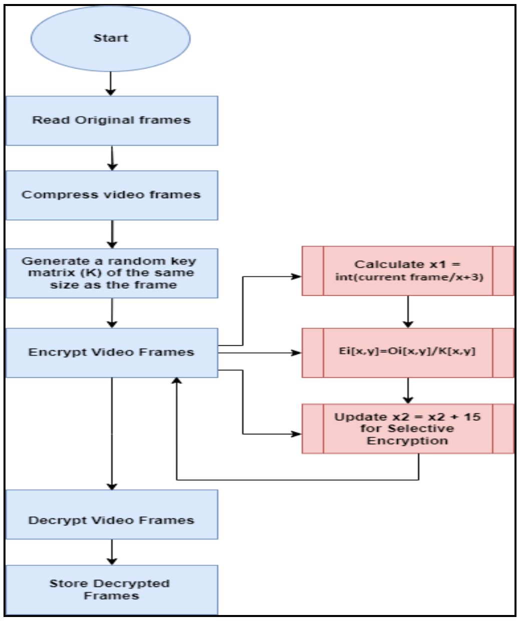

Start
Read Original frames
Compress video frames
Generate a random key matrix (K) of the same size as the frame
Encrypt Video Frames
Calculate x1 = int(current frame/x+3)
Ei[x,y]=Oi[x,y]/K[x,y]
Update x2 = x2 + 15 for Selective Encryption
Decrypt Video Frames
Store Decrypted Frames

Fig. 3. Flowchart for the proposed algorithm.

V. Experimental Results and Evaluation

The proposed scheme analyses five CCTV videos from different cameras that are described in Table II. The captured CCTV videos have different sizes, resolutions, lengths, frame counts, and frame rates. The need for higher resolution, longer recording time, or considerations for storage space are specific requirements of the surveillance system. The experimental run on Intel Core i5 CPU @ 2.4GHz and 8 GB RAM on Windows 10 OS.

In this experiment, an 1800 square feet area in the front and garden is considered, and an encryption technique is used to optimize security. To evaluate the efficiency of the proposed system, five cameras were positioned in important areas. To evaluate the algorithm's capacity by optimizing encryption time and storage efficiency and its effect on data security is the main aim of this paper. Results showed how well the encryption system protected CCTV video and optimized security.

TABLE II DIFFERENT CCTV VIDEOS

CCTV Video	Video size(KB)	Video Length (seconds)	Frame Count	Frame Rate/sec	Resolution
CCTV1	2528	29	731	25	640×352
CCTV2	6028	30	756	25	848×480
CCTV3	4942	24	604	25	848×480
CCTV4	2429	23	357	15	352×288
CCTV5	2538	24	363	15	352×288

A. *Compression*

CCTV video files are compressed to reduce file size to maximize storage before encryption. With this process, important information is retained and unnecessary information is removed. The file size is reduced by using compression techniques to reduce file size without reducing quality. Various compression algorithms are available to reduce the size of a video. Intra-frame and Inter-frame compression techniques are the most widely adopted techniques. Intra-frame compression which reduces the size of individual frames by using spatial redundancy within specific frames and is implemented by Discrete Cosine Transform (DCT) and Wavelet Transform. In the DCT method, pixel data is transformed into a set of low and high frequencies, whereas wavelet transform as the name suggests uses wavelets to convert the pixel data into wavelet coefficients to reduce the precision of less important data. On the other hand, Inter-frame compression uses temporal similarities to decrease the redundancy between frames. Methods used for Inter-frame compression are Motion Estimation and Compensation, Predictive and Transform Coding. Motion Compensation stores only the variation between frames where motion is detected. Predictive coding uses prediction from the previous encoded frame and the next frame. On the contray transform coding, a frame is transformed, and then transformed coefficients are quantized and encoded.

Modern video standards such as H.264/AVC (Advanced Video Coding) and HEVC (High-Efficiency Video Coding) or H.265 are combined with these compression techniques to balance video quality and compression. Higher compression efficiency is achieved by HEVC, but advance hardware is required to implement this in CCTV. Therefore H.264/AVC is used in the proposed algorithm to balance between compression and quality, and it supports existing hardware and software. The selective encryption algorithm is used after compression to protect the data from manipulation or unwanted access. This combined approach ensures effective storage, less bandwidth requirements, and enhanced CCTV security.

B. *Entropy*

The degree of unpredictability or randomness in the video frame's pixel values describes entropy. It measures how much disorder or information is present in the image. Higher entropy means more pixel complexity, whereas more regular patterns are an indication of lower entropy[19]. Entropy of different CCTV videos is shown in Table III.

The following formula can be used to calculate entropy(H):

$$H=-\sum ni=1\ Pi*\log2(Pi)$$

Where:

- n is the count of unique pixel values in the frame.
- Pi is the probability of occurrence of each unique pixel value.

