IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received December 29, 2019, accepted January 6, 2020, date of publication January 14, 2020, date of current version January 27, 2020.

Digital Object Identifier 10.1109/ACCESS.2020.2966656

SMSH: Secure Surveillance Mechanism on Smart Healthcare IoT System With Probabilistic Image Encryption

JALALUDDIN KHAN[1], JIAN PING LI[1], BILAL AHAMAD[2], SHADMA PARVEEN[3], AMIN UL HAQ[1], GHUFRAN AHMAD KHAN[4], AND ARUN KUMAR SANGAIAH[5]

[1]School of Computer Science and Engineering, University of Electronic Science and Technology of China, Chengdu 611731, China
[2]College of Computing and Information Technology, Shaqra University, Sharqra 11961, Saudi Arabia
[3]School of Management and Economics, University of Electronic Science and Technology of China, Chengdu 611731, China
[4]School of Information Science and Technology, Southwest Jiaotong University, Chengdu 611756, China
[5]School of Computing Science and Engineering, Vellore Institute of Technology (VIT), Vellore 632014, India

Corresponding authors: Jalaluddin Khan (jalal4amu@yahoo.com) and Jian Ping Li (jpli2222@uestc.edu.cn)

This work was supported by the National Natural Science Foundation of China under Grant 61370073, National High Technology Research and Development Program of China under Grant 2007AA01Z423, the Project of Science and Technology Department of Sichuan Province, Chengdu Civil-Military Integration Project Management Company Ltd., and Sichuan Yin Ten Gu Technology Company Ltd.

ABSTRACT The Internet of Things is made of diverse networked things (i.e., smart, intelligent devices) that are consistently interconnected, producing meaningful data across the network without human interaction. Nowadays, the Healthcare system is widely interconnected with IoT environments to facilitate the best possible patient monitoring, efficient diagnosis, and timely operate with existing diseases towards the patients. Concerning the security and privacy of the patient's information. This paper is focused on Secure surveillance mechanism for a medical healthcare system with enabled internet of Things (sensors) by intelligently recorded video summary into the server and keyframes image encryption. This paper is twofold. Firstly, a well-organized keyframe extraction mechanism is called to extract meaningful image frames (detected normal/abnormal activities keyframe) by the visual sensor with an alert sent to the concerned authority in the healthcare system. Secondly, the final decision about the happened activity with extracted keyframes to keep highly secure from any adversary, and we propose an efficient probabilistic and lightweight encryption algorithm. Our proposed mechanism verifies effectiveness through producing results, robustness in nature, minimum execution time, and comparatively secure than other images (keyframes) encryption algorithms. Additionally, this mechanism can reduce storage, bandwidth, required transmission cost, and timely analysis of happened activity from any adversary with protecting the privacy of the patient's information in the IoT enabled healthcare system.

INDEX TERMS Secure surveillance, Internet of Things, privacy, security, image encryption.

I. INTRODUCTION

Nowadays, Internet of Things (IoT) is intended to nurture speedily due to the creation of information communication and might be supposed as a description of ubiquitous computing because of IoT extends replacement with the direct user involvement to the continuously interconnected collaborative working devices (sensor connected devices) without human interaction [1]–[3]. IoT applications are coherently worked as a built-in sensor within the smart applications such as intelligent healthcare system, smart wireless multimedia surveillance networks (SWMSN), smart cities, radio-frequency identification tags (RFID), self-driving vehicles (SDV), drones surveillance systems (DSS), automobiles, biochip remote surveillance on farm animals, smart homes, smart transportation system (STS) and smart industry monitoring system etc [4]–[9]. These recent research and development in high processing abilities birth as an intelligent IoT (Internet of Things) ecosystems that are more than capable of working coherently (intelligently meaningful interaction with the surroundings).

Wireless multimedia surveillance networks (WMSN) are one of the essential areas of IoT enabled ecosystem which works with visual sensors, uniformly observation in each

The associate editor coordinating the review of this manuscript and approving it for publication was Wei Wei.

