Received: December 12, 2022. Revised: January 23, 2023. 

International Journal of
Intelligent Engineering & Systems

http://www.inass.org/

# Privacy Security System for Video Data Transmission in Edge-Fog-cloud Environment

**Ekhlas K. Gbashi[1] Abeer Tariq Maolood[1] Yaseen Naser Jurn[2]***

[1]*University of technology, Iraq*
[2]*University of information technology and communications, Iraq*
* Corresponding author's Email: yaseen.naser@uoitc.edu.iq

**Abstract:** Fog computing is an efficient paradigm to diminish latency and congestion of networks, in which the applications and data are no longer deployed in the cloud alone. Alternatively, the cloud server is improved with devices working near the edge layer and end users such as mobile applications and sensors respectively in internet of things (IoT) scenarios. Video surveillance system is a critical issue needs considerable computing and network instruments to provide the substantial quality of data. Multimedia communication includes videos transferring between fog and cloud server via secure channel is considered a critical problem needs to resolve. This paper proposes a light-weight cryptographic scheme to provide the secrecy and privacy for the transferred video data within edge-fog-cloud platform. Specifically, the framework of the proposed cryptographic scheme involves three main phases; secret key (SK) generation algorithm and distribution processes, pre-processing of video frames based on frame region of interest extraction FROI approach, and video data encryption/decryption phase using 2D chaotic map. The major parameters that effect on video encryption performance within edge-fog-cloud infrastructure are latency, accuracy and practicability. The secret key generation process is implemented into central fog node (CFN), while keys distribution and management processes are implemented into cloud computing layer for higher security distribution procedure. Common evaluation benchmarks were utilized in the experimental results to analyse and evaluate the proposed cryptographic scheme. The performance evaluation of the proposed cryptographic scheme is carried out based on some of metrics which are memory consumption rate, encryption time, rate decryption time, key sensitive analysis and computation complexity via using urban surveillance video dataset (USVD). The results of these metrics prove that the proposed scheme has been very suitable for securing transmit video data for edge-fog-cloud structure against intruders. Scientific comparisons against stat of art methods are conducted in our experiments to highlight the performance evaluation of the proposed scheme. Finally, the finding results based on scientific comparisons show that the proposed scheme is more appropriate for transfer encryption video frames from fog-layer to cloud-computing layer.

**Keywords:** Video security, Edge-fog-cloud structure, Surveillance system, Network security, IoT network security.

## 1. Introduction

The cloud computing services has been extended to the fog computing for users and devices at the network edges. The fog computing is present enhancement the services quality to the end user for complimenting work of IoT cloud. Over the present scientific revolution, the combination of cloud and fog computing has protruded out as the pioneer platform for storing and processing of big data. This technique is utilized for many applications and services like education, healthcare, manufacturing, surveillance systems and others. Newly, at utilizing edge-fog-cloud structure, our different environments (life, study, work, etc.) will changes to smart and friendly for usage. Where, the large number of heterogeneous devices such as smartphones, actuators, monitoring sensors and so on will be smoothly integrated [1-4]. The exchanges image and video data between these different applications is

very important issue. Therefore, the process of exchanging video data for different applications and different aims cannot be applied with unsecure channel. Hence, the processes of securing the exchange data are very necessary to keeping the specialized information. The scheme presented for this purpose must be have important and scientific features such as; high security level of information, high complexity of securing algorithm, low complexity for implementing encryption and decryption scheme, and minimum time of processing.

In this paper, a lightweight cryptographic scheme is proposed for securing the exchanges video data between fog and cloud layer. The proposed cryptographic scheme consists of three main phases; secret keys generation and distribution, frame region of interest extraction FROI approach and 2D-chaotic map-based video data encryption/decryption processes. The performance evaluation and scientific comparisons are carried out based on general dataset called urban surveillance video dataset (USVD).

The rest of this paper is organized as follows: Related work is detailed in section 2, the problem definition is presented in section 3, objectives and contributions are exhibits in section 4, in section 5 methodology is discussed, while framework is presented in section 6, the performance evaluation with their results is presented in section 7, finally the conclusion is exhibits in section 8.

## 2. Related work

Fog-computing technique was adopted in variant applications such as sharing bridge between cloud computing service and edge sensors. This structure causes to make different applications more efficient and up to date for future works. However, fog computing technology faces many challenges in meeting the security and privacy requirements of the transmitted/exchanged data. These challenges occur due to the limitations of fog computing resources. Consequently, the security of video data in fog computing is one of main challenges for utilizing fog computing into different applications. This section presents different algorithms which are proposed by several researchers for solving security issues of video data within fog computing environment.

The public and private video surveillance systems have been optimized based on utilizing fog computing in order to increase privacy and security level. The exchanging video data is implemented between end sensor node (camera) and cloud computing via fog layer. Recently, there is an urgent demand to secure these video data to protect it against different types of espionage and theft. For this purpose, a lot of research presents different schemes to secure video data. The mixing structure of edge devices/fog/cloud computing within big data and internet of think (IoT) are typical structure for major computing for different applications. The problem of secure media data was addressed widely [5-13].

The framework of research [14], was presented to secure video data by addressing some of challenges such as; data modifications, data leakage and confidentiality breach of the multimedia data into cloud-fog-IoT network. This framework was designed to implement different functions such as; data store, search and share the secure multimedia data in the cloud-fog IoT network. The main encryption methods used are; AES (advanced encryption standard) for data encryption, (MAC) message authentication code for integrity of data safe, (SSL) for safety of data exchange, data pointers and hashing for purpose of easy search of data in both fog and cloud computing layers. The drawbacks of their work can be summarized in few points such as; there is no results and scientific comparisons presented in this work. Also, this work was depended on high complexity of implementation due to utilized AES algorithm for encryption video data. In [15], an algorithm was presented for secure media-packet surveillance system of smart cities based on applied efficient video encoding. This algorithm was aimed to reduce the required memory of sensor nodes within environment of the network. Their work focuses on reduces the memory size but not taken into considerations the time of process for securing media packet. In addition to that the media packet was not classified to video data or image data in the presented scheme and experimental results.

