Advances
2024, Vol. 5, No. 3, pp. 84-92
https://doi.org/10.11648/j.advances.20240503.13

Research Article

Lightweight Encryption Model for IOT Security and Privacy Protection

Iqra Naz*, Rehmat Illahi, Neelam Shahzadi, Hafiz Gulfam Umer Ahmad

Department of Computer Science and Information Technology, Ghazi University, Dera Ghazi Khan, Pakistan

Abstract

We are witnessing the era of Internet of Things (IoT), where its applications such as smart cities and smart homes catch sensitive data gathered mostly by IoT surveillance cameras among other sensors or devices. Therefore, security and privacy protection is a key concern during transmitting such sensitive data across the IoT network to be processed and stored on Cloud. In this paper, we proposed a lightweight encryption model that complies with the limited resources of IoT devices in terms of process and memory. Also, the encryption model also provides a high level of security for the transmitted data through a constant change of the key used for encrypting of transmitted IoT data. In addition, the key size used to encrypt transmitted data in the proposed model is large enough which makes it hard to break by the attackers. The experimental results show outstanding results with an average of 150.5 ms of encryption time for a key size 80 bits where the key size is relatively large and with an average PSNR of 7.13 compared to other algorithms.

Keywords

Image Cryptography, IOT, Privacy and Security Preservation, Devices

1. Introduction

The Internet of Things (IoT) is quickly spreading and is projected to grow much quicker in the coming years, leaving prior innovation celebrations irrelevant. It is expected that by 2025, they will be over 25 billion linked Internet of things gadgets [1]. IoT devices, which are expected to connect every aspect of our lives, can be any technology, mechanical or digital device, or an object that can transmit and generate data in a network with no having to involve human or computer relationships, such as closed-circuit TV (CCTV) cameras, autos, and home devices, via device tags, sensors, actuators [2, 3]. The Internet of Contents (IoT) devices are designed to collect data and communicate it to other related IoT devices, where the data can be stored, examined, and accessed by anyone with a smart phone or tablet. IoT devices can detect, acquire, analyze, filter, and exchange data on a massive scale as a result. They also enhance the quantity of data collected, generated, saved, and exchanged between devices in the Internet of Things or the cloud. Each IoT device must have its own human being online identity in order to communicate consistently. Nowadays, with the significant progression in IoT empowering innovations starting with RFID, connectivity, Cloud, and Big data analytics have been presented in numerous fields and applications such as smart homes, smart cities, water, power, traffic control, surveillance. Due to the ability for public as well as private companies to privately and securely monitor buildings and public areas in immediate time

*Corresponding author: Iqran2756@gmail.com (Iqra Naz)

Received: 17 July 2023; **Accepted:** 4 August 2023; **Published:** 29 September 2024

using smart surveillance and safety IoT enabled solutions, the advent of Internet of Things (IoT) devices such as in-home or street camera surveillance has helped to build safer cities, homes, and communities. However, as it is possible to obtain information from IoT cameras or devices whenever this data is transferred to the cloud, such as photos of people's faces or car registration plate numbers among those checking zone, the security of such information is thus put at risk by the use of surveillance cameras in open areas. Furthermore, if the cameras are positioned within private spaces, such as houses, these places are open to surveillance recordings as well. In addition, these IoT gadgets may be used to track people's activities and conduct inside of their houses in real-time [4]. Sadly, the IoT sector has not given security and privacy concerns as much attention. IoT monitoring devices are anticipated to be placed in system often, making them easy targets and potentially the weakest link in an encrypted technology design [5].

However, the handling and analysis of the huge amount of such sensitive data generated by IoT camera footage is fraught with security and privacy issues, as well as worries about unauthorized people trying to access this private information [6-8]. With the development of IoT applications and the availability of cloud-based computing for the storage and analysis of data produced by IoT, intelligent towns are imminent. On the opposite end of the spectrum, there are certain problems with stored in the cloud applications for the IoT. Certain of these problems are related to security and latency, and they can be solved with the help of computing at the edge and fog technology paradigms that are presently in place [9-11]. The security problem for cloud-based applications is not suited for fog computing amenities that are visible to users or Internet monitoring systems due to the significant difference of fog and cloud services [12, 13].

The security issue can be solved using a number of encryption methods, however these techniques are unsuitable for internet of things devices with limitations.