TABLE III ENTROPY OF DIFFERENT CCTV VIDEOS

CCTV Videos	Entropy of the frame(bits per pixel)
CCTV1	7.6841
CCTV2	7.7560
CCTV3	7.7914
CCTV4	7.6794
CCTV5	7.0398

The frame may contain diverse patterns, textures, or information. Higher entropy is generally considered good for encryption. It suggests that the pixel values in the frame are more random and less predictable, which aligns with the goal of encryption, thus making the content difficult to discern without the decryption key.

Fig. 4 makes it clear that, out of all the CCTV feeds, CCTV3 has the highest entropy. The entropy values which are closer to eight is considered to be an ideal value as highlighted by Gbashi et al. [12]. The reason for this increased entropy is that CCTV3 comes from the front door camera, which records a feed with more diverse material. CCTV5, on the other hand, has the lowest entropy due to the backyard camera. The reason is less amount of variation in information is captured resulting in a more uniform feed and lower entropy. The changes in entropy levels of the CCTV videos depend upon different video quality, camera placement, and scene detailing.

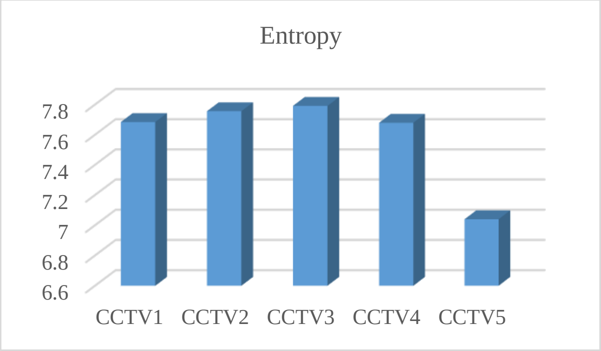


Fig. 4. Frame entropy (bits per pixel).

C. *Correlation Analysis*

The correlation coefficient describes the relationships between adjacent video frames and the distribution of pixels. The correlation value tells the relationship between neighboring frames. A higher correlation value means a closer linear link and a lower correlation value defines a more nonlinear relationship [12]. The correlation between pixels at matching positions is calculated in adjacent frames, and then a new frame with less data is created using the variations between them. Using this method results in a near-zero correlation value and a nonlinear relationship between neighboring frames.

Table IV presents the experimental results for nearby frame correlation coefficients for both the original and encrypted frames. These findings imply that the original and encrypted frames show very little association. As a result, this lack of association indicates that there is no pattern at all, making statistical cryptanalysis impossible.

A correlation coefficient that is close to zero, like in the case of CCTV1 frame 50, CCTV2 frame 50, CCTV3 frame 10 of CCTV3, CCTV4 frame 100, and CCTV5, denotes the lack or very weak linear relationship between the original and encrypted frames depicted in Fig. 5. The correlation coefficient is a statistical measure that expresses the direction and intensity of a linear relationship between two variables. Values that are close to 0 in this context indicate that there is little to no linear relationship between the encrypted and original frame contents. This is good news for encryption because it means that the content of the original frame is successfully hidden during the encryption process. The more closely the correlation coefficient approaches zero, the more skillfully the encryption process masks any observable links or patterns in the data as described by Gbashi et al. [12]. A negative correlation coefficient in the context of encryption would still suggest that the relationship between the original and encrypted frames has been effectively obscured by the encryption process, making it challenging for an observer to deduce the original frame's content from the encrypted frame without the decryption key.

TABLE IV COMPARISON SIMULATION RESULTS OF THE CORRELATION COEFFICIENT

Random Frames	CCTV1	CCTV2	CCTV3	CCTV4	CCTV5
Frame 0	-0.001182	0.0003209	-0.0004950	0.0003168	0.0019212
Frame 10	-0.001530	0.00019326	-0.0001918	0.0019271	0.0027840
Frame 50	-0.000273	-0.0005638	-0.0006569	-0.0025389	0.0009055
Frame 100	-0.001595	-0.0033022	0.0006837	-0.0022497	0.0007022

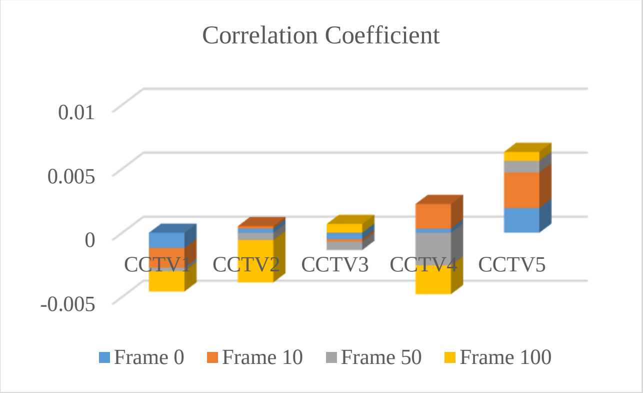


Fig. 5. Comparison results of the correlation coefficient.