The issues of privacy and security of structures edge, fog and cloud computing are discussed and listed the proposed solutions in [16]. This research listed the security and privacy problems of each structure individually with the solution list of each problem. Also, the privacy and security of fog-computing for IoT applications have been discussed and presented in [17]. The inclusive understanding of security and privacy issues of fog computing have been presented. This research presents scientific survey to review the fog computing literature about the privacy and security issues.

In [18], the data communication between cloud and user was secured based on provide improved practical cloud technique. The aim of this technique

is to secure video data before storing into cloud. The technique of this approach make the privacy video data is vulnerable to hacking by other participants. This point is main drawback of like technique. Therefore, the securing of video data into fog-layer before sending it to the cloud-layer is very important and efficient approach to protect privacy video data.

Video protection has been greatly sponsored by suggesting many encryption schemes [19-26]. In [19], the encryption algorithm called random data encryption algorithm (RDEA) based on permutation was proposed and investigated. In this algorithm, the specific part of frame was selected randomly and encrypted this part with the second part of the same frame based on permutation scheme. This algorithm was suitable for IoT due to the encryption ratio was 93.75% less than AES algorithm. On contrast, the drawback of this scheme is the attackers can recover original frame partly based on utilize the file structures for instance header marker or end-of-file (EOF) marker due to using the encryption video frame partially.

In the research work of [20], the permutation based on faro-shuffle was presented as video data encryption algorithm. This algorithm was presented to resist the file structure inference attack based on encrypts the video data stream before the compression process stage. On contrast, the drawback of their work, it was vulnerable onto face the known plaintext attacks due to it used the fixed list of permutation for all video frames. In addition, it was weak against the brute-force attacks because the complexity is very low due to using the faro-shuffle algorithm.

In research [21], the video encryption algorithm was presented based on changes the settings of video pixels of every frame and changes the frame contents simultaneously. The finding results show that, their algorithm has time computation lower than different algorithms, good security, robustness to analytical attacks, known-plaintext, and brute-force. On the other hand, the weak point of this algorithm is high complexity of its computational due to use three different algorithms for encryption/decryption process. The first algorithm used for I-frames shuffling, 3D rossler and 3D logistic map.

The Henon chaotic map based media privacy protection was applied by researches [22-25] in order to generate pseudo random sequence desired for encryption/decryption image/frame data. The number of encryption keys is based mainly on the original image size. However, Henon map provides low computational complexity, high security and good randomization. Therefore, it's used for video protection with different schemes.

Finally, the encryption scheme is proposed in this work to overcome the drawbacks and weak points described in previous works presented in this related work.

## 3. Problem definition

Recently, the abrupt evolution of IoT networks has led to exponential increasing of multimedia data usage such as images and videos. Therefore, the privacy securing of the transmitted videos to the cloud, which are collected by several surveillance cameras could be considered as a critical issue that needs to address and resolve for the purpose of storage into cloud platform in secure manner. Commonly, video surveillance system includes set of cameras located at end user (edges) to capture and transmit unsecure video sequence to the cloud. In this paper, the considered IoT network consists of edge-layer, fog-layer (fog-nodes) and cloud-layer. Consequently, the exchange video data between fog-layer and cloud-layer should be secured against intruders. As a result, a new cryptographic scheme of video data is proposed and investigated in this paper to encrypt the transmitted video data into fog-layer before sending it to the cloud-layer in term of edge-fog-cloud structure.

## 4. Objectives and contributions

The substantial aim of this paper is to propose cryptographic scheme within edge-fog-cloud structure to implement the privacy security of the transmitted video data from edge sensors passing through fog layer towards cloud platform storage space. The video data is video frames captured by a camera of surveillance system. The main contributions of this work can be summarized as follows:

1. Decreasing the execution time of video processing in fog domain and reduces the storage size required in the cloud.
2. An efficient lightweight cryptographic scheme of video data is proposed and validated, which is implemented in fog domain.
3. A key generation algorithm for cryptographic scheme is introduced to achieve the security of transmitted video data through IoT network.

This paper proposes a light-weight cryptographic scheme for securing the transmitted video sequence between fog and cloud, which included; secret key generation and distribution by

using chaotic map method; frame region of interest extraction FROI approach and applying 2D-chaotic map on video data to achieve video encryption/decryption processes.

## 5. Methodology

In order to ensure the privacy and security of the transmitted video data and overcome the latency problem, we have proposed a light weight encryption/decryption method of video data applicable for real time applications. The encryption scheme uses a lightweight 2D chaotic map to provide high security level for transferring the private video data. In this context, frame region of interest extraction (FROI) scheme is implemented for each frame as pre-processing phase to decrease the computation time. The proposed encryption/decryption processes and FROI scheme are implemented within fog-layer for securing video data collected from edge cameras, saving processing time and saving the required storage capacity into cloud-layer. The pre-processing phase consists of two operation modes; first mode is computing the frame differences between current frame and references frame. Second, frame region of interest extraction mode. Accordingly, we have focused on the interested information of the current video and ignored the redundant frames along video sequence.

## 6. Framework

The framework of this paper is implemented based on special steps illustrated as follows:

### *A. Structure of suggested network*

In this work, the suggested IoT network includes the following layers; edge sensors (video cameras), fog-layer (include video analysis center) consists of multiple fog nodes, keys generation center and cloud-layer. It's worth noting, we have selected specific fog node as center node of fog-layer which named central fog node (CFN).

In this context, the keys generation and the synchronization operations between fogs nodes are controlled by the CFN and cloud-layer. The secret keys are generated in CFN then upload to the cloud-layer for the purpose of keys distribution management. The secret keys should be transmitted to the cloud-layer in secure manner to prevent the attackers. Fig. 1 illustrates the structure of suggested network.