Due to their limited memory and computation capacity, IoT devices usually played data only when someone crucial has been spotted or activated. The fog or edge nodes inside networks of IoT devices are used as a way of delegating the security issue, with the edges of the network handling data safety and analysis directly. Furthermore, in a broker-based architecture, any intermediate node can be set up as a broker to relay data among the sender and the subscriber. IoT devices as well as cameras may be programmed to be a MQTT manufacturer, while servers or the cloud needing to receive camera data can be established as MQTT subscribers. Therefore, the broker-based structure must ensure that the publisher's and subscribers' confidentiality is protected. Furthermore, some authentication techniques have taken into account the limitations of the Internet of Things by adopting a lightweight verification protocol and a system of public keys [14]. However, homomorphic safeguarding has freshly used since of its exceptional strength and capacity on operations of compromised data, but it is unsuitable to be employed within IoT coalitions due its computing cost [15, 16]. Consequently, any digital encryption approach to use for the data encryption of responsive data obtained by IoT devices like as surveillance photos should look at the goods open within IoT machines. Additionally, it need to be correctly fast to fulfil the needs of immediate time tracking photographs functions and also should be appropriate and useful techniques to provide security for these data given away IoT network [17-19].

As we are conscious of the constraints of IoT monitoring recording devices, the main achievement of this article is the discovery of a fast sufficient algorithms to encryption and decrypt immediate time broadcasting of photographs and video in respect of computing time and memory space. The recommended method in this paper offers a high amount of security for transmitted data by changing the key employed for encrypted transmitting data on a regular basis. In additionally the key strength used to encrypt communicated data in the recommended model is large sufficiently which making it hard to penetrate by the attackers. The balance of the paper is laid out as follows: The following part highlights the most relevant work. Section 3 offers a revised version of the proposed model's approach. Section 4 addresses the evaluation and testing of the suggested design, as well as compared to existing models. Finally, the fifth part draws a conclusion related to this article.

2. Related Work

A number of approaches have been given to address the challenge of safely transmitting information inside internet of things networks by taking into account the limited assets of IoT devices.

A lightweight method of encryption built around identifying Region of Interests (RoI) that employs binary sequences for each role in inside the presentation, with each role in block of the video functioning as the activation of an 8-layer Layered Cellular Automata (|LCA) [20]. knowing that each the layer of the LCA can be considered as a structure of a sequence of 1D CAs, the LCA's ultimate state may be changed to an each pixel grid of the password-protected RoI inside the video, with each RoI shut of the footage serving as the setup of an 8-layer of Layered Cellular Automation (|LCA) [20]. considering that each the layer of the LCA can be regarded as an arrangement of a progression of 1D CAs, a haphazardly picking the reversible Elementary Cellular Automata (ECA) standards for LCA training and then collecting the LCA's final state that may be transformed to a pixel grid of the image that is encrypted. They used half transform to provide improved perplexity of the encrypted picture and for each layer to function precisely as they did in previous layers. They also applied an inconsistent shift change to each 1D CA. The authentication process used in the aforementioned method allows users to access monitoring recordings on-demand. LCA-based encrypting using the fundamental concepts and modifications is inherently efficient and straightforward to implement since it is a fundamentally parallel system. Furthermore, each RoI is divided into a sequence of hexadecimal blocks, each of which is concurrently encrypted. Certainly, the technique conforms with the continuous functioning of surveillance equipment and protects the confidentiality of data collected by IoT cameras, but the computational expenses for such an approach is seen as a big issue given the capabilities offered among IoT devices. A. Adeel et al. offered an approach to the leaks of information through internet protocol (IP) traffic of IoT monitoring devices, even when the contents of the payload were secured [21]. They looked into the leaks through assessing network traffic characteristics such as size of packets and video bitrate. It is possible to look into them using metadata irrespective of whether a conventional encryption approach is employed for data passing from IoT surveillance cameras. They got to reach the conclusion that there is a breach of privacy in the camera's data. [22] Offered a Chaos-Based cryptosystem for encrypting surveillance camera streams. They use a medical case study in which a portable camera was used to monitor someone with diabetes and communicate encrypted real-time footage of the individual to a specified data facility. They utilised the chaotic map approach Arnold cat map, and their results show that encrypting and decrypting the film takes 0.0071 seconds. While the results are fantastic, chaos-based approaches are still not mature enough to be used for picture and video decryption when compared to plain text. Another lightweight solution encrypts real-time audio-visual data using a chaotic map, Chebyshev map, and a secure hashed to secure communication of audio-visual hearing-aid messages to the cloud, however their method requirements a lot of power and compute. The researchers of [23] devised a system for protecting visual medical data using the Feistel Encryption Scheme, an encryption standard called the Advanced Encryption Standard (AES), and a genetic technique to reduce computing time by using the GPU. This system was tested using IoT audiovisual medical data to compare encryption techniques such as MARS, RC6, 3-DES, DES, and Blowfish are in terms of computing running time and capacity for both encryption and decryption, as well as the avalanche effect. Their findings showed that their method has the smallest calculations time and highest capacity for the decryption and encryption procedures, as well as the highest avalanche effect as compared to current encryption methods; however, their approach does not work well with the decryption and encryption processes of live streaming of IoT surveillance cameras. In a smart city situation provided in [24], a security strategy for sending media packets using Internet of Things (IoT) networks was used. This safety approach is based on combining Identity, Route, or Location (IRL), as well as intermediate nodes, for the routing at the IoT sensor level, and for the overall security of the IoT network, they used and adapted Simple Algorithm for Data Security (PADS) [25] to be appropriate to the original standard of compressing video (HEVC) for multimedia file transmission. This technique was only employed on the query and answer communication paradigm involving the IoT instrument and the IoT network, not on the continuous transmission of sensor data pictures. An identification schema based on the use of public keys [14] was used to construct a mutual lighter authentication protocol suitable for connected devices with tiny power networks since such an encryption schema does not demand large computations and calculations. In terms of calculation time and cypher text size, the shared authentication protocol is compared to other systems such as Elliptic Curve Cryptography (ECC), Algebraic Erase (AE), and NTRU. The investigators also claim that the model works better without a trusted third party to coordinate the setting up process across multiple IoT devices, however they haven't verified their design with immediate picture streaming owing to the high computational time and private key distribution. [26] proposes immediately encrypted confidential transfer among any two devices in an IoT network. They that applies their strategy to a smart home situation in which there is a key generation focused that induces private keys for all home IoT devices (sensors or the actuators) network of things based on the unique identity of each IoT device within the home IoT network, which increases the amount of time needed for computation to feed their approach. Following that, all of the IoT devices within the home collect data, some of which is sensitive data that must be delivered securely by encrypted with the private key. An the solution in [27] depends on the use integrated IoT multi-view security cameras to improve processing capacity, which may then be used for analysis and select critical frames in the streaming video and remove insignificant data that is redundant. Because keys were only required to be scrambled using the lightweight probability key frames encoding Algorithm, just a minimal amount of data needed to be transferred. The encryption method is based on the usage of a 2D chaotic map to create PRNG for image encoding, as well as an RBG photo encryption technique for key frame, while the hidden key is utilised to decode transmitted data in order to obtain the originating key frame.