D. Bit Rate Overhead Analysis

The bit rate overhead measures the variation in bit rate before and after encryption It is expressed as a percentage change relative to the original bit rate as stated in Table V. The sign of the overhead value indicates the direction of the change.

1) Negative bit rate overhead: A negative overhead number indicates a drop in the bit rate after the operation. Negative overhead in the context of video compression or encryption means that the processed video uses fewer bits than the original, which lowers the file size or bit rate. In general, this is preferable since it suggests effective encryption without appreciable quality loss. Negative overhead in video encryption reduces bit rate, resulting in smaller files and better quality without significant loss of quality.

2) Positive bit rate overhead: Positive overhead in video encryption indicates an increase in bit rate, possibly due to additional data added, potentially indicating a need for quality improvement or security measures. Often, the objective is to accomplish efficient encryption or compression while limiting the influence on file size and preserving a sufficient level of video quality [20].

The bit rate is reduced by 90% in the first video, and by more than 40% in all other scenarios seen in Fig. 6. This implies that the video file was significantly compressed without sacrificing the visual quality. This demonstrates how well the encryption method reduces file size. In general, negative overhead levels are better since they show a reduction in file size or bit rate without noticeably lowering quality as suggested by Chen et al. [20].

TABLE V BIT RATE OVERHEAD OF DIFFERENT CCTV VIDEOS

Video	Original	Encryption	Overhead
CCTV1	712000	650000	-0.9087
CCTV2	1644000	630000	-0.6167
CCTV3	1685000	609000	-0.6385
CCTV4	827000	487000	-0.4111
CCTV5	864000	488000	-0.4351

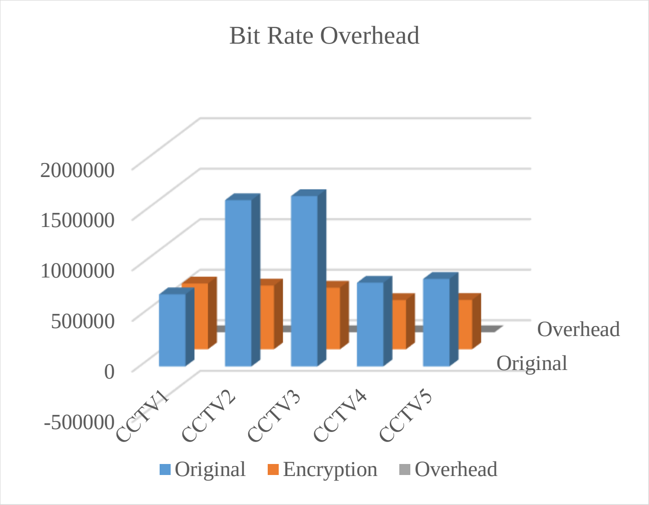


Fig. 6. Bit rate overhead of different CCTV videos.

E. Encryption Efficiency

Video encryption time overhead is dependent on various aspects, including the encryption algorithm, frame rate, resolution, and compression format. Encryption takes longer in videos with higher resolution and frame rate. Encryption time is affected by many factors. One is Compression as it adds more steps to the processing and the others are the security level, key length, complexity of the video, and encryption algorithm used. Besides these, buffering and network performance are crucial where real-time encryption is done [21]. The encryption time overhead in CCTV surveillance applications is optimized as described in Table VI and it is clearly shown in Fig. 7.

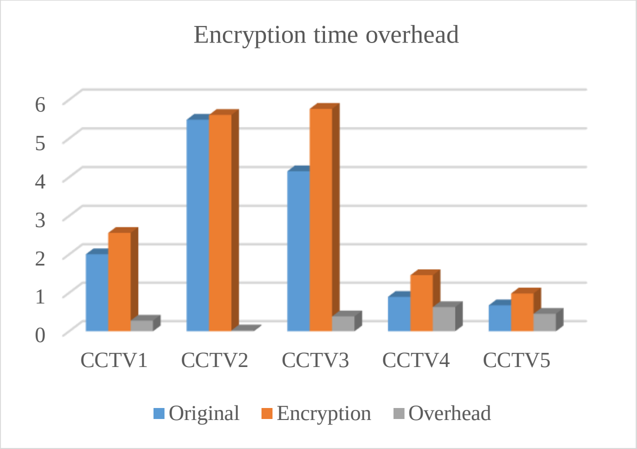


Fig. 7. Encryption time overhead of CCTV videos.

Table VII presents the encryption speed for five different CCTV videos and describes the variation in encryption efficiency for randomly chosen frames. This eventually helps to effectively safeguard sensitive video data in real-time surveillance scenarios.