### *B. Proposed cryptographic scheme (encryption-scenario)*

The framework of the proposed cryptographic scheme (encryption and decryption) process is

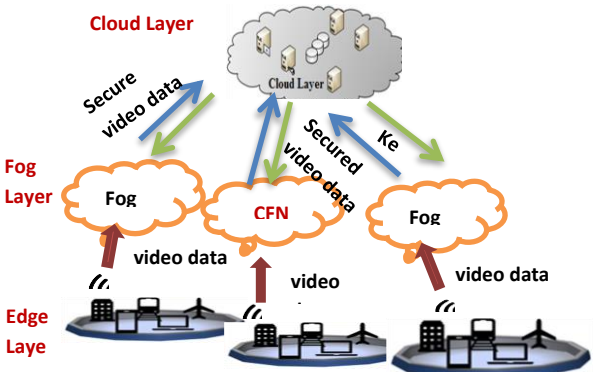



Figure. 1 structure of suggested network

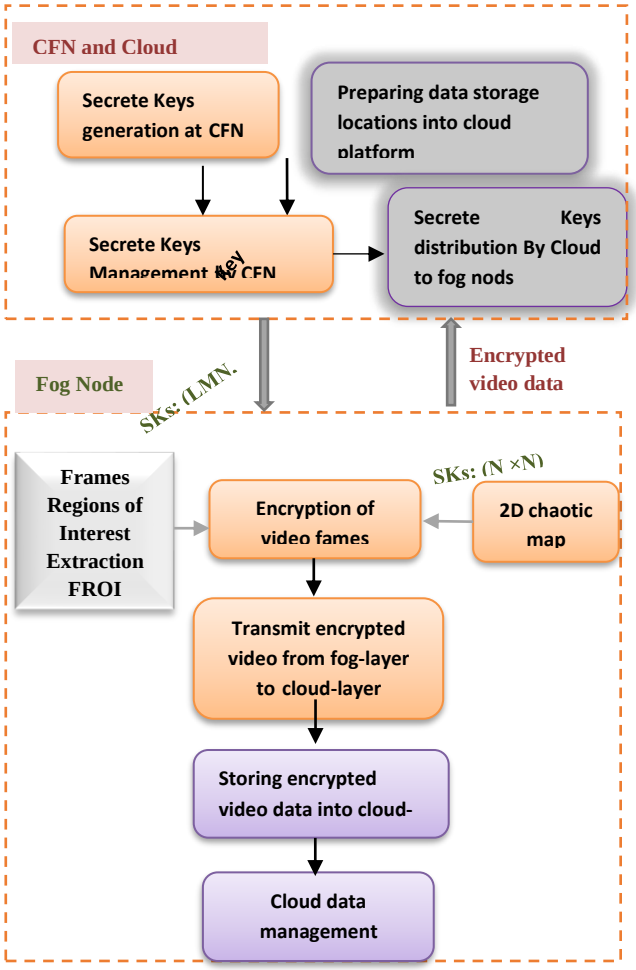



Figure. 2 Schematic of the proposed cryptographic scheme-encryption scenario

implemented in fog-layer to secure the exchanged video data between fog and cloud layers. The proposed cryptographic scheme involves multilevel; first level corresponds to keys generation process implemented into CFN. Second level represents a pre-processing of video frames based on extracting the most informative regions (action frames) from original video sequence using frame region of

interest extraction approach (FROI) to detect the changes along video sequence. Then, this process led to reduce the computation time. In third level, applying the 2D lightweight chaotic map to encrypt (or decrypt) interested video frame based on generation an array of chaotic keys to ensure more secure video data. The schematic of the proposed cryptographic scheme-encryption scenario is illustrated in Fig. 2.

### *C. Keys generation algorithm*

This subsection explains the workflow of first level in the proposed cryptography scheme, in which represents by secrete keys generation algorithm. These keys are required for implementing the proposed encryption/decryption scenarios. In order to generate the secrete keys SKs, the initial values of parameter α within the range of [1.07, 1.4] should be setting first, in which the variation of α parameter leads to create a variant chaotic map. Hence, this process causes to encrypt the video frames data with different chaotic maps based on same encryption scheme. For encryption and decryption scheme the secret key is selected based on synchronization process into whole network. Where, the secret keys SKs are adopted in both encryption and decryption schemes. The keys generation algorithm is implemented in the CFN to make the procedure of generation the secret keys is high secure and increases the privacy of SKs. Subsequently, the generated SKs are uploaded to the cloud-layer for the purpose of distribution SKs in the network. The main properties of this algorithm are lightweight, fast process with high randomization. The following steps represent the workflow of secret keys generation algorithm.

Step 1: Initialize No. of codes *Ncode* (user defined).
Step 2: Repeat until end of *Ncode*
Step 3: Initialize the input vector *A* randomly within range [1.07, 1.4], for example *A*= [1.07, 1.08, 1.09, 1.1, 1.2, 1.3, 1.38, 1.4], which included the sequence of α parameter with different values to exploit later for chaos map-based keys generation. *A* vector could be setting with different initializations based on user demand, with same vector length - 8 digits.
Step 4: labeling each element in vector *A* according to its index in vector *A* with IDX value.
Step 5: Implementing a random scrambling of vector *A* elements based on special condition to provide the randomize ordering of vector *A* elements.
Step 6: set the code number (list minimum number) LMN to each vector *A* indexes IDXs as binary value-8 digits to preserve into a table data structure named TCODE.