3. Methodology

Authorities distribute and install a significant number security cameras for watching the streets and sites in towns and institutions. The cameras in question are constantly sending an ongoing supply of photos and movies to a server-side database. Several of these webcams are placed in highly sensitive locations such as diplomatic missions, military bases, and offices. As a result, movies and photos captured by such cameras must be sent in an indistinguishable or compressed form. To deal with this issue, a suggested model using a lightweight algorithm for encryption that meets the following objectives has been developed:

1) It must be quick enough for encryption and decoding live pictures and video.
2) Does not necessitate a large amount of assets (memory

space and CPU time).

3) Meets a high level safety for the transfer of data. This is done by:
   a. Changing the key used on a regular basis.
   b. Make use of robust and big key.

The main structure of the suggested system can be seen in Figure 1. The following are the key elements of this model:

1) *IoT Cameras*: a group of IoT webcams used to monitor various locations.
2) *Central Server*: a system of computers linked to edge servers that executes a protocol used to identify the keys that IoT sensors will use to encrypt video/images.
3) *Edge Server*: a computing device that distributes various keys to the linked IoT cams and receives encryption videos/images from these cameras.
4) *Key*: a secret key that allows IoT camera to encrypt the videos/images they capture. The central server uses the identical key to decode the receiving videos/images.
5) *Encryption algorithm*: a simple method used by IoT webcams to encrypt videos/images with a key retrieved from a nearby server, which is updated on a regular basis.
6) *Decryption algorithm*: a lightweight method employed by the central server to decrypt videos/images sent by IoT sensors using a preset key.