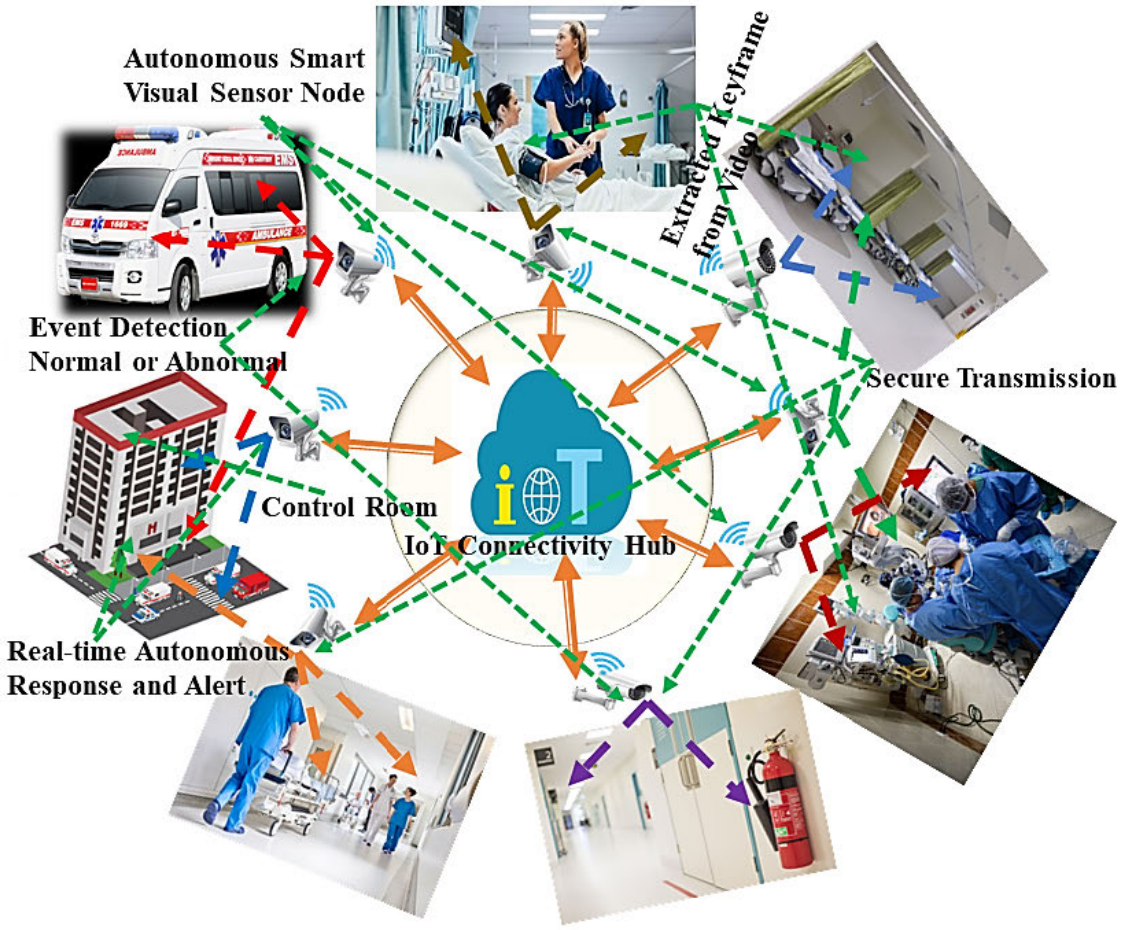


FIGURE 1. Secure surveillance mechanism on smart healthcare into IoT ecosystem.

aspect (views), uninterruptedly capturing images and as a result, it is producing a vast quantity of multimedia (visual data) with substantial redundancy [10]–[15]. Due to more redundant visual data availability in the intelligent system it is commonly agreed with the researcher that surveillance network processed meaningful, informative visual data and should be adequately recorded for the future usages, like tracing patient activities (normal or abnormal), doctors diagnosis activities, operation rooms activities, how staff (nurses) handling patients and hygienic healthcare facilities into the hospital in each wards. The main emphasis should be captured all the possible abnormal event detection through data analysis with the proper management and video abstraction. The reason behind this is that sending all the visual data by communication lines prior to processing is not reasonable because it consumes a lot of bandwidth constraints and energy. In addition, it is relatively tough as well as time spent for a specialist to resourcefully extract actionable intelligence from the massive amount of surveillance data [16].

Therefore, it is required such a type of machinery that can collect all critical visual information separately by employing the high processing and communication abilities of smart IoT enabled visual sensors. These mechanisms can intelligently select proper sight (views) from different locations (multi-views) surveillance records captured by the various IoT enabled sensors. These can smoothly process visual data in real-time, and only informative (relevant) data send to concern authority for future usage.

Furthermore, it is most important that surveillance specialists took favorable verdicts by investigating typical video data, relevant contents of the original massive sequence of visual information. A conventional smart healthcare surveillance system is shown in the ''Fig 1'' for capturing every critical movement to detect any normal or abnormal activities intelligently and reported in real-time to concern authority to take actionable response against the happened events promptly. Surveillance or monitoring in the smart healthcare system by Wireless multimedia sensor networks (WMSNs), it needs two essential requirement robustness and well-organized resource utilization [17], [18]. For achieving robustness in real-time surveillance, our system should ready to investigate each visual sensor in a certain period to solve the technical malfunctioning or natural disasters and human interaction.

Further, the nature of transmitting visual data in the WMSN is wirelessly to the base station as well as a visual processing hub. This type of communication before vulnerable to several security issues, consequently, essential to send imaging data securely to the base station with a proper security mechanism to deal with any alteration or modification from the untrusted parties. Furthermore, we feel that the utilization of devoted transmission of visual data in WMSNs is relatively problematic in nature due to the congested spectrum allocation mechanism.

Therefore, in this article, we emphasis to address such types of problems by using the intelligent system as well as power-efficient which can manage every sensor intelligently and autonomously to gather only the most relevant data in real-time and take appropriate action with respective scenarios. In this way, this mechanism can be capable of reducing transmission costs and congested bandwidth consumptions. Furthermore, our main objective to make a security prototype. For secure transmission of visual data within the smart healthcare system to concern authority with improved utilization and protection of WMSNs resources. Technically this system is generated an encrypted image of keyframes before transmission for achieving higher security in nature during the communication within the smart healthcare WMSNs.

Paper contributions are listed as follows:

1. We propose a Secure Surveillance Mechanism with Probabilistic Image Encryption on Smart Healthcare IoT System.
2. The proposed system emphasis firstly, extract meaningful image frames (detected normal/abnormal activities) from summarized video in keyframe extraction module.
3. Secondly implemented an efficient probabilistic and lightweight encryption algorithm at extracted keyframes to keep highly secure from any adversary.
4. The proposed scheme is utilized TensorFlow, python, lightweight YOLOv3 algorithm for extraction of keyframes and MATLAB simulation is evaluated for its cryptographically secure communication to reduce transmission cost with congested bandwidth consumptions efficiency.
5. The proposed research certifies some of the imperatival properties, for example, patients' privacy as an encrypted data from any adversary.
6. The various rigorous security analysis shows that numerous known attacks can withstand with the proposed research work.

The remaining section of this article is described as follows. Section II has explained briefly in terms of related work. Section III has explained briefly a novel proposed secure surveillance mechanism which consists keyframe extraction model from visual data and lightweight keyframe encryption algorithm. Section IV has analyzed experimental results and discussion. Section V has explained various rigorous security analysis in terms of different security parameters, and Finally, Section VI is providing concluding remarks as well as future work.