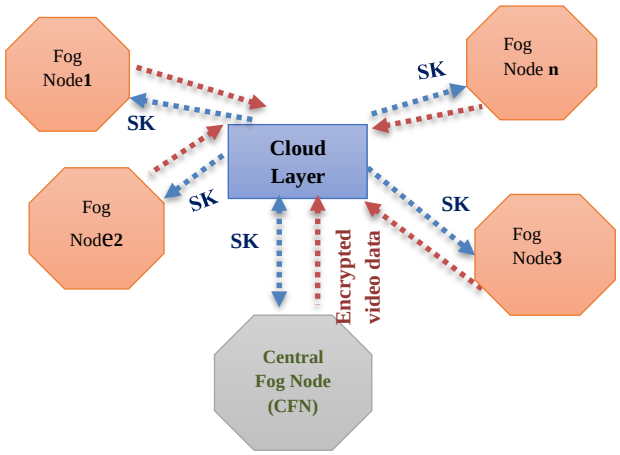



Figure. 3 Distribution process of secret keys SKs

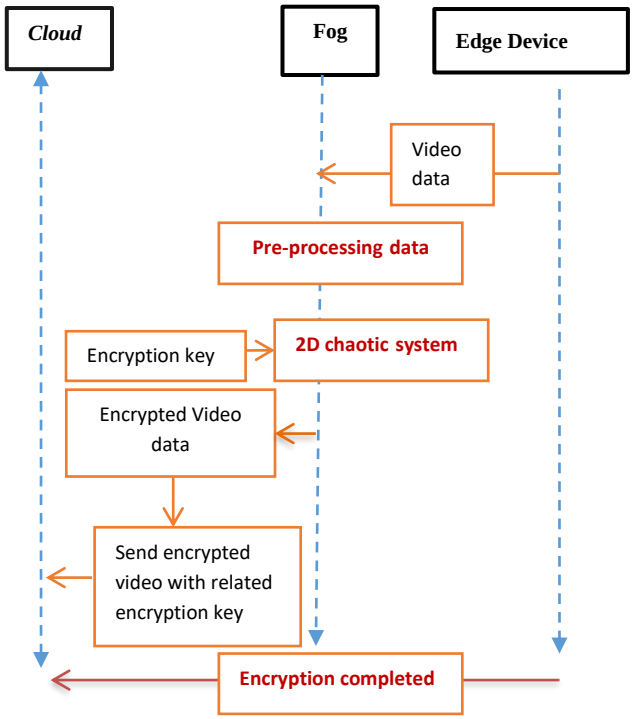



Figure. 4 Encryption cycle of video data

Step 7: Storing vector *A* elements with their indexes IDXs and binary codes LMNs into TCODE table.
Step 8: Sending TCODE table to cloud layer .
Step 9: End.

### *D. Keys distribution management*

The process of keys distribution management is applied by cloud-layer in our framework to distribute the SKs to all fog-nodes located in same fog-layer. Schematic of key distribution management strategy is illustrated in Fig. 3. Where, the generation of secret keys is implemented into (CFN). Subsequence, the generated SKs are sending to cloud-layer before distribution. Finally, the SKs distribution process is achieved by cloud-layer to ensure the high efficiently protection of secret keys distribution to the fog-layer.

### E. Proposed encryption-scheme scenario

In order to encrypt the interested video frames at fog nodes, we have used the SKs which are generated at CFN-node. Since the SKs are uploaded to the cloud-layer for preserving it and distribution to all fog nodes authorized by cloud-layer.

The encryption scheme is a second level of the proposed cryptographic scheme which is performed by implementing a pre-processing (FROI) to reduce the size of processed video data by extract the most informative frames and decrease the encryption processing time. The third level of proposed scheme is encryption process which implemented by applying using light-weight 2D-chaotic map to produce (N×M) matrix chaos keys. These keys are used for encryption each frame with (N×M) dimensions (where N = width, high=M of matrix chaos keys) before uploading the encrypted video to cloud-layer. The encryption process is carried out by X-ORing the pre-processed video frames by their related (N×M) chaos keys as illustrated in Fig. 4.

### F. Proposed decryption-scheme- scenario

The workflow of decryption scenario is presented in this section. The SKs of encryption/decryption tasks are generated at CFN and are sending to the cloud-layer for distribution these keys to all fog-nods. The decryption process algorithm is illustrated in Fig. 5. The decryption workflow starts when end user sending (decryption request) to the cloud-layer through fog-layer to download video from cloud-layer. The received encrypted video from cloud-layer at the fog-node is associated with their related SKs. The light-weight chaotic map is utilized to decryption the encrypted video for retrieve the original video based on X-ORing logical operation which is performed between encrypted video frame and chaotic map.

### G. Frame region of interest extraction (FROI) algorithm

The main idea of FROI algorithm is simplest by extracting the interested regions in the current frame compared with reference frame *RF*. To this end, we have implemented the FROI algorithm to minimize the size of processed video data based on extracting the differences between sequence frames and references frame by computing the frames differences. As a result, the processing time of the whole video sequence will be decreased. The reference frame is selected and updated periodically from sequences video frames based on predefined interval of video frames named *Rstep*.

The first frame *F1* of the input video is selected as initial reference frame *RF*, then it is updated according to *Rstep* interval as illustrated in Eq. (1):

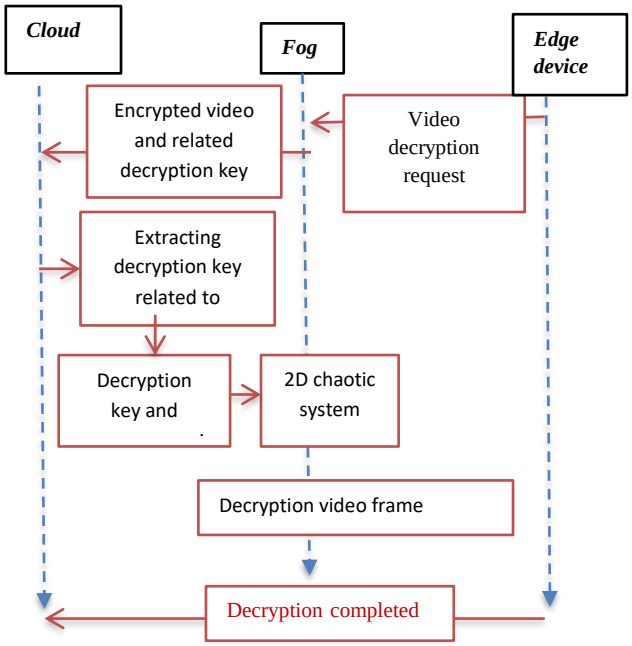



Figure. 5 Decryption cycle of video data

$$RF = I \ mod \ (Rstep) \tag{1}$$

Where *I* is represents the current frame indexing. The main steps of FROI-algorithm are clarified in Fig. 6.