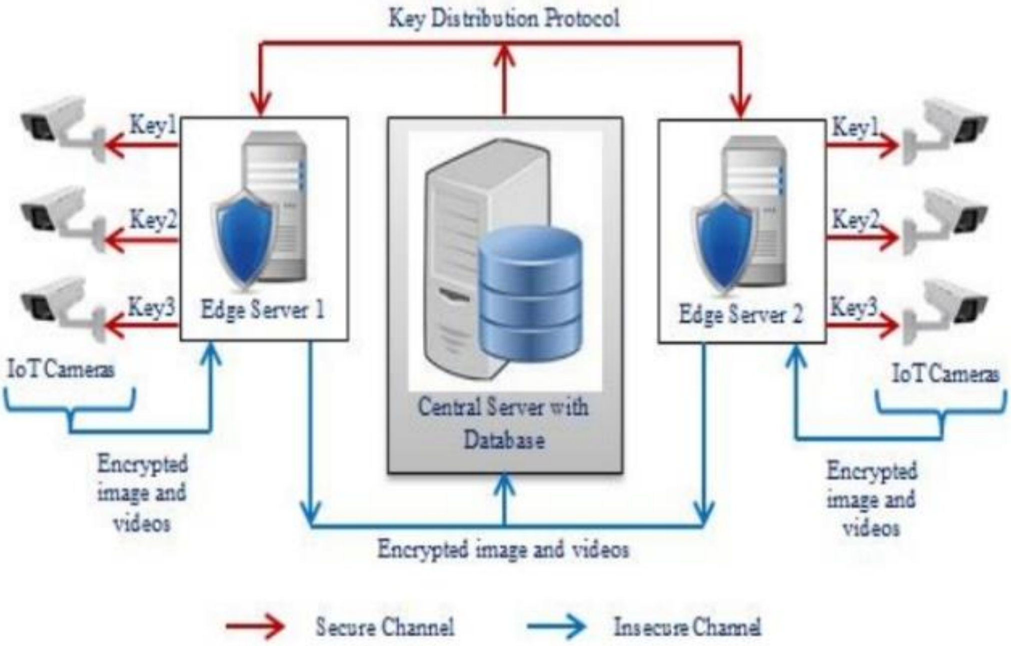

Key Distribution Protocol
Key1
Key2
Key3
Edge Server 1
Central Server with Database
Edge Server 2
Key1
Key2
Key3
IoT Cameras
IoT Cameras
Encrypted image and videos
Encrypted image and videos
Encrypted image and videos
Secure Channel
Insecure Channel

Figure 1. General framework of the proposed model.

The suggested model's deployment consists of a number of steps, which are outlined below:

Stage 1: Using encrypted connections, the central server transmits a set of data to each edge server. This table gives data that IoT cameras use as an authentication key to encrypt videos/images. The server creates the values in every row of the table's contents at random and applies them beginning with the time supplied in that row. The time interval across times in every page of the table for each edge server is determined by the amount of sensitivity of the locations discovered by IoT cameras. Table 1 is an example of such a table; each value in each row symbolizes a bite-sized piece of the secret key. Where The camera ID is a number used to identify each camera, Time is a plenty that represents the beginning time for key performance, XOR Value is a number used by the algorithm that secures data to perform XOR logical operation on video/image bytes, and ROTATE Value is a the amount used by the encryption algorithm to accomplish ROTATE logical operation on video/image bytes.

Table 1. An Example of the table used by edge server.

Key Portion Size			
Camera ID	**Time**	**XOR Value**	**ROTATE Value**
34900	12:35	17780	678943
34900	01:00	200	8765314
34900	01:45	9067	981183

Stage 2: The edge servers produces sections of the secret password to the established camera based on the time calculated in every row of the table.

Stage 3: Each IoT device encrypts the videos/images collected using sections of the key acquired form the edge server. The following procedures are included in the encryption algorithm version utilised in the proposed model:

A) *Substitution (XOR) operation*: The XOR operation is performed on each byte in the source data (which will begin with Index = 0 and repeating) using formulae (1), (2), and (3), where Current Time factor symbolises the global time beginning with the Initial Time and enhancing periodically, Value1 stands for the initial 2-byte value obtained by carrying out XOR logical operation between three 2-byte values, and Value2 represents 1-byte value obtained by carrying out XOR logical operation between three 2-byte values. Every bytes of Data in the resulting Value2 has a distinct value.

Value1 = (Camera ID, XOR Value, Present Time) (1)

Value2 = (Left 1⁄2 (Value1), Right 1⁄2 (Value1) (2)

New data [index] equals Old data [index] Value of XOR (3)

B) *The translation (ROTATE) action*: The ROTATE procedure is performed to each byte in the information that was provided (from Index = 0 to (232-1) and repeated). First, the value in the Requirement Value parameter is determined for the byte of data at Indexed using equation (4).

New data [index] equals Old data [index] XOR Value2 (4)

The equation (5) is then applied if the outcomes of the two halves of Condition Value (each half containing 2 bytes) disagree. Otherwise, no changes are made to the byte content in Data in Index.

Rotate Right (Data old [index], 4) OR Rotate Left (Data old [index], 4) = Data new [index] (5)

The change in the character value in the Data varies greatly from byte to byte since it is determined by the ROTATE Value and the Index.

Stage 4: The encryption bytes of the source information associated with the videos/images produced by Stage 3 are transmitted via the IoT video to the server on the edge and subsequently to the central server. After receiving the private information from the IoT camera, a centralised server performs the same two processes (substitution and transposition) as in the encrypted phase, but in reverse order, to decode the inbound encrypted data and retrieve the source data.