II. RELATED WORK

Recent developments in wireless multimedia sensor networks (WMSNs) birth as a smart healthcare system that facilitates best practices in the hospital activities with the connection of security, privacy, and safety of the patients. Ensuring security, confidentiality, and safety, it is needed to analyze visual surveillance data as well as adoptive encryption mechanism which can verify the truthfulness of the system which is built for the absolute protection or safety towards the patients. While bringing comfort to human lives, the large information of surveillance raises the challenge of consuming time and space when the video is retrieved. Therefore, some information views need to be gained without viewing the entire video, and video summary methods are suggested to extract the keyframes. Over the previous two decades, video summary has gained comprehensive study attention. It aims to abbreviate one lengthy video or various images in a very compact form, like video skimming and static storyboarding. Zong et al. reported on [18] four requirements should be met by multi-video summarization (MVS) conciseness, representativeness, adjustment of queries and understandability. MVS process can be considered as a common problem of visual pattern exploration, and his hypergraph based dominant set (HDS) method to cluster the main content into groups as well as centroids are selected keyframes for each group. This step promises the representativeness of the summary. For obtaining conciseness, used QD-MMR (query dependent maximum marginal relevance) method and achieving understandability applied GTC (graph-based topical closeness) algorithm. In another article, Ji *et al*. [20] explained [20] MVS process via multi-modal weighted archetypal analysis (MVS-MWAA) to extract an efficient, concise summarization, which is mutually informative, representative and ensuring summarization comfortable, understood applied to rank from the bottom to top (RBT) approach.

Fei *et al*. [21], the profound network predicted picture memorability score is presented and coupled with the keyframe extraction entropy value. Not only are the summaries generated semantically interesting, but they also maintain the videos' variety. To estimate the efficiency of user summaries and produced summaries, f-measures are introduced in parallel. Song *et al*. [22] explained the event-based video synthesis method is more appropriate for video surveillance synthesis than the keyframe-based strategy, integrating the random forest with trajectory characteristics to detect unusual events and achieving excellent outcomes. Modeling a disjoint max-coverage approach to produce a summarized series with extra coverage and the minimum number of frames. Mehmood *et al*. [16] reported [16] the dynamic technique of visual saliency is grounded on the fact that salient motion attracts human visual attention, which can be calculated by temporal gradients, which reflect as a novel approach by reducing computation costs. Using the

prioritization algorithm which extracts semantically valuable video frames from videos, therefore, this technique reduced consumption required bandwidth. Furthermore, the author claimed that the performance of his technology (image-based temporal gradients) is noticeably better than the existing one like delta entropy as well as delta edge.

Hamza *et al*. [23] addressed a new idea which is efficient cryptosystem to provide security into secure surveillance approach at the IoT ecosystem. Further explanation of the cryptosystem, he mentioned that this approach has three-fold. firstly, A lightweight automated summarization methodology focused on a convenient histogram clustering method has been used to retrieve keyframes through video surveillance. Secondly, for compressing the generated data size, he is incorporated a discrete cosine transformation (DCT) methodology. Thirdly, the proposed method uses a discrete fractional random transformation (DFRT) to perform a successful image encryption technique. Furthermore, he ensured his system is fast, safe and effective in real-time processing by reducing transmission as well as storage costs. In another article, Hamza *et al*. [24] explained a framework which is video summarization for outdoor patients and based on Wireless capsule endoscopy methodology. In this approach, using a lightweight video description method and keyframes are retrieved. Utilizing a cryptosystem in which 2D Zaslavsky chaotic map are used to enhance security prototype of keyframes. Li *et al*. [25] proposed system which should meet sensor node criteria for minimal computational complexity, lower power expenditure and low overhead storage. Furthermore, he is presented a compressed sensing model and a parallel reconstruction approach, that approach is trying to reduce time complexity of the image encryption. Handling image encryption the author is preferred chaotic environment to integrate quantization as well as diffusion method to enhance security during transmission.

The digital image cryptographic encryption can be widely categorized into two main groups, such as color image encryption as well as grayscale image encryption. It's often seen cryptographic techniques and concepts of the gray-level picture can also be expanded to color picture encryption by applying in the red green and blue plane. Huang *et al*. [26] expressed his technique for color image encryption in which permutation-diffusion occurred simultaneously, and permutation-diffusion (PDSO) is interacting remarkably well between confusion-diffusion. As a result, it gained a better security aspect with high efficiency in this method. Chai *et al*. [27] described color image crypto technique grounded on chaos and DNA encryption, he decomposed a color image into all three planes (red, green, blue) and instantaneously intra-inter component permutation mechanism dependent on the plaintext (SCPMDP) is operated to shuffle them, furthermore converted as well as recombined permuted sequence into DNA matrix. Finally, enhancing security applied second confusion operation with scrambling images and getting cipher images. Generating pseudo-random chaotic sequences author assembled the four-wing hyper-chaotic system in his mechanism.

Wang and Li [28] reported a new composite chaotic color image encryption with a tent map and logistic map for crucial initial processing. He obtained image scrambling through Arnold map function. The encryption utilizes the chaotic neural network of Hopfield, which has a substantial impact on the method of diffusion. The suggested method showed noise attacks, anti-cutting and information entropy comparatively better than the existing algorithm. Broumandnia [29] explained a five-stepped color image encryption technique for confusion and diffusion characteristics in 3D space based on replacement and permutation activities. Applied 3D modular chaotic map and 3D permutation operations to transform an image into a 3D space, which improves period (time), speed, and key space during RGB image encryption. Hua and Zhou [30] The CTBCS can engender chaotic maps with complicated dynamic behaviors by using two combine chaotic maps as seed maps to perform a more complex nature as well as dynamic behaviors. The encryption system utilizes high-efficiency scrambling to separate neighboring pixels and utilizes random order replacement to distribute a small change of pixel in the plan as well as cipher image. Furthermore, he showed that the CTBCS produced chaotic maps display significantly more complex, chaotic behaviors than the current ones.

Hamza *et al*. [31] expressed a profitable probabilistic cryptosystem to secure the confidentiality of keyframes and privacy of patients. A new PRNG based on chaos that relies on cascading and mixing two of the 2D chaotic maps' orbits. His cryptosystem's encrypted images exhibit random nature that ensures computing effectiveness as well as the greatest level of safety against multiple assaults for keyframes. In addition, it performs the patient data without exposing any information, maintaining the privacy of the patient by only enabling approved users to decrypt. In another article, Valandar *et al*. [32] proposed a fast color image encryption technique, that is based on the suggested 3D chaotic map. This method produces three numbers in general and Bitxored with RGB channels. Continue the process by splitting an image into 4×4 sections and altering the places of these components. The proposed method splits each portion into 16×16 blocks and afterward, the sections are permuted with various map keys. Experimental findings indicated that encrypted image histograms are consistent and the correlation between host and cipher image is very near to zero.