As shown in Fig. 6, the instruction: (frame subtraction) *FSB* (*FI*, *RF*) referred to the subtraction of current frame *FI* from the reference frame *RF*, in which stored in the current difference frame $diff_i$. The original video is denoted by *V*, while $\hat{V}$ corresponds to the updated video which consists of set of reference frames *RFs* as well as set of interested shots of video *V*.

Each video frame resultant from FROI algorithm contents (only the interested frames) will be passed to the third level of the proposed cryptographic method-encryption process.

The main contributions of FROI algorithm can be summarized as follows:

1. Make the video data with minimum size.
2. The complexity and processing time are reduced in both encryption and decryption sides.
3. The redundancy of video frames is decreased through depending on step size *Rstep* for reference frame denoting.

Finally, FROI algorithm is implemented at both sides of cryptographic method (encryption and decryption).

### *H. 2D-Chaotic map-based lightweight encryption*

The lightweight chaotic map [22] is suggested to use in our framework to encrypt the stream video

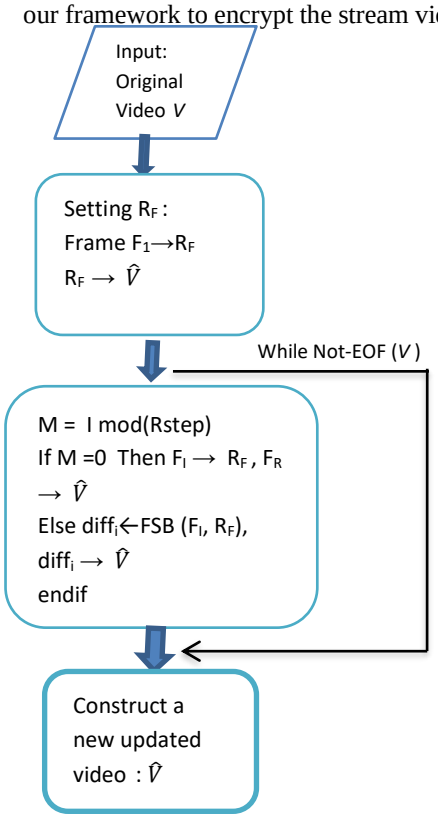



Figure. 6 Frame region of interest extraction (FROI-algorithm) workflow

frames into fog-node before sending it to the cloud-layer. This method is utilized to safe the streaming video data against unauthorized accessibility. We have adopted the lightweight chaotic map to generate ($N$×$M$) encryption keys to implement the encryption process with high level security performance, low processing time to increase the resistivity of the encrypted video against different types of attacks.

The Henon chaos map is utilized in this work as a lightweight encryption method as presented in [22]. Also, it is a common type of chaotic encryption methods used to encrypt different multimedia files such as video, text and voice, due to its high security level performance [23]. The lightweight chaotic map is described in Eqs. (2) and (3):

$$X_{n+1} = 1 - \alpha {X_n}^2 + Y_n \quad (2)$$

$$Y_{n+1} = \beta X_n \quad (3)$$

Where, the initial parameters are α =1.4, β = 0.3. The $Xn$ and $Yn$ are considered the current pixel positions, while the next pixel position is $Xn+1$ and $Yn+1$. The values of both $Xo$ and $Yo$ are the initial values that will get the next pixel positions $Xn+1$ and $Yn+1$, at initial conditions [23-25].

In this work, the initial values of α is (α ∈ [1.07, 1.4]) are taken from the first level of our framework (SKs generation algorithm) and β = 0.3 based on different references [22-25], while the $Xo$ and $Yo$ are setting to $Xo$ = 0.5 and $Yo$ = 0.5 as initial values. The two-dimension chaotic map $Xn$, $Yn$ where (n = 1, 2, . . ., $N$) are the generated keys method adopted in this work. Hence, the ($N$×$M$) resultant lightweight chaos map keys are used finally to encrypt video frames after applying the FROI-algorithm. The output encrypted video frames are obtained by XORing the input original video frames with (N×M) chaotic map as illustrated in Eq. (4).

$$Encryption - video\ frame = original\ video frame\ XOR\ (N \times M) chaos\ map \quad (4)$$

## 7. Performance evaluation

In this section, the performance of the proposed encryption scheme will be investigated and evaluated based on standard evaluation metrics. The performance evaluation has been performed using public surveillance video dataset (USVD) [26]. The proposed method is implemented using MATLAB R2018 programming environment with laptop computer of core i7, 2.90 GHz processor, and 16 GB RAM. For the performance evaluation we have using standard metrics such as; security evaluation, Key space analysis, encryption speed, memory efficiency and key sensitive analysis.

### A. Dataset description

In our experiments, we have used public video dataset called urban surveillance video dataset (USVD) which is largest and most comprehensive dataset [26]. For this purpose, we have selected specific video files to implement scientific comparisons between the proposed scheme with other related works, to prove that the proposed cryptographic scheme is more suitable for securing the translated video between fog-layer and cloud-layer.

### B. Security evaluation

The security evaluation metric is adopted for evaluation the performance of the proposed cryptographic scheme. The comparison of color composition for both proposed scheme and related work in literature sultana algorithm [20] is implemented for performance evaluation. This comparison is illustrated in Fig. 7.