TABLE VI ENCRYPTION TIME OVERHEAD OF DIFFERENT CCTV VIDEOS

Video	Original	Encryption	Overhead
CCTV1	2.0040	2.5594	0.2771
CCTV2	5.4845	5.6084	0.0225
CCTV3	4.1545	5.7645	0.3875
CCTV4	0.8952	1.4594	0.6302
CCTV5	0.6766	0.9837	0.4538

TABLE VII RESULT OF ENCRYPTION TIME (IN SECONDS) FOR DIFFERENT CCTV FRAMES WITH AVERAGE ENCRYPTION TIME

CCTV Videos	Frame 0	Frame 50	Frame 100	Frame 150	Average
CCTV1	0.04803	0.03464	0.03753	0.03357	0.00171
CCTV2	0.08812	0.06305	0.05923	0.05731	0.00261
CCTV3	0.12913	0.05824	0.05576	0.05399	0.00245
CCTV4	0.04807	0.02142	0.02138	0.02554	0.00179
CCTV5	0.03423	0.02149	0.01954	0.01931	0.00178

Fig. 8 provides a comparative comparison of the encryption speed times for randomly picked frames from different CCTV videos, expressed in frames per second. Interestingly, every CCTV video shows varying encryption speed performances at various frame rates, that is due to the randomness of pixels in every frame as every video is from a different CCTV video. When compared to other CCTV movies in the dataset, CCTV1, CCTV4, and CCTV5 perform better on average, with the quickest encryption speed time of 0.00171, 0.00179, and 0.00178 respectively frames per second. The encryption algorithm being utilized is one of the possible causes of these variances in encryption speed timings. With the fastest and most reliable encryption speeds, CCTV5 is the best choice for real-time applications. Reliability is further demonstrated by CCTV4 and CCTV1, with low and constant encryption times. Given the variations in video size and resolution, CCTV2 and CCTV3 nevertheless offer performance appropriate for real-time applications despite longer encryption periods as demonstrated by Alawi and Hassan [22].

F. Decryption Efficiency

The proposed algorithm uses optimized decryption procedures that are specially designed for the chosen encryption technique in order to prioritize decryption efficiency. The information displayed in Table VIII and Fig. 9 demonstrates how well the algorithm performs in terms of decryption efficiency and speed. By use of enhanced decryption algorithm and effective cryptographic key management, the algorithm guarantees the prompt restoration of original content without sacrificing security. As a result, the method is particularly effective in decrypting data, making it possible to quickly and easily retrieve encrypted video footage.

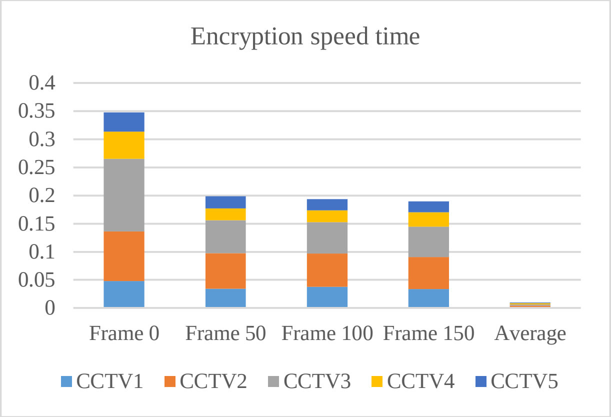


Fig. 8. Result of encryption time (in seconds) for different CCTV frames with average encryption time.

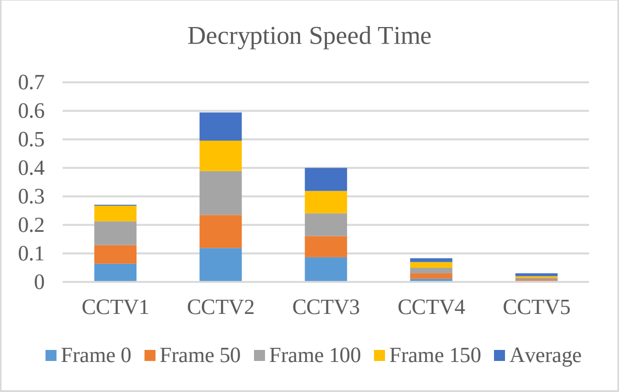


Fig. 9. Result of decryption time (in seconds) for CCTV video frames.

TABLE VIII RESULT OF DECRYPTION TIME (IN SECONDS) FOR DIFFERENT CCTV VIDEO FRAMES

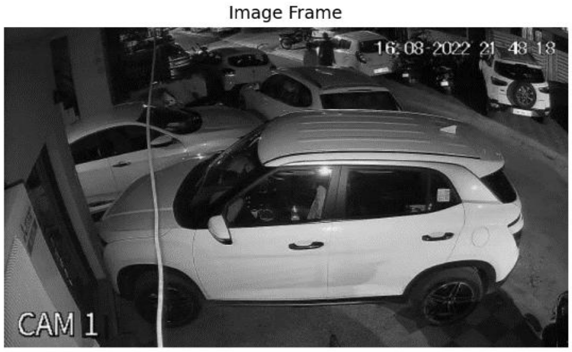
CCTV Videos	Frame 0	Frame 50	Frame 100	Frame 150	Average
CCTV1	0.06465	0.06517	0.08280	0.05468	0.00400
CCTV2	0.11907	0.11594	0.15378	0.10657	0.09978
CCTV3	0.08690	0.07434	0.07906	0.07852	0.08153
CCTV4	0.01116	0.01973	0.01913	0.01973	0.01409
CCTV5	0.00499	0.00399	0.00618	0.00573	0.00930