Alawida *et al*. [33] recommended new image encryption based on the perturbation of the chaotic hybrid system. As part of a new chaos-based technique, the suggested hybrid system combines and cascades two chaotic maps. Chaotic performance assessment showed that the new hybridization approach has stronger complexity, sensitivity and a wider range of chaotic parameters particularly in comparison to other newly proposed methods of chaotification. Asgari-Chenaghlu *et al*. [34] presented a polynomial mixture of 1D chaotic maps mixed into an algorithm for dynamic

image encryption. It is unique because it not only has a butterfly folding impact but also demonstrates generalization nature over any mixture of polynomials. Regulated polynomial combination parameters therefore trigger the butterfly folding impact. In addition, numerous simulation assessments demonstrate the superiority of the suggested chaotic system and image encryption scheme has greater statistical as well as cryptanalytic characteristics relative to state-of-the-art schemes.

Mondal *et al*. [35] reported highly secure image encryption operations for secure communication and storage of images which is mainly focused on cellular automata (CA) and chaotic skew tent sequences. The chaotic skew tent sequence is operated for the CA as the original vector generator that requires an original bit sequence of 128 bit to produce pseudo random number sequence (PRNS). By using the PRNS, first permuted plain image pixels for removing high correlation among the adjacent pixels in the plain image. After that permuted image is encrypted by the chaotic skew tent sequence using a single random number. Combining of the chaotic map and CA provides a higher key space scheme and a quicker PRNS generator. Kumar and Acharya [36] proposed multiple piece-wise linear chaotic map (PWLCM) scheme which is suggested to use as an effective color image encryption system. First, the suggested system conducts rotational permutation procedures based on two multi-way blocks and then row-column rotational permutations. Lastly, the row, column as well as block diffusion activities are performed. This system is easy and secure because with only PWLCM schemes it includes easy rotational permutation activities. The benefits of this system in terms of operational complexity and simulation time are high security, high key space, high effectiveness, and simplicity.

III. PROPOSED WORK SECURE SURVEILLANCE MECHANISM

Increasing demand for continuous monitoring, improving visual sensor technologies, and advancing IoT technologies have required effective management and timely analysis of the digital world produced by the ever-increasing amount of monitoring networks in the smart healthcare systems. These techniques enable the video information to be analyzed automatically to produce an independent reaction in real-time. Visual sensor networks (VSN) have now become smarter, allowing them to conduct complicated information processing in real-time with enhanced storage and processing capacities. For secure video surveillance recorded in hospital settings, their processing capabilities can be used to evaluate the video stream to recognize keyframes and then throw away insignificant and redundant visual information, thus trying to minimize the demands for bandwidth. In order to produce video-view summaries of surveillance footage in real-time, the enhanced communication capabilities of sensor nodes can also be used to conduct advanced scene analysis in conjunction. After recognizing unusual occurrences such as patient's emergency needs or patients fell with high blood pressure or patients feel heart attack symptoms and shouting to attract emergency cure, the intelligent sensors can also be used to produce an independent reaction using the smart healthcare IoT infrastructure. Besides, keyframe security can be achieved through the application of lightweight encryption algorithms, taking into account processing capacities, memory and transmission limitations. A typical proposed smart healthcare surveillance system is shown in the ''Fig 1''. The following sections illustrate the details of this structure and its primary personifications.

A. KEYFRAME EXTRACTION MODEL FROM VISUAL DATA

The visual processing hub (VPH) receives visual information from visual sensors as a video frame in the smart healthcare surveillance networks, leading to significant amounts of video information. The transportation of the all video streaming is unrealistic due to the broader range (distance) between the base station and visual processing hub (VPH) due to bandwidth as well as the energy limitations of WMSNs. Researchers have used distinct compression [37], [38] and video summary methods [18]–[21] to address this problem in order to decrease the quantity of visual information at the visual processing hub (VPH) so that only most relevant video frames are furthered to the base station (BS) for processing. Considering energy constraints as well as the bandwidth, keyframe extraction employed to reduce data redundancy in which [16] expressed his thought in terms of salient motion detection. Our proposed extraction YOLOv3 algorithm for keyframes is lightweight because it is utilized a training image dataset and characterized to detect human presence from the recorded videos, which are conceptually showing in the ''Fig 3''. YOLOv3 algorithm [39] is an efficient not only in the detection of images and videos but also in the real-time scenario. We trained this model into the darknet platform [40]. Furthermore, it was converted into the TensorFlow environments. For high precision, it is required to train the model with more samples of images like any vast dataset. With the intention of this, the model was trained by the well-known wider-face dataset [41]. YOLOv3 prefers to use in the images or video; however, the resolution of the image should be the factor of 32. The default resolution is originally set to 416x416. This algorithm is preferred height, and the width of the image should be the same size. We don't need to change the resolution of the image before input, and we had designed programmatically to convert the resolution of the image automatically when required resolution. The model is a floating-point by default, which is converted into the fixed-point model by using TensorFlow, so that, this computationally competent algorithm can be easily employed on a smart healthcare IoT system as well as any small devices, for example, visual sensors which have bandwidth constraints, processing, and energy. We tested this model by using Face Database (FDB) [42]. The employed approach proposes a method to increase detection precision when promoting a real-time process by modeling YOLOv3's bounding box (bbox), the most symbolic of single-stage detectors.