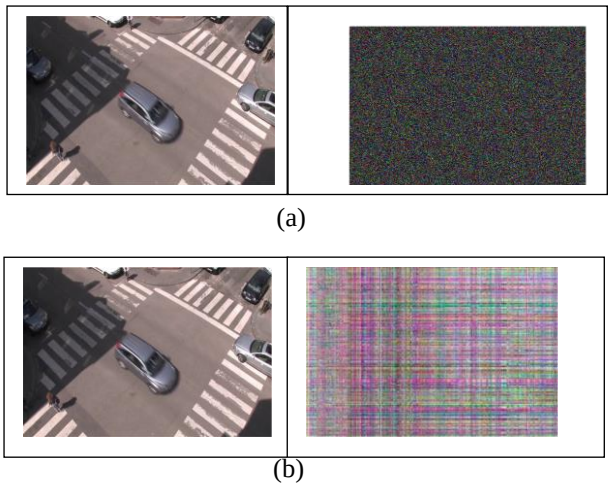


Figure. 7 Comparison of colour composition for both: (a) proposed scheme and (b) sultana algorithm [20]

Table 1. Comparison of encryption time analysis

| Encryption scheme | Encryption time (msec.) |
|---|---|
| **Proposed method** | 0.00254 |
| **JLVEA [21]** | 1.294 |
| **Liu [19]** | 0.515 |
| **Sult [20]** | 70.386 |

On the bases of the original information included in the original video frame, it has local color composition. These colors are removed completely after applied encrypted the original frame. When, the encrypted frame and original frame have the different color information, this prevents the attacker to deduce several of original information from the encrypted frame. This section presents, the experimental results of the proposed scheme to prove that the encrypted video frame is resistant against different attackers and have no similarity between original and encrypted frame.

The security evaluation metric is adopted for evaluation the performance of the proposed cryptographic scheme. The comparison of color composition for both proposed scheme and related work in literature sultana algorithm [20] is implemented for performance evaluation. This comparison is illustrated in Fig. 7.

On the bases of the original information included in the original video frame, it has local color composition. These colors are removed completely after applied encrypted the original frame. When, the encrypted frame and original frame have the different color information, this prevents the attacker to deduce several of original information from the encrypted frame.

### C. Key space analysis

We have used two main phases to generate the secret keys used for video data encryption/decryption tasks. First phase represents by the key generation algorithm at CFN to generate variant values of α parameter with its related IDX value and LMN code composed of 8-digite. The second phase characterized by using the selected α parameter to generate the chaos map with (N×M) chaos keys. In this way the key space will be 28 ×2N×M, which represent a higher key space with higher specifications.

### D. Encryption time evaluation

The key parameter of measuring the execution efficiency for the encryption scheme is an encryption time analysis. In this work, at the presented edge-fog-cloud structure, the proposed cryptographic scheme is analyzed and evaluated based on encryption time. This analysis is very important to evaluate the proposed scheme based on the computation of encryption time which must be reduced to minimum time. Therefore, a lightweight and efficient encryption scheme with low computation time is very essential and required for different media applications.

The proposed encryption/decryption scheme achieving reduces time processing the whole video based on eliminating the identical frames from sequences video frames. These processes make encryption/decryption schemes are very suitable for real time application. For this purpose, the FROI-algorithm is proposed as a pre-processing phase for decreases the encryption frames number and accelerates the encryption process time. Hence, by applying the FROI-algorithm, the size of encrypted data (N×M) in each frame is reduced by specific reduction ratio based on the ratio of differences between current frame and reference frame. The encryption time analysis of the proposed scheme is compared with different methods of literature research works as illustrated in Table 1.

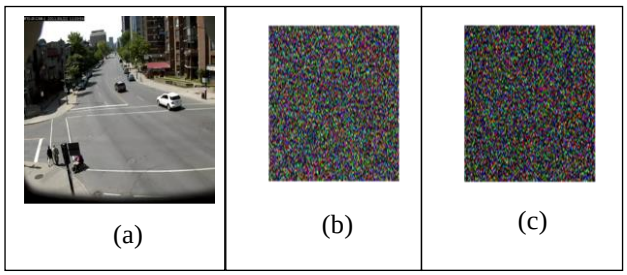
From these results, the encryption time of the (proposed scheme/encryption process) is very low comparing with other algorithms presented in Table 1. Noteworthy, these comparisons are implemented based on using same video files.

### E. Memory efficiency analysis

The memory usage is efficiently analysis for the proposed scheme which is implemented based on computing the memory consumption rate (MCR) factor at encryption case. This metric is utilized to recognize the efficient scheme for encryption process memory based on compute the memory usage by encryption and decryption process. The

Table 2. Comparisons of memory consumption rate

| Algorithm | MCR (Memory Consumption Rate) |
|---|---|
| **Liu [19]** | 5.12 KB |
| **JLVEA, [21]** | 15.4 KB |
| **Proposed algorithm** | 4.5 KB |



(a) (b) (c)

Figure. 8 present the secret key sensitive testing based on encryption and decryption selected video frame using two different secret keys and two different chaotic maps. (a) Original selected video frame (VER1), (b) Encrypted frame (VER1) using secret key SK1, and (c) Decrypted the encrypted video frame (encrypted VER1) using SK2

Table 3. Comparisons the fog-cloud compatibility with Ref [21]

| Algorithm | Ref[21] | Proposed scheme |
|---|---|---|
| **Encryption time (msec)** | 1.294 | 0.00254 |
| **MCR** | 15.4 KB | 4.5 KB |
| **Computation complexity** | high | low |
| **Fog-cloud compatibility** | weak | good |

comparisons of the proposed scheme with related research works are presented in Table 2. The finding results in this table show that, the proposed scheme is efficient for using the memory at encryption case due to the proposed scheme apply the FROI-algorithm before the encryption process.

**F. Key sensitive analysis**

The key sensitive metric is very important features for the proposed scheme evaluation. Any change in the secret key (SK) cause to incorrect decryption results. This means, if one parameter of SK was changed, the original video frame cannot be return by decryption scheme. Therefore, the video frame cannot be decrypted in the correct order without knowing the correct map of all secret keys.