Every CCTV video is suitable for real-time applications; the reasons for variations in decryption durations are related to the sizes and formats of the videos. CCTV5 regularly has the smallest decryption timings (0.00399 to 0.00618 seconds), while CCTV2 consistently has the highest decryption times (0.10657 to 0.15378 seconds). With the fastest, most reliable decryption times, CCTV5 exhibits the best performance. Additionally dependable and with quick decryption times is CCTV4. While CCTV3 and CCTV2 have longer and more inconsistent decryption times but are still appropriate for real-time application as described by Alawi and Hassan [22].

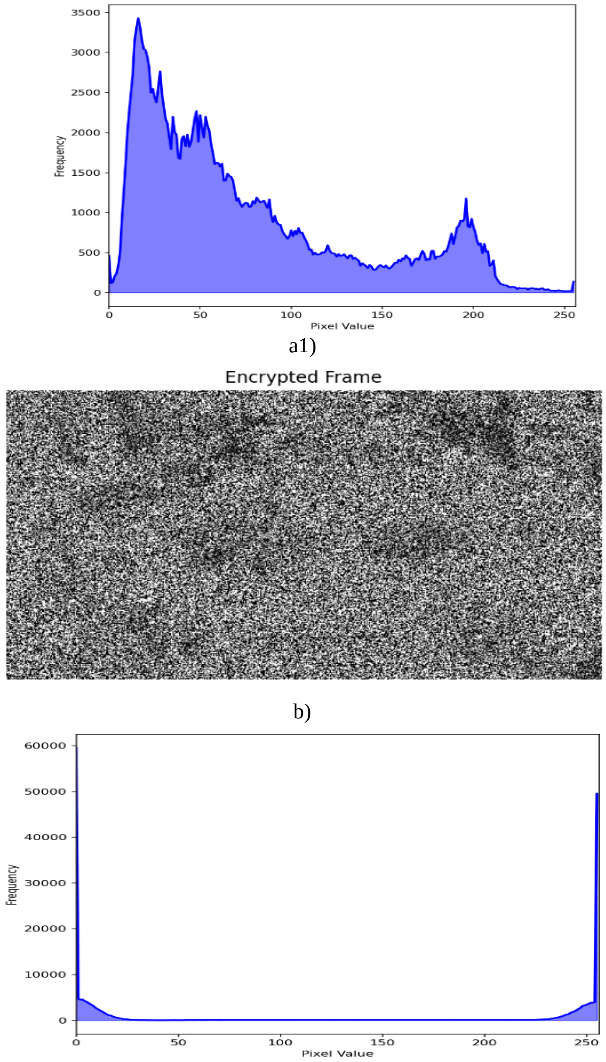
G. Histogram Analysis

Using the pixel distribution in each frame, the histogram analysis describes the visual relationships between the original and encrypted frames. In an attempt to recover the original frames, statistical attacks try to take advantage of this predicted relationship. The notable differences between the encrypted frame histograms and the original frame histograms highlight how well the encryption approach works to fend off statistical attacks [23]. The chi-square test is used to demonstrate the homogeneity of pixels and is used in the study of the histogram.

Typically, cryptanalysts use the distribution of pixels to carry out statistical attacks. It is clear from the figures how the original and encrypted video frames' histograms differ from one another. This prevents statistical attacks on the video frames. The original video frame is shown in Fig. 10(a) of the supplied figures, while Fig. 10(a1) shows the histogram of the frame before encryption. The histogram of the encrypted video frame (b) is shown in Fig. 10(b1). These figures make it clear that the histograms of original and encrypted video frames are distinct. This implies that video frames are secured against any statistical attacks as stated by Ravikumar and Kavita [24].



a)



a1)

b)

b1)

Fig. 10. a) Original frame, a1) Histogram of the original frame, b) Encrypted Frame, b1) Histogram of encrypted frame.

VI. COMPARATIVE ANALYSIS AND DISCUSSIONS

The experiments are carried out to compare the results with state-of-the-art algorithms to confirm the suggested scheme efficiency for CCTV video security. Encryption time, decryption time, and correlation coefficient results of the proposed technique are compared statistically with the algorithms from current related literature. For the tested CCTV videos, Table IX presents the numerical values of the proposed scheme for Encryption time and decryption time per frame in comparison to the suggested techniques in recent literature.

TABLE IX COMPARISON OF AVERAGE ENCRYPTION AND DECRYPTION TIME IN SECONDS

Reference	Average Encryption Time per frame	Average Decryption Time per frame
[25]	0.01219	0.01206
[15]	0.7306	0.6278
[26]	0.03549	0.03625
CCTV1	0.00171	0.00400
CCTV2	0.00261	0.09978
CCTV3	0.00245	0.08153
CCTV4	0.00179	0.01409
CCTV5	0.00178	0.00930

It can be seen from Fig. 11 that the encryption time of the proposed technique is better than what is proposed in the literature and very close to zero. Therefore, the proposed technique is successful in optimizing encryption time and is well suited for real time applications.