4. Testing, Evaluation & Discussion

Three primary goals have been defined for the recommended cryptography paradigm. In this part, we'll pretend if the source material were photos in order to put the suggested encryption technique to the test. To get started, the encryption technique employed must be light enough to run on an Internet of Things camera CPU. This involves using a minimum of resources as possible (processor time and memory). Second, for the purpose to ensure a high level of safety for the data conveyed, the key used in the procedure of encryption must be updated on a regular basis. Third, the key size (in bits) utilised in the method for encryption must be as high as practicable to make it difficult for attackers to break. Fourth, the encrypting method has to create the highest total of data distortion. This impact could be checked mathematically by computing the encrypted image's Peak Signal to Noise Ratio (PSNR) and analytically by comparing the histograms of both the original and decrypted pictures. The suggested cryptography model was developed at Google's Colab using the programming language Python and a computer machine with an Intel (Core-i3) 2.40 GHz CPU and 4.0 GB RAM.

The aims of the recommended cryptographic model are looked at and evaluated in this section. Each examination gets evaluated by drawing comparisons to known algorithms. The discussion of the findings aided in drawing certain inferences.

4.1. Speed of the Encryption Algorithm

Most encryption algorithms attempt to scramble data using complicated theoretical and logical formulae. It lengthens the actual duration of the algorithm while additionally raising the difficulty for intruders. Likewise, using equations requires greater time to execute than using logical procedures.

To be sure, the durability of any encryption system is established mostly by the key used rather than the technique. As a result, all of the steps included in the proposed algorithm for encryption are logical (XOR and ROTATE operations), which reduces the time necessary to finish the encryption process.

In regards to memories, the XOR and ROTATE processes are carried out on each bit of data on their own, which implies that the CPU does not require a large amount of memory to conduct these kinds of operations.

Many graphic photos had been encrypted using the two-step proposed encryption method and various well-known methods of encryption such as DES (Data Encryption Standard) to assess the speed of the suggested method. Figure 2 depicts some of the pictures employed in the studies, while Table 2 details the encryption times for the pictures in question.

ATM

Bank

Figure 2. Illustrations from the tests.

Table 2. The encryption time of the proposed, DES algorithms.

Image	Encryption time (sec)	
	Proposed Algorithm	**DES**
Bank	210	367
Palace	134	271

4.2. The Key Used in the Encryption Algorithm

Regarding the size of the encrypting method's memory, the XOR and ROTATE operations are done on each byte of data on their own; this indicates that the proc Because of the security of the videos/images provided by IoT cameras, the key employed by the cameras to secure the information they send must be changed on occasion. This is actually done in the suggested strategy, in which the edge server obtains a table containing independently generated keys by the central server on a regular basis. The edge server transmits each key to the appropriate table based on its creation time. Previously said, the duration of change of the key applied to each IoT camera is determined by the degree of sensitivity of the locations observed by that camera, and it lowers as the sensitiveness of the location grows.

4.3. The Size of the Key Used in the Encryption Algorithm

To achieve an exceptionally high degree of safety for transferred encrypted data, the key chosen must be as big as feasible. The quantity of bits in a key determines its size in cryptography algorithms. Table 1 displays the size (in bytes) of each component of the key utilised in the recommended encryption technique. The total quantity of the key used in the suggested technique in bits (where 1 byte = 8 bits) is 80 bits, which is computed using equation (6).

$$\text{Total Size of Key} = ((\text{Camera ID}) + (\text{Time}) + (\text{XOR Value}) + (\text{ROTATE Value})) \tag{6}$$

Table 3 relates the key sizes (in bits) employed in the suggested technique to those used in other established encryption techniques. The illustration clearly shows that the recommended strategy employs a relatively big key size, which makes the key difficult for attackers to crack.

Table 3. Compares the key sizes used in the suggested technique to those used in other known encrypted schemes.

Encryption Algorithm	Key size in bits
Proposed Algorithm	32
DES	16

4.4. The Proportion of Distortion in the Encrypted Data

Table 2 illustrates the chosen PSNR values of the encrypted pictures for the matching source images in Figure 2. PSNR is computed using solution and s. As indicated in Table 4, the PSNR values obtained in trials suggest that the proposed method produced a high fraction of deformation in the data that was encrypted, and it is reasonably close to the comparable PSNR of existing encryption techniques.

$$\text{NMAE}= \sum_{k=0}^{1\ Size-1} \frac{|I(k)-E(k)|}{I(size)} X\ 100 \tag{7}$$

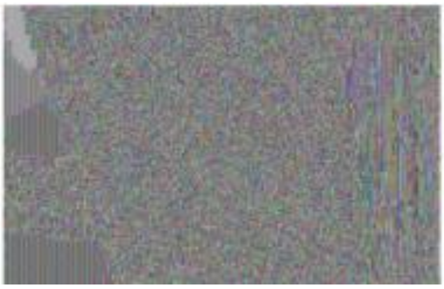
$$\text{PSNR}= 10.log10(\frac{maxi2}{NMAE}) \tag{8}$$

Max where: And db is the largest feasible pixel number for the picture I. A decibel is a unit of measurement.