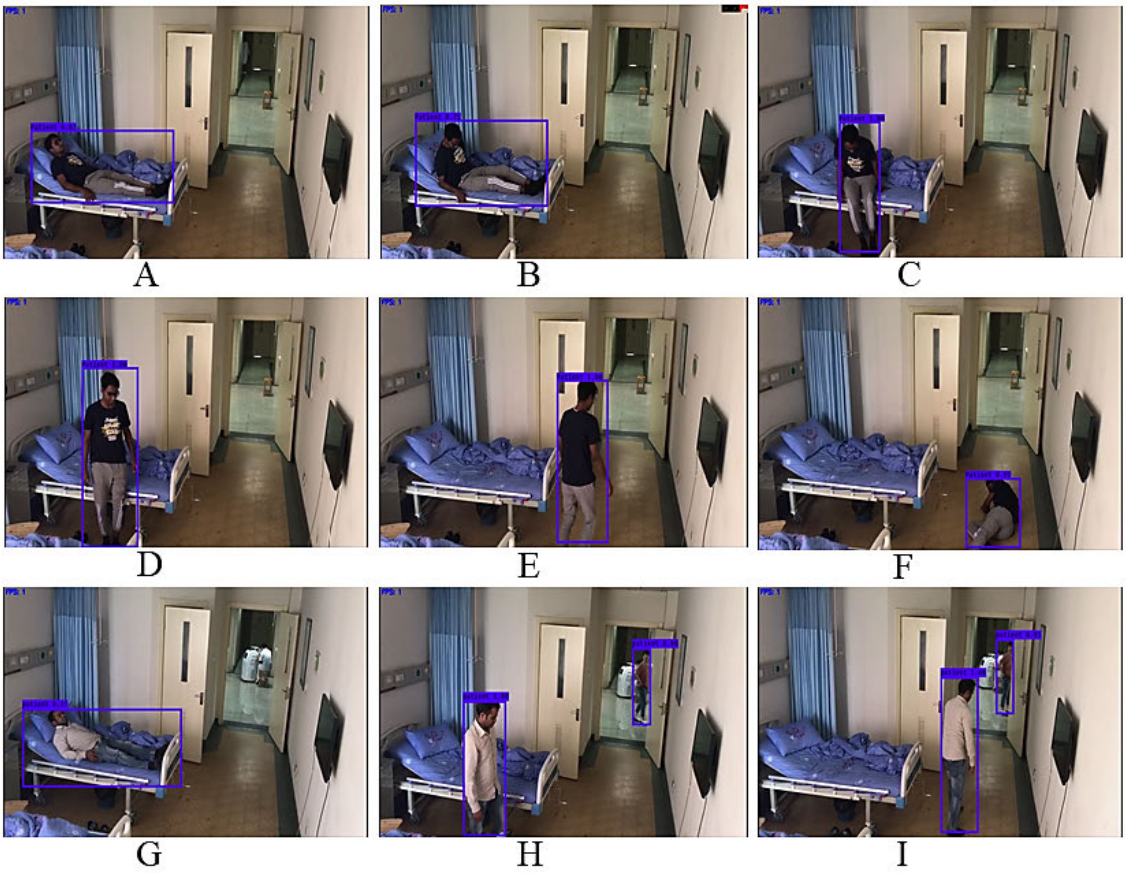


FIGURE 2. Extracted keyframes of patients from visual sensors.

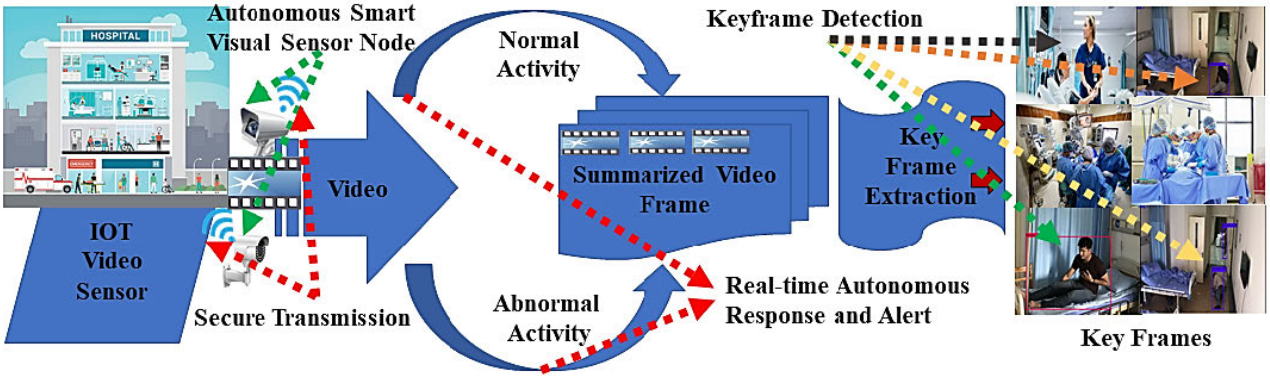


FIGURE 3. Keyframe extraction process from visual sensors.

The average accuracy of the model is 88-90% with 1-16 FPS (file per second) on Intel Core i5-5th generation system, which is more appropriate regarding patient's monitoring in the smart healthcare system as shown extracted keyframe in "Fig 2". Extracted keyframe from recorded video, which is clearly shows into the "Fig 2", from each sub-section A to I. Every interaction or movements of the patient is accurately detected with high precision and within the bounding boxes. This extraction process is employed with deferent patients in various hospital wards into the smart healthcare setup, and as a resulted keyframe is shown into the "Fig 2" A to I sub-section. After that effectively and significantly produced keyframe from keyframe extraction model is passed to the lightweight encryption model for further secure operation.