As presented in previous section of this paper, the generation of chaotic map depends on the initial value (α) at the encryption side. Using of two different values of (α) within different one bit (or one digit) leads to generate two different chaotic maps and two different encrypted frames for the same original video frame. For the key sensitive testing of the proposed scheme at the encryption side, the following steps are implemented:

1. The secret key (SK1) at (α = 1.08) is selected to generate chaotic map (CM1). And, the (SK2) at (α = 1.09) is used to generate (CM2).
2. The (CM1) is used for encryption the selected video frame for instance (VFR1).
3. At the decryption side, the (CM2) is used for decryption process of (encrypted VFR1).
4. The finding result is not to be same of the original frame.

Fig. 8, shows the key sensitive testing and analysis based on encryption selected frame using specific secret key SK1 selected from TCODE table and decryption this frame using different secret key SK2 selected from TCODE table also.

On the bases of these results, the proposed scheme has very sensitive to small changing in the (SK) secret key. The sensitivity of secret key at encryption/decryption schemes makes the proposed cryptographic scheme is very strength to make Brute-force attack infeasible.

**G. Comparison study**

This section presents comparisons results of the proposed video encryption scheme with the results of other related works. This comparison implemented based on comparison parameters (encryption time, memory consumption rate (MCR), computation complexity, number of pixels changes rage (NPCR), and unified average changing intensity (UACI)). The target of these comparisons is to confirmation the relevance of the proposed encryption scheme to encrypt the video data before transmission from fog-layer to the cloud-layer.

The work presented in [21] include processes of few modules at encryption scheme such as (seed management module, permutation list management module, an image processing module, and a communication module) as well as depends on separation the color channel for each frame and sending encrypted stream with related encrypted seed. Hence, the implementation of these processes was increased the computations complexity and increase the implementing time for encryption and decryption processes. This comparison result is presented results in Table 3.

On the other hand, the work presented in [22] had been depended on analyses the video frame

Table 4. Employed video files for comparison purposes

| File Name | handshake_right.avi | xylophone1.avi |
|---|---|---|
| **Frame Number** | 145 | 69 |
| **Width** | 640 | 320 |
| **Height** | 480 | 240 |
| **Video Compression** | 'MJPG' | 'DX50 |

Table 5. Comparisons proposed method versus different methods

| Metric | | Ref [22] | Proposed scheme |
|---|---|---|---|
| **Encryption time (msec)** | | 109.345181 | 0.00362 |
| **Decryption time (msec)** | | 124.711446 | 0.00355 |
| **Sensitivity Analysis** | **NPCR %** | 99.687% | 99.892% |
| | **UACI %** | 33.47 % | 33.96% |
| **Computation complexity** | | high | low |
| **Fog-cloud compatibility** | | middle | good |

based on extract I-frame, shuffling each I-frame, separate I-frame into (R, G, and B) color, applied confusing and defusing methods, finally introduce the encrypted I-frame. There work caused to increase the time consuming and increased the complexity of computation. For the purpose of comparison between their work and proposed cryptographic scheme, two video files are utilized. Where, these files adopted by [22] for the performance evaluation and comparisons with other works. The descriptions of these video files are illustrated in Table 4.

The comparison results between proposed work and work of [22] are illustrated in Table 5. This comparison is carried out based on encryption/decryption time and sensitivity analysis (number of pixels changes rage (NPCR) and unified average changing intensity (UACI)). The mathematical formulations of (NPCR and UACI) were implemented based on equations presented in [22].

Both tables (Tables 3 and 5) have some measure metrics which are depended to show the compatibility of proposed encryption scheme for transmit the video data between fog-layer and cloud-layer. The finding results in both tables are proving the compatibility of the proposed scheme for transmit video stream from fog-layer to cloud-layer.

## 8. Conclusion

This paper proposed cryptographic scheme to secure the transmitted video between edge-layer and cloud-layer via fog-layer and. The proposed scheme consists of frame region of interest extraction (FROI-algorithm), light-weight chaotic map, SK generation algorithm. The FROI was utilized to reduce the computation process time. The light-weight chaotic map is used to encrypt and decrypts the current video frame. The SKs generation algorithm to generate the important secretes keys for encryption and decryption video frames. Whole these steps are implemented into fog-layer to transmit video frame to the cloud-layer with secure manner. The distribution of SKs is managed by cloud-layer.

## Conflicts of interest

The authors declare no conflict of interest.

## Author contributions

This work is a contribution of the authors: “Conceptualization, Ekhlas K. Gbashi, Abeer Tariq Maolood, Yaseen Naser Jurn; methodology, Ekhlas K. Gbashi, Abeer Tariq Maolood, Yaseen Naser Jurn; software, Yaseen Naser Jurn and Ekhlas K. Gbashi; validation, Ekhlas K. Gbashi and Abeer Tariq Maolood; formal analysis, Ekhlas K. Gbashi, Abeer Tariq Maolood and Yaseen naser Jurn; writing-original draft preparation, Ekhlas K. Gbashi, Abeer Tariq Maolood; writing-review and editing, Ekhlas K. Gbashi and Yaseen naser Jurn; visualization, Ekhlas K. Gbashi andAbeer Tariq Maolood.

## Acknowledgments

This research was sponsored by Computer Science Department in University of Technology located at Baghdad-Iraq. It was funded by University Technology.

## References


[1] F. Cicirelli, A. Guerrieri, G. Spezzano, A. Vinci, O. Briante, A. Iera, and G. Ruggeri, "Edge computing and socialinternet of things for large-scale smart environments development", *IEEE Internet Things Journal*, Vol. 5, No. 4, pp. 2557–2571, 2017.

[2] T. J. Feng and W. H. Ning, "An efficient and secure data auditing scheme based on fog-to-cloud computing for Internet of things scenarios", *International Journal of Distributed Sensor Networks*, Vol. 16, No. 5, 15 pages, 2020.