Table 4. The encoded pictures' PSNR results.

Image	PSNR	
	Proposed algorithm	**DES**
Bank	8.00	8.01
ATM	7.13	7.15

By contrasting original and encryption photos, the blurred impact in the pic that appears while executing the recommended method may be directly checked. Figure 3 depicts the coded versions of the source photos seen in Figure 2.



Bank

ATM

Figure 3. *Displays the encoded pictures of the origin images seen in Figure 2.*

Figure 4 also shows histograms of bytes values for the original and encrypted picture (data). The encrypted picture histogram shows the suggested approach was successful in causing an important alteration in the probability distribution of the byte in the encrypted picture.

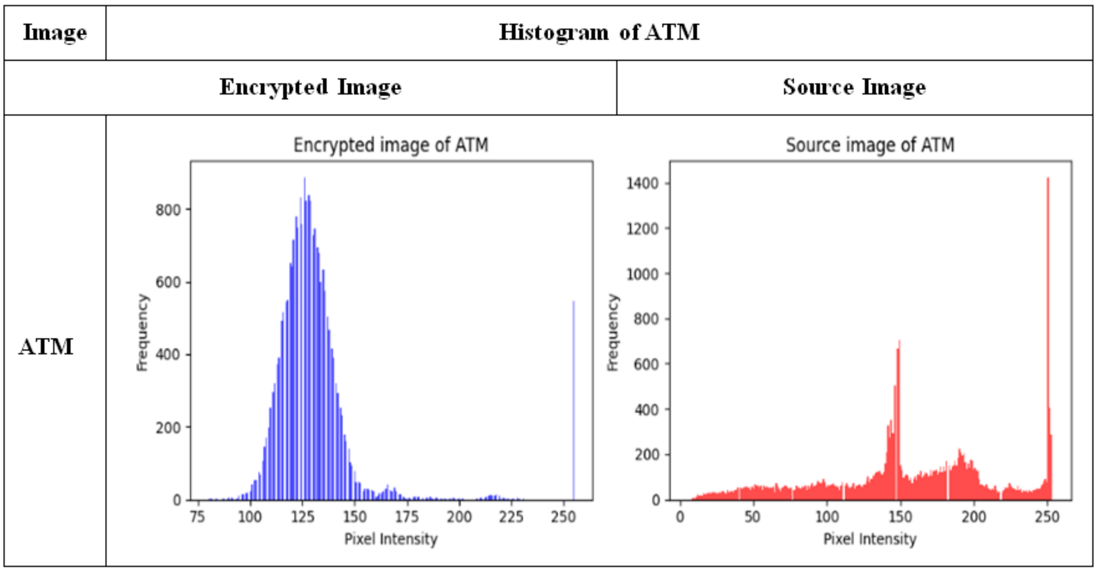


Figure 4. *Shows the histograms of the encoded and source photos used in the tests.*

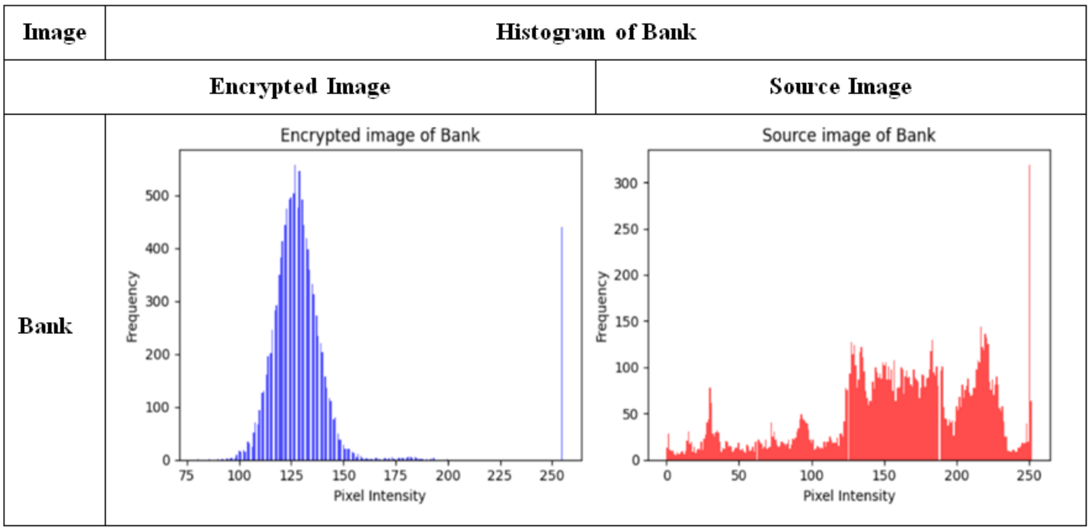


Figure 5. *Shows the histograms of the encoded and source photos used in the tests.*