B. PROBABILISTIC AND LIGHTWEIGHT KEYFRAME ENCRYPTION ALGORITHMS

This section introduces and analyzes the suggested cosine-transform-based chaotic sequence (CTC) [30] characteristics as well as an encryption process in a smart healthcare IoT

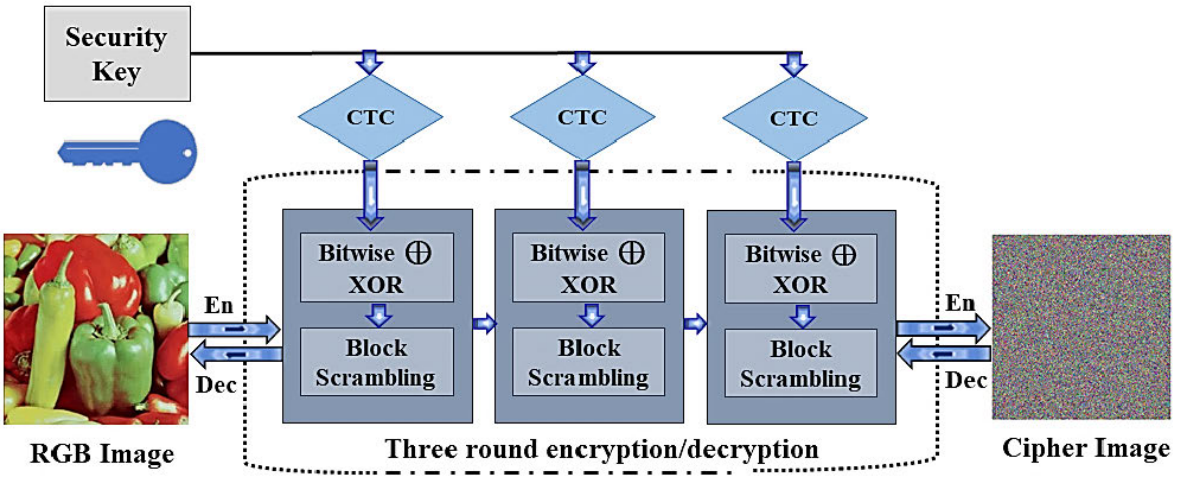


FIGURE 4. Keyframes encryption process.

system for keyframes which is extracted from the visual sensor stream. The suggested algorithm has two main parts: the first component is intended to use the latest cosine-transform-based chaotic sequence (CTC) [30] to generate PRNG appropriate for our suggested image encryption and the second component is designed to perform three round of confusion – diffusion procedures for the keyframe as shown in the "Fig 4". Most monitoring systems are recorded videos in RGB format via high-resolution visual sensors. We are, therefore, proposing a fast RGB keyframe encryption algorithm that ensures both privacy and keyframe confidentiality. We also use a CTC randomized sequence, which makes it impossible for intruders to know anything with the ciphered frames about the original data. This limits the accessibility of the data needed to construct a model of cryptanalysis to attackers.

1) COSINE-TRANSFORM-BASED CHAOTIC SEQUENCE (CTC)

The proposed CTC sequence is aimed for the addressing the drawbacks or weaknesses in frail chaos and weak dynamic tendencies of existing chaotic maps. The CTC can be described as mathematically:

$$x_{i+1} = cos\left(\pi\left(F\left(a, x_i\right) + G\left(b, x_i\right) + \beta\right)\right) \tag{1}$$

where $F\left(a, x_i\right)$ and $G\left(b, x_i\right)$ are the two current chaotic maps, which are recognized as a typical seed map among them a and b are known as a control parameter and β is used as a constant shifting operator (set as $\beta = -0.50$). Table 1 is briefly described all the symbols and notations used in our experimental setup. As shown in Eq. (1), the CTC sequence first integrates $F\left(a, x_i\right)$ and $G\left(b, x_i\right)$ outputs with a β constant shifting operator and then operates a cosine transformation to accumulate the output. The overall combination procedure can shuffle the chaos structure of the both two seed sequence maps efficiently, and cosine transform displays very complicated non-linearity. Therefore, the CTC sequence of newly chaotic maps has more complex in nature.

TABLE 1. Symbols and notations used in this paper.

Symbol	Description
CTC	Cosine-transform-based chaotic sequence
a and b	Control parameter
β	Constant shifting operator
r	Parameter of the produced chaotic maps
FN	Finite Number
IN	Integer Number
⊕	Bitwise XOR
Φ(α)	Cumulative density function of standard normal distribution
H_0	Null hypothesis
H_1	Alternate hypothesis

Because the CTC sequence seed maps $F\left(a, x_i\right)$ and $G\left(b, x_i\right)$ can be the same existing chaotic maps, consumers have the flexibility to make countless fresh chaotic maps using distinct configurations of existing maps. The actual combination of cosine-transform-based chaotic sequence (CTC) is used in this proposed method with the help of logistic maps and sine maps which is mathematically defined as follows:
Logistic Map:

$$x_{i+1} = L\left(r, x_i\right) = 4rx_i\left(1 - x_i\right) \tag{2}$$

Sine Map:

$$x_{i+1} = S\left(r, x_i\right) = rsin\left(\pi x_i\right) \tag{3}$$

Using Eq. (2) and Eq. (3) we can mathematically define cosine-transform-based chaotic sequence (CTC) is:

$$x_{i+1} = cos\left(\pi\left(4rx_i\left(1 - x_i\right) + \left(1 - \mathrm{r}\right) sin\left(\pi x_i\right) - 0.5\right)\right) \tag{4}$$

we fixed Eq (2) and (3) in Eq. (4) and mentioned a replaces to r and b replaces to $1 - \mathrm{r}$, where r is known as a parameter of the produced chaotic maps $\mathrm{r} \in [0, 1]$.

2) COSINE-TRANSFORM-BASED CHAOTIC SEQUENCE IMAGE ENCRYPTION SYSTEM (CTC-IES)

In cryptography, chaotic maps are always produced their complex nature, which dominates the security aspect of the corresponding cryptosystem. We modeled the CTC-IES in this section, which is the combination of two seed maps (Logistic and Sine). It implements the eminent confusion-diffusion mechanism, which is a high-secure encryption framework as Illustrated in the "Fig 4" to comply with the real-time processing requirements of IoT devices in the smart healthcare system. The secure key generates initial-states (x_0, y_0) intended for the CTC map to create chaotic sequences, that provide bitwise XOR and block Scrambling. Bitwise XOR operation performed to encrypt in each channel of color images [I_R, I_G, I_B] separately with designed block scrambling to disperse adjacent-pixels into dissimilar positions rapidly, which is determined through the chaotic sequence. "Fig 4" is showing, three rounds of diffusion and block scrambling operations in which keyframe images are ensuring adequately encrypted data as a cipher-image without recognizing actual keyframes in the smart healthcare system.