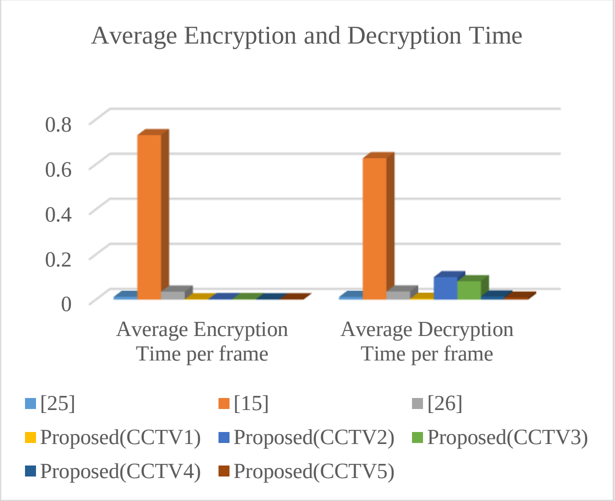


Fig. 11. Comparison of average encryption and decryption time (in seconds) for CCTV video frames.

The comparison of correlation coeficients with the recent literature are given in Table X. Moreover, it is also observed that correlation coefficient of the proposed algorithm is better than the schemes in literature as shown in Fig. 12. The correlation coefficients of the proposed scheme are very close to zero which prevents it from statistical attacks.

TABLE X COMPARISON OF CORRELATION COEFFICIENTS

Reference	Correlation Coefficient
[25]	-0.0045
[15]	-0.0029
[26]	0.00733
Proposed(CCTV1)	-0.0011
Proposed(CCTV2)	0.00032
Proposed(CCTV3)	-0.0004
Proposed(CCTV4)	0.00031
Proposed(CCTV5)	0.00192

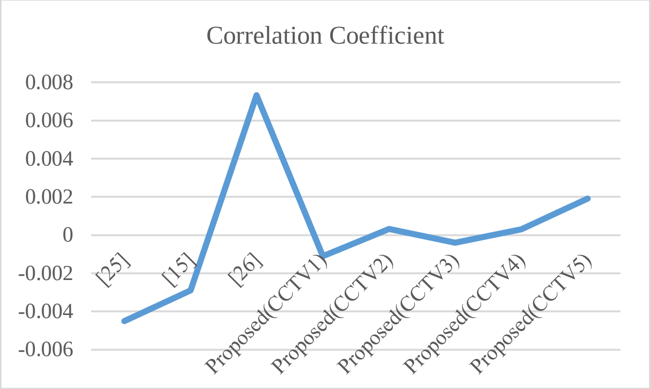


Fig. 12. Comparison of correlation coefficients for CCTV video frames.

The proposed technique works well according to different video resolutions, frame rates, or compression standards as encryption process is done after compression. Individual video frames are encrypted using our suggested frame-level selective encryption technique. This preserves adaptability across various video resolutions and frame rates while guaranteeing independence from video codecs and compression standards. This preserves adaptability across various video resolutions and frame rates while guaranteeing independence from video codecs and compression standards. Furthermore, scalability is demonstrated by the consistent performance across measured resolutions (640×352, 848×480, and 352×288), although frame rate differences mostly impact temporal density rather than the encryption process. Consequently, the design of the approach guarantees strong applicability across a variety of video setups and compression standards.

There are significant trade-offs when employing selective encryption in IoT CCTV devices. Higher video resolutions or frame rates result in a greater computational cost since more data must be processed, even though the proposed approach is quicker and more effective than encrypting the entire video. This may cause encryption on low-power IoT CCTV devices to lag. However, to minimize this trade-off, encryption, and decryption process is minimized. The technique is beneficial for real-time streaming because it avoids the delays associated with full encryption, making it suitable for real time applications. Overall, although there is a trade-off between computational speed and the volume of data being encrypted, the proposed technique effectively balances these needs for CCTV surveillance systems. At the same time, it maintains compression efficiency, which helps save storage.

By encrypting selected video data, the proposed selective encryption technique disrupts correlations in the video data and shows resilience against statistical attacks. The robust AES algorithm used in this technique has a strong cryptographic design that makes it naturally resistant to adaptive chosen-plaintext attacks. Because of the avalanche effect of AES, even a small alteration to the plaintext produces an entirely different ciphertext, making it nearly impossible for an attacker to deduce significant connections between the selected plaintexts and their matching ciphertexts, and even the encryption keys. The use of compression before encryption substantially strengthens the method's resistance to chosen plaintext attacks in the setting of selective encryption. Non-linear changes are applied to video data by using compression resulting in scrambling the data and eliminating redundancies in the plaintext frames. Because of this procedure, it is very difficult for an attacker to create plaintext frames that might expose ciphertext. In terms of key management, the technique is made to work with safe key distribution and exchange protocols that are used in real time environments such as Diffie-Hellman key exchange. In order to prevent attacks like key reuse or interception, these protocols offer safe methods for creating, allocating, and rotating encryption keys.