5. Conclusion

When those cameras are put in highly valuable regions such as diplomatic missions' army institutions, and positions, a novel encrypted scheme was suggested for secure data transfer for IoT surveillance equipment. Furthermore, the suggested encryption model adheres to IoT device resource constraints in the areas of time spent processing, memory space, and electrical consumption. Experimental the results show that the model we propose requires fewer resources, such as time as well as disc space than previous ways while maintaining a high degree of information safety via a continual modification of the encryption algorithm used the encrypting conveyed IoT data. Furthermore, the key size used for encrypting received data in the suggested technique is high enough that attackers will find it difficult to crack.

Abbreviations

IoT	Internet of Things
CCTV	Closed-Circuit Television
RFID	Radio-Frequency Identification
MQTT	Message Queuing Telemetry Transport
AES	Advanced Encryption Standard
GPU	Graphics Processing Unit
DES	Data Encryption Standard
ECC	Elliptic Curve Cryptography
AE	Advanced Encryption
PSNR	Peak Signal-to-Noise Ratio
HEVC	High Efficiency Video Coding
PRNG	Pseudo-Random Number Generator

Conflicts of Interest

The authors declare no conflicts of interest.

References

[1] Mehmood, M. Sajjad, W. Ejaz, and S. W. Baik, Saliency-directed prioritization of visual data in wireless surveillance networks, Information Fusion, vol. 24, pp. 16–30, 2015. https://doi.org/10.1016/j.inffus.2014.07.002

[2] T. Yu, V. Sekar, S. Seshan, Y. Agarwal, and C. Xu, Handling a trillion (unfixable) flaws on a billion devices: Rethinking network security for the internet-of-things, in Proceedings of the 14th ACM Workshop on Hot Topics in Networks, 2015, pp. 1–7.

[3] M.-H. Maras, Internet of Things: security and privacy implications, International Data Privacy Law, vol. 5, no. 2, p. 99, 2015. https://doi.org/10.1093/idpl/ipv004

[4] F. Al-Turjman, H. Zahmatkesh, and R. Shahroze, An overview of security and privacy in smart cities' IoT communications, Transactions on Emerging Telecommunications Technologies, no. June, pp. 1–19, 2019, https://doi.org/10.1002/ett.3677

[5] K. Zhang, J. Ni, K. Yang, X. Liang, J. Ren, and X. S. Shen, Security and privacy in smart city applications: Challenges and solutions, IEEE Communications Magazine, vol. 55, no. 1, pp. 122–129, 2017. https://doi.org/10.1109/MCOM.2017.1600267CM

[6] Y. He, F. R. Yu, N. Zhao, V. C. M. Leung, and H. Yin, Software-defined networks with mobile edge computing and caching for smart cities: A big data deep reinforcement learning approach, IEEE Communications Magazine vol.55, no. 12, pp. 31-37, 2017 https://doi.org/10.1109/MCOM.2017.1700246

[7] Z. Maamar, T. Baker, M. Sellami, M. Asim, E. Uglianin, and N. Faci, Cloud Vs edge: who serves the Internet of Things better?, Internet Technology Letters, vol. 1, no. 5, p. e66, 2018.

[8] R. Mahmud, R. Kotagiri, and R. Buyya, Fog computing: A taxonomy, survey and future directions, in Internet of everything, Supringer, 2018, pp. 103-130.

[9] B. Al-Shargabi, S. Al-Jawarneh, and S. M. A. Hayajneh, A cloudlet based security and trust model for e-government web services, Journal of Theoretical and Applied Information Technology, vol. 98, no. 1, pp. 27–37, 2020.

[10] N. Li, D. Liu, and S. Nepal, Lightweight mutual authentication for IoT and its applications, IEEE Transactions on Sustainable Computing, vol. 2, no. 4, pp. 359–370, 2017. https://doi.org/10.1109/TSUSC.2017.2716953

[11] B. Al-Shargabi and O. Sabri, A study of Adopting Cloud Computing from Enterprise Perspective using Delone and Mclean IS Success Model, International Journal of Computer Science and Information Security, vol. 14, p. 32, 2016.