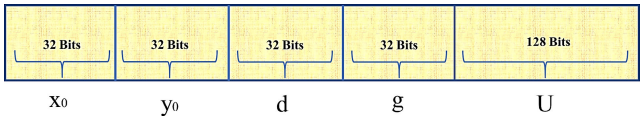


FIGURE 5. The key structure of CTC-IES.

3) KEY STRUCTURE

The secure key governs the preliminary situations of the CTC sequence. Concerning to [43], it is preferred to withstand various types of attacks when the key space of any chaos-based cryptosystem should meet the proportions of 2^{100}. The length of the secure key in CTC-IES is set 256 bits. Consequently, key space should be 2^{256}. "Fig 5" demonstrates the complete structure of the secret key which consists of five component $K = \{x_0, y_0, d, g, U\}$ among them original initial states are (x_0, y_0), d is known as the parameter of disturbance to distract the initial state, g is the initial state coefficient and U includes four disturbance parameter coefficients as $\{U_1, U_2, U_3, U_4\}$. Individually of x_0, y_0, d, g, U_1, U_2, U_3, U_4 is 32-bit long. Variables x_0, y_0, d, within [0,1] are float values and individually can be attained as of a 32-bit stream by:

$$\text{Float Number } (FN) = \sum_{i=1}^{32} Bin_i \times 2^{-i}.$$

g, U_1, U_2, U_3, U_4 are integer coefficients, which can all be acquired through integer value as:

$$\text{Integer Values } (IN) = \sum_{i=1}^{32} Bin_i \times 2^{i-1}$$

The initial states can be further computed as described for the three rounds of encryption mathematically can be expressed at Eq. (5):

$$\begin{cases} x_0^i = (x_0 \times g + d \times U_i) \bmod 1; \\ y_0^i = (r_0 \times g + d \times U_i) \bmod 1, \end{cases} \tag{5}$$

The CTC map can produce uniformly distributed chaotic sequences, as shown in the "Fig 6" for bitwise XOR and block scrambling operation using the initial states (x_1, y_1).

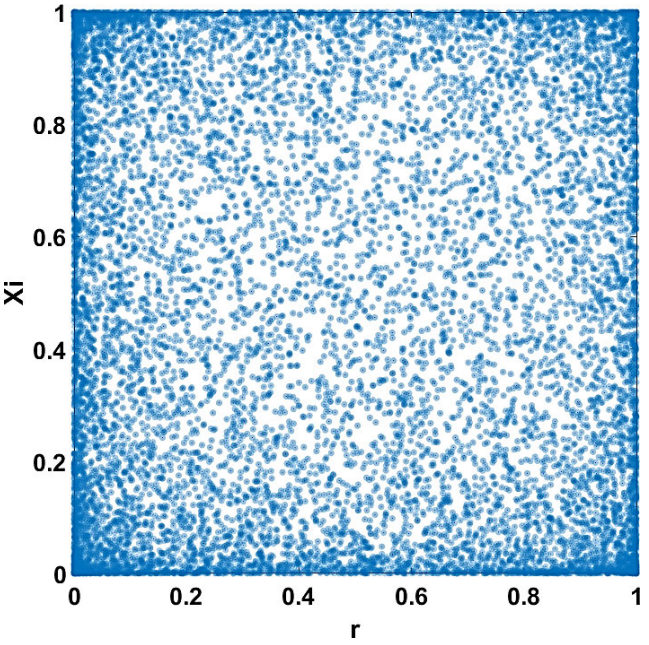


FIGURE 6. Complex CTC sequences.

4) LIGHTWEIGHT IES

The keyframe encryption/decryption method of the suggested CTC-IES algorithm is displayed in Table two, three and four, respectively. The mechanism for encryption is defined as follows:

Step 1.

The original keyframe image is permuted through the cosine-transform based chaotic sequences by the using a random secret key to attaining the complex nature of the chaotic sequence. Furthermore, reshaping keyframe images with newly generated complex chaotic sequence and splitting keyframe color image into three color channels like red(R), green(G), and blue(B). Each color image remains in the form of a matrix (I_R, I_G, I_B) for the further three-rounds operation of bitwise XOR and block scrambling.

Step 2. Each keyframe matrix data is diffused through the bitwise XOR with the conjunction of block scrambling operation to produce the cipher image.

Step 3.

The cipher image is confused by the block scrambling algorithms to acquire the resulted encrypted cipher image.

The method for decryption is followed by the inverse block scrambling and inverse bitwise XOR operation, which is used successively to decrypt the cipher image into

TABLE 2. Algorithm 1: encryption operation by using bitwise XOR.

Input: Keyframe image size MxN with initial state $\left(X^{i}_{0}, Y^{i}_{0}\right)$	
Output: Cipher keyframe Image C	
1.	Read MxN RGB keyframe Image
2.	Resize RGB keyframe image
3.	Generating random number for key
4.	Generating key (calling keygen function by using random number)
5.	Generating CTC sequence (calling ChaoticSeq function by using secret key);
6.	Reshape image (by using chaotic sequence)
7.	Split RGB keyframe image into 3 channels (I_R, I_G, I_B) r = rgb(:,:,1); g = rgb(:,:,2); b = rgb(:,:,3);
8.	Start three rounds for loop *(for m=1:3);*
9.	Bitwise XOR performed in each image channels (I_R, I_G, I_B)
10.	Performed block scrambling algorithm *(bitwise operated keyframes size (I_R , I_G , I_B,), block size, key, state);*
11.	End *(end for loop);*
12.	Merging each cipher color channels keyframe image
13.	Cipher keyframe image (encrypted) *C=CipherImage;*

TABLE 3. Algorithm 2: cosine-transform-based chaotic sequence generation.