[3] A. Marica, R. Giuseppe, C. Claudia, M. Antonella, L. Valeria, and T. Carlos, "Fog Computing in IoT Smart Environments via Named Data Networking: A Study on Service Orchestration Mechanisms", *Future Internet*, 2019, Vol. 11, No. 222, 21 pages, 2019.

[4] A. Jukan, F. Carpio, X. Masip, A. J. Ferrer, N. Kemper, and B. U. Stetina, "Fog-to-Cloud Computing for Farming: Low-Cost Technologies, Data Exchange, and Animal Welfare", *Computer*, Vol. 52, No. 10, pp. 41-51, 2019.

[5] J. Li, Y. Zhang, X. Chen, and Y. Xiang, "Secure attribute-based data sharing for resource-limited users in cloud computing", *Computer and Security*, Vol. 72, pp. 1-12, 2018.

[6] P. Li, J. Li, Z. Huang, G. C. Zhi, C. W. Bin, and C. Kai, "Privacy-preserving outsourced classification in cloud computing", *Cluster Computing*, Vol. 21, No. 1, pp. 277–286, 2018.

[7] J. Li, X. Chen, and M. Li, "Secure deduplication with efficient and reliable convergent key management", *IEEE Transaction on Parallel and Distributed Systems*, Vol. 25, No. 6, pp. 1615-1625, 2014.

[8] J. Li, X. Huang, J. Li, X. Chen, and Y. Xiang, "Securely outsourcing attribute-based encryption with check ability", *IEEE Transaction Parallel and Distributed Systems*, Vol. 25, No. 8, pp. 2201-2210, 2014.

[9] S. Ivan, S. Wen, X. Huang, and H. Luan, "An overview of fog computing and its security issues", *Concurrency Computation Practice and Experience*, Vol. 28, No. 10, pp. 2991-3005, 2015.

[10] T. Wu, S. Wen, Y. Xiang, and W. Zhou, "Twitter spam detection: survey of new approaches and comparative study", *Computer and Security*, Vol. 76, pp. 265-284, 2017.

[11] J. Jiang, S. Wen, S. Yu, Y. Xiang, and W. Zhou, "Identifying propagation sources in networks: state-of-the-art and comparative studies", *IEEE Communications Surveys and Tutorials*, Vol. 19, No 1, pp. 465-481, 2017.

[12] Y. Wang, S. Wen, Y. Xiang, and W. Zhou, "Modeling the propagation of worms in networks: a survey", *IEEE Communications Surveys and Tutorials*, Vo. 16, No. 2, pp. 942-960, 2017.

[13] S. Wen, M. Haghighi, C. Chen, Y. Xiang, W. Zhou, and W. Jia, "A sword with two edges: propagation studies on both positive and negative information in online social networks", *IEEE Transactions and Computers*, Vol. 64, No. 3, pp. 640-653, 2015.

[14] S. K. Sood, "Mobile fog based secure cloud-IoT framework for enterprise multimedia security", *Multimedia Tools and Applications*, Vol. 79, pp. 10717–10732, 2020.

[15] A. Vasileios, E. Kostas, P. Y. Ishibashi, K. 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, 2017.

[16] S. Parikh, D. Dave, R. Patel, and N. Doshi, "Security and Privacy Issues in Cloud, Fog and Edge Computing", *Procedia Computer Science*, Vol. 160, pp. 734–739, 2019.

[17] I. Yehia, A. Valmira, H. O. Ashraf, and J. A. A. Ahmad, "Fog computing security and privacy for the Internet of Thing applications: State-of-the-art", *Privacy and Security Journal, Wiley*, Vol. 4, Issue 2, No. 145, pp. 1-26, 2021.

[18] D. Soni, D. Srivastava, A. Bhatt, and A. Aggarwal, "An Empirical Client Cloud Environment to Secure Data Communication with Alert Protocol", *Mathematical Problems in Engineering*, Vol. 2022, Article ID 4696649, 14 pages, 2022.

[19] F. Liu, H. Koenig, and Puzzle, "A novel video encryption algorithm", In: *Proc. of the IFIP International Conference on Communications and Multimedia Security*, Berlin, Germany, pp. 88–97, 2005.

[20] S. F. Sultana and D. C. Shubhangi, "Video encryption algorithm and key management using perfect shuffle", *International Journal of Engineering Research and Application*, Vol. 7, pp. 1–5, 2017.

[21] Y. Junhyeok and K. Mihui, "JLVEA: Lightweight Real-Time Video Stream Encryption Algorithm for Internet of Things", *Sensors*, Vol. 20, pp. 1-14, 2020.

[22] M. M. Eid, M. E. S. E. Kenawy, and I. Abdelhameed, "A Fast Real-Time Video

Encryption/Decryption Technique Based on Hybrid Chaotic Maps", *Journal of Computer Science and Information Systems*, Vol. 2, Issue 2, 8 pages, 2021.

[23] N. S. Raghava and A. Kumar, "Image Encryption Using Henon Chaotic Map With Byte Sequence", *International Journal of Computer Science Engineering and Information Technology Research*, Vol. 3, Issue 5, pp. 11-18, 2013.

[24] A. Soleymani, M. J. Nordin, and E. Sundararajan, "A chaotic cryptosystem for images based on Henon and Arnold cat map", *Scientific World Journal*, Vol. 2014, pp. 1-21, 2014.

[25] J. Lin and X. Si, "Image encryption algorithm based on hyper chaotic system", *International Workshop on Chaos-Fractals Theories and Applications*, IWCFTA 2009, pp. 153–156, 2009.

[26] J. P. Jodoin, G. A. Bilodeau, and N. Saunier, "Urban Tracker: Multiple Object Tracking in Urban Mixed Traffic", *IEEE Winter Conference on Applications of Computer Vision (WACV14), Steamboat Springs*, Colorado, USA, pp. 885-892, 2014.