The method reduces risks in two ways for real-world attack scenarios where an adversary might try to deduce encrypted content from unencrypted frames or statistical redundancy. First, the attacker cannot reconstruct meaningful content from unencrypted frames alone since selective encryption is applied which disrupts important visual information. Second, applying compression before encryption removes correlations and redundancies from the CCTV video data and it further distorts patterns that may otherwise be exploited.

VII. Conclusion

This paper highlights significant discoveries and shows the importance of security in IoT based CCTV video surveillance systems. This study offers a new method for video encryption that combines selective encryption with compression to enhance security and efficiency. The approach is ideal for demanding real-time applications as demonstrated by experiments, since it can selectively encrypt data after compression, which minimizes computational overhead and hence guarantees efficient utilization of system resources. Through testing and analysis, the algorithm's effectiveness and resistance to statistical attacks is proven. Still, it needs constant monitoring and improvement to strengthen its defenses against new threats. With the promise of increased security in a world growing more and more data-centric, this study represents a major advancement in the support of video encryption techniques. In the future, adding authentication techniques to encryption will be crucial to enhancing security and guaranteeing that sensitive data is only accessed by authorized individuals.

Acknowledgment

This work was supported by the Deanship of Scientific Research, the Vice Presidency for Graduate Studies and Scientific Research, King Faisal University, Saudi Arabia under the project KFU250656.

Conflict of Interest

On behalf of all authors, the corresponding author states that there is no conflict of interest.

References

[1] A. Zhaxalikov, A. Mombekov, and Z. Sotsial, "Surveillance Camera Using Wi-Fi Connection," Procedia Comput. Sci., vol. 231, pp. 721–726, Jan. 2024, doi: 10.1016/J.PROCS.2023.12.147.

[2] Y. Myagmar-Ochir and W. Kim, "A Survey of Video Surveillance Systems in Smart City," Electronics (Switzerland), vol. 12, no. 17. Multidisciplinary Digital Publishing Institute, p. 3567, Aug. 23, 2023. doi: 10.3390/electronics12173567.

[3] A. Kumar, S. Sharma, N. Goyal, A. Singh, X. Cheng, and P. Singh, "Secure and energy-efficient smart building architecture with emerging technology IoT," Comput. Commun., vol. 176, pp. 207–217, Aug. 2021, doi: 10.1016/j.comcom.2021.06.003.

[4] D. Dhingra and M. Dua, "A chaos-based novel approach to video encryption using dynamic S-box," Multimed. Tools Appl., vol. 83, no. 1, pp. 1693–1723, Jan. 2024, doi: 10.1007/S11042-023-15593-6/METRICS.

[5] [5] J. Dai, Q. Li, H. Wang, and L. Liu, "Understanding images of surveillance devices in the wild," Knowledge-Based Syst., vol. 284, p. 111226, Jan. 2024, doi: 10.1016/J.KNOSYS.2023.111226.

[6] M. Surya Priya, D. Diana Josephine, and P. Abinaya, "IOT Based Smart and Secure Surveillance System Using Video Summarization," in Lecture Notes in Electrical Engineering, 2021, vol. 735 LNEE, pp. 423–435. doi: 10.1007/978-981-33-6977-1_32.

[7] S. Rani, S. H. Ahmed, and R. Rastogi, "Dynamic clustering approach based on wireless sensor networks genetic algorithm for IoT applications," Wirel. Networks, vol. 26, no. 4, pp. 2307–2316, May 2020, doi: 10.1007/S11276-019-02083-7/METRICS.

[8] C. segun ODEYEMI, B. A. OMODUNBI, O. M. OLANIYAN, and A. A. SOLADOYE, "INTERNET OF THINGS (IoT) BASED REMOTE SURVEILLANCE CAMERA FOR SUPERVISION OF EXAMINATIONS," LAUTECH J. Eng. Technol., vol. 18, no. 1, pp. 109–116, May 2024, Accessed: May 22, 2024. [Online]. Available: https://www.laujet.com/index.php/laujet/article/view/634

[9] M. Tahir, Y. Qiao, N. Kanwal, B. Lee, and M. N. Asghar, "Privacy Preserved Video Summarization of Road Traffic Events for IoT Smart Cities," Cryptography, vol. 7, no. 1, p. 7, 2023, doi: 10.3390/cryptography7010007.

[10] S. Gangadharaiah and L. B. Bhajantri, "Secure data dissemination and routing in Internet of Things," Int. J. Inf. Technol., pp. 1–18, Apr. 2024, doi: 10.1007/s41870-024-01848-4.