[12] D. Chialva and A. Dooms, Conditionals in homomorphic encryption and machine learning applications, arXiv preprint arXiv: 1810.12380, 2018.

[13] H. Abualese, T. Al-Rousan, and B. Al-Shargabi, A New Trust Framework for E-Government in Cloud of Things, International Journal of Electronics and Telecommunications, vol. 65, no. 3, pp. 397–405, 2019, https://doi.org/10.24425/ijet.2019.129791

[14] [S. R. Masadeh, H. A. Al-Sewadi, and M. A. F. Al-Husainy, Embedded key cryptosystem for cloud computing applications, in Proceedings of the 2nd International Conference on Future Networks and Distributed Systems, 2018, pp. 1–7. https://doi.org/10.1145/3231053.3231078

[15] X. Zhang, S. H. Seo, and C. Wang, A Lightweight Encryption Method for Privacy Protection in Surveillance Videos, IEEE Access, vol. 6, pp. 18074–18087, 2018, https://doi.org/10.1109/ACCESS.2018.2820724

[16] C. Wampler, S. Uluagac, and R. Beyah, Information leakage in encrypted ip video traffic, in 2015 IEEE Global Communications Conference (GLOBECOM), 2015, pp. 1–7.

[17] N. Mekki, M. Hamdi, T. Aguili, and T. H. Kim, A real-time chaotic encryption for multimedia data and application to secure surveillance framework for IoT system, Proceedings - 2018 International Conference on Advanced Communication Technologies and Networking, CommNet 2018, pp. 1–10, 2018, https://doi.org/10.1109/COMMNET.2018.8360271

[18] A. Adeel, J. Ahmad, and A. Hussain, Real-Time Lightweight Chaotic Encryption for 5G IoT Enabled Lip-Reading Driven Secure Hearing-Aid, pp. 1–14, 2018.

[19] S. Aljawarneh, M. B. Yassein, and W. A. Talafha, A resource-efficient encryption algorithm for multimedia big data, Multimedia Tools and Applications, vol. 76, no. 21, pp. 22703–22724, 2017, https://doi.org/10.1007/s11042-016-4333-y

[20] V. A. Memos, K. E. Psannis, Y. Ishibashi, B.-G. Kim, and B. B. Gupta, An efficient algorithm for media-based surveillance system (EAMSuS) in IoT smart city framework, Future Generation Computer Systems, vol. 83, pp. 619–628, 2018.

[21] R. A. Shaikh, H. Jameel, B. J. d'Auriol, H. Lee, S. Lee, and Y.-J. Song, Achieving network level privacy in wireless sensor networks, Sensors, vol. 10, no. 3, pp. 1447–1472, 2010.

[22] D. Christin, A. Reinhardt, P. S. Mogre, and R. Steinmetz, Wireless sensor networks and the internet of things: selected challenges, Proceedings of the 8th GI/ITG KuVS Fachgespr äch Drahtlose sensornetze, pp. 31–34, 2009.

[23] C. Wang, J. Shen, Q. Liu, Y. Ren, and T. Li, A Novel Security Scheme Based on Instant Encrypted Transmission for Internet of Things, Security and Communication Networks, vol. 2018, 2018, https://doi.org/10.1155/2018/3680851

[24] K. Muhammad, R. Hamza, J. Ahmad, J. Lloret, H. Wang, and S. W. Baik, Secure surveillance framework for Mohammed Abbas Fadhil Al-Husainy et al., International Journal of Advanced Trends in Computer Science and Engineering, 9 (2), March - April 2020, 1840 – 1847 1847 IoT systems using probabilistic image encryption, IEEE Transactions on Industrial Informatics, vol. 14, no. 8, pp. 3679–3689, 2018, https://doi.org/10.1109/TII.2018.2791944

[25] S. Ullah, L. Marcenaro, and B. Rinner, Secure smart cameras by aggregate-signcryption with decryption fairness for multi-receiver IoT applications, Sensors (Switzerland), vol. 19, no. 2, 2019, https://doi.org/10.3390/s19020327

[26] L. Pang, M. Kou, M. Wei, and H. Li, Anonymous Certificateless Multi-Receiver Signcryption Scheme Without Secure Channel, IEEE Access, vol. 7, pp. 84091–84106, 2019, https://doi.org/10.1109/ACCESS.2019.2924654

[27] M. A. F. Al-Husainy and H. A. A. Al-Sewadi, Implementing Binary Search Tree Concept for Image Cryptography, International Journal of Advanced Science and Technology, Vol. 130, pp. 21- 32, 2019. https://doi.org/10.33832/ijast.2019.130.0