[11] M. Rana, Q. Mamun, and R. Islam, "Lightweight cryptography in IoT networks: A survey," Future Generation Computer Systems, vol. 129. North-Holland, pp. 77–89, Apr. 01, 2022. doi: 10.1016/j.future.2021.11.011.

[12] E. K. Gbashi, E. Shakir, A. Tariq Maolood, E. Khalaf Gbashi, and E. Shakir Mahmood, "Novel lightweight video encryption method based on ChaCha20 stream cipher and hybrid chaotic map Modeling carbon nanotubes with different structure at millimeter wavelength antennas View project Novel lightweight video encryption method based on ChaCha20 ," Artic. Int. J. Electr. Comput. Eng., vol. 12, no. 5, pp. 4988–5000, 2022, doi: 10.11591/ijece.v12i5.pp4988-5000.

[13] S. Cheng, L. Wang, N. Ao, and Q. Han, "A Selective Video Encryption Scheme Based on Coding Characteristics," Symmetry 2020, Vol. 12, Page 332, vol. 12, no. 3, p. 332, Feb. 2020, doi: 10.3390/SYM12030332.

[14] D. Lee and N. Park, "Blockchain based privacy preserving multimedia intelligent video surveillance using secure Merkle tree," Multimed. Tools Appl., vol. 80, no. 26–27, pp. 34517–34534, Nov. 2021, doi: 10.1007/s11042-020-08776-y.

[15] W. El-Shafai, A. K. Mesrega, H. E. Ahmed, N. Abdelwahab, and F. E. Abd El-Samie, "An efficient multimedia compression-encryption scheme using latin squares for securing internet of things networks," J. Inf. Secur. Appl., vol. 64, no. November 2021, p. 103039, 2022, doi: 10.1016/j.jisa.2021.103039.

[16] M. Sivalakshmi, K. R. Prasad, and C. S. Bindu, "Improved privacy protection technique for enhancing security of real-time video surveillance," J. Inf. Optim. Sci., vol. 45, no. 5, pp. 1389–1399, 2024, doi: 10.47974/jios-1711.

[17] J. Y. Yu and Y. G. Kim, "Coding Unit-Based Region of Interest Encryption in HEVC/H.265 Video," IEEE Access, vol. 11, pp. 47967–47978, 2023, doi: 10.1109/ACCESS.2023.3276243.

[18] S. Sharma, H. Jindal, A. Jain, S. Singh, and P. S. Binner, "Optimizing Video Compression and Transmission for Real-Time Applications," in 2023 IEEE Region 10 Symposium, TENSYMP 2023, 2023. doi: 10.1109/TENSYMP55890.2023.10223679.

[19] K. M. Hosny, M. A. Zaki, N. A. Lashin, and H. M. Hamza, "Fast colored video encryption using block scrambling and multi-key generation," Vis.

Comput., vol. 39, no. 12, pp. 6041–6072, Dec. 2023, doi: 10.1007/s00371-022-02711-y.

[20] C. Chen, X. Wang, G. Liu, and G. Huang, "A Robust Selective Encryption Scheme for H.265/HEVC Video," IEEE Access, vol. 11, pp. 17252–17264, 2023, doi: 10.1109/ACCESS.2022.3210132.

[21] J. Yun and M. Kim, "JLVEA: Lightweight Real-Time Video Stream Encryption Algorithm for Internet of Things," Sensors 2020, Vol. 20, Page 3627, vol. 20, no. 13, p. 3627, Jun. 2020, doi: 10.3390/S20133627.

[22] A. R. Alawi and N. F. Hassan, "A Proposal Video Encryption Using Light Stream Algorithm," Eng. Technol. J., vol. 39, no. 1B, pp. 184–196, 2021, doi: 10.30684/etj.v39i1b.1689.

[23] "Secure and Lightweight Encryption Model for IoT Surveillance Camera by Mohammed Abbas Fadhil Al-Husainy, Bassam Al-Shargabi :: SSRN." https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3591979 (accessed Nov. 26, 2022).

[24] S. Ravikumar and D. Kavitha, "IoT based home monitoring system with secure data storage by Keccak–Chaotic sequence in cloud server," Journal of Ambient Intelligence and Humanized Computing, vol. 12, no. 7. Springer, pp. 7475–7487, Aug. 02, 2021. doi: 10.1007/s12652-020-02424-x.

[25] A. Hafsa, M. Fradi, A. Sghaier, J. Malek, and M. Machhout, "Real-time video security system using chaos- improved advanced encryption standard (IAES)," Multimed. Tools Appl., vol. 81, no. 2, pp. 2275–2298, Jan. 2022, doi: 10.1007/s11042-021-11668-4.

[26] D. Jiang, T. Chen, Z. Yuan, W. xin Li, H. tao Wang, and L. liang Lu, "Real-time chaotic video encryption based on multi-threaded parallel confusion and diffusion," Inf. Sci. (Ny)., vol. 666, p. 120420, May 2024, doi: 10.1016/j.ins.2024.120420.