Input: Key and Keyframe image size MxN	
Output: Chaotic sequence	
1.	Read key K (and assign to x)
2.	Read r *(r ∈ [0, 1])*
3.	Initialize Chaotic sequence
4.	*for m=1:1000*
5.	$X = cos\left(\pi \times \left(4 \times r \times x \times (1 - x) + (1 - r) \times sin(\pi \times x) - 0.5\right)\right)$
6.	*end*
7.	*for m=1: MxN*
8.	$X = cos\left(\pi \times \left(4 \times r \times x \times (1 - x) + (1 - r) \times sin(\pi \times x) - 0.5\right)\right)$
9.	*S(m)=X*
10.	*end*
11.	Chaotic sequence

a keyframe image. Table two, three, and four demonstrated the pseudocode for both the bitwise XOR procedure and the block scrambling procedure, respectively, where S is a CTC sequence generated by the combination of two chaotic cosine logistic as well as sine map, and m x n is the original keyframe image size. The secure key is used throughout the CTC sequence and is created by using the random key generation algorithm.

IV. EXPERIMENTAL RESULTS AND DISCUSSIONS

This section enforces and discusses the experimental results of the proposed CTC-IES at the environment of MATLAB 2018a software and all the test images are used from well-known USC-SIPI [44] digital image database repository. An encryption method should always be able to encrypt various kinds of digital images into high-security cipher images. The information on the keyframe image can only be fully recovered by using the appropriate secret key. Without the appropriate (proper) secret key, no information about the original keyframe image can be obtained. ''Fig 7 and 8'' illustrates each sub-section from A to P, the CTC-IES encrypted images are using keyframe extraction image for smart healthcare IoT system. ''Fig 7'' sub-section A and I is the plain image in which A is the plain image from regular hospital monitoring image and I is the standard test image Lena. In the Lena test image J, K, L is the histogram of the color channel red, green and blue respectively, encrypted color channel of Lena histogram is N, O and P. ''Fig 8'' sub-section A and I is the keyframe image. In the keyframe image B, C, D, J, K, L is the histogram of color channel red, green and blue

TABLE 4. Algorithm 3: block scrambling.

Input: Bitwise operated keyframe channels *(I_R, I_G, I_B)* size MxN, block size, key, state	
Output: Scrambled cipher keyframe channels *(scramble I_R, scramble I_G and scramble I_B)*	
1.	Read *MxN I_R, I_G, I_B* channels separately (bitwise XOR operated image)
2.	Resize bitwise XOR operated image by dividing block size s
3.	Randomize state with key (secure key from function)
4.	Randomize Matrix R
5.	*If W=0* (forward scrambling means encrypt w=0)
6.	*[~, loc1] =sort(R);* (sorting matrix R)
7.	*k=1;* (initializing variable)
8.	*for i=1: a*
7.	*for j=1: b*
8.	$c_i = cei1\left(\frac{loc1(k)}{b}\right)$;
9.	$c_j = loc1(k) - (c_i - 1) \times b$;
10.	$temp = in\big((s \times i - s + 1) : s \times i, (s \times j - s + 1) : s \times j\big)$;
11.	$in\big((s \times i - s + 1) : s \times i, (s \times j - s + 1) : s \times j\big) = in\big((s \times ci - s + 1) : s \times ci, (s \times cj - s + 1) : s \times cj\big)$;
12.	$in = \big((s \times ci - s + 1) : s \times ci, (s \times cj - s + 1) : s \times cj\big) = temp$;
13.	$k = k + 1$;
14.	end
15.	end
16.	Scramble cipher keyframe channels *(scramble I_R, I_G and I_B)*

respectively, encrypted color channel of keyframe image histogram is F, G, H, N, O and P. Where a color keyframe image is encrypted, it's all the three channels (red I_R, green I_G and blue I_B) are encrypted separately. As it can be observed, there are patterns in the four keyframe images and one test image, but CTC-IES can encrypt these to be uniformly distribution cipher images. Intruders or attackers have difficulty accessing the original keyframe image information from their uniformly distribution of the pixels. Therefore, the proposed CTC-IES can recover the original keyframe images completely from the subsequent cipher images because each step is fully reversible.

There is a robust encryption efficiency in a keyframe CTC-IES algorithm because it is used a fast speed of execution, minimum computational complexity in the bitwise XOR operation and block scrambling method. Thus, a fast encryption rate can be achieved by the CTC-IES approach. Table 5 addresses the time taken to encrypt an image or keyframe, different test images and comparison with other encryption algorithms with the different sizes. The experimental encryption works (cryptosystem) are conducted on the platform such as follows: Intel(R) Core (TM) i5-6500 CPU 3.20 GHz with 8 GB of memory (RAM), Windows 10 OS. It can be demonstrated that the proposed CTC-IES exhibits faster keyframe encryption in terms of speed comparison to the other image encryption algorithms for different sizes of the image which is illustrated on the Table 5.

It also requires a keyframe image encryption algorithm to produce high-quality, decrypted images. A significant variance of a pixel in the keyframe image can affect all pixels in the encrypted cipher image in the CTC-IES encryption procedure, which can ensure high-security rates for the cipher images. However, a subtle variance of a pixel in the encrypted cipher-image can affect just some pixels of the decrypted outcome in the decryption procedure. In this circumstance, if a CTC-IES encrypted cipher image loses some data (information), the decryption method can also recover much of the original keyframe image's visual content. "Fig 9" demonstrates the quality of the image after decrypted when the CTC-IES cipher images suffer from any noise or dissimilar percentages of data loss. From "Fig 9" (A), it can be witnessed that the decryption method can completely recover the original keyframe image if the encrypted cipher image has no data loss. Even if the encrypted cipher images had already noise or lose some information, however, their decrypted outcomes comprise the most visual data from the original keyframe images, as can be seen from "Fig 9" (B) to (C). Thus, the implemented CTC-IES can easily decrypt high-quality of the encrypted cipher images.

V. SECURITY ANALYSIS

In order to demonstrate the CTC-IES' superiority, this section examines its level of security in the following aspects: such as computational complexity and speed test, information entropy analysis, resistance to differential attacks analysis, statistical attack analysis, secret key analysis and comparative analysis with existing surveillances schemes. To further illustrate the efficacy of CTC-IES, we compare this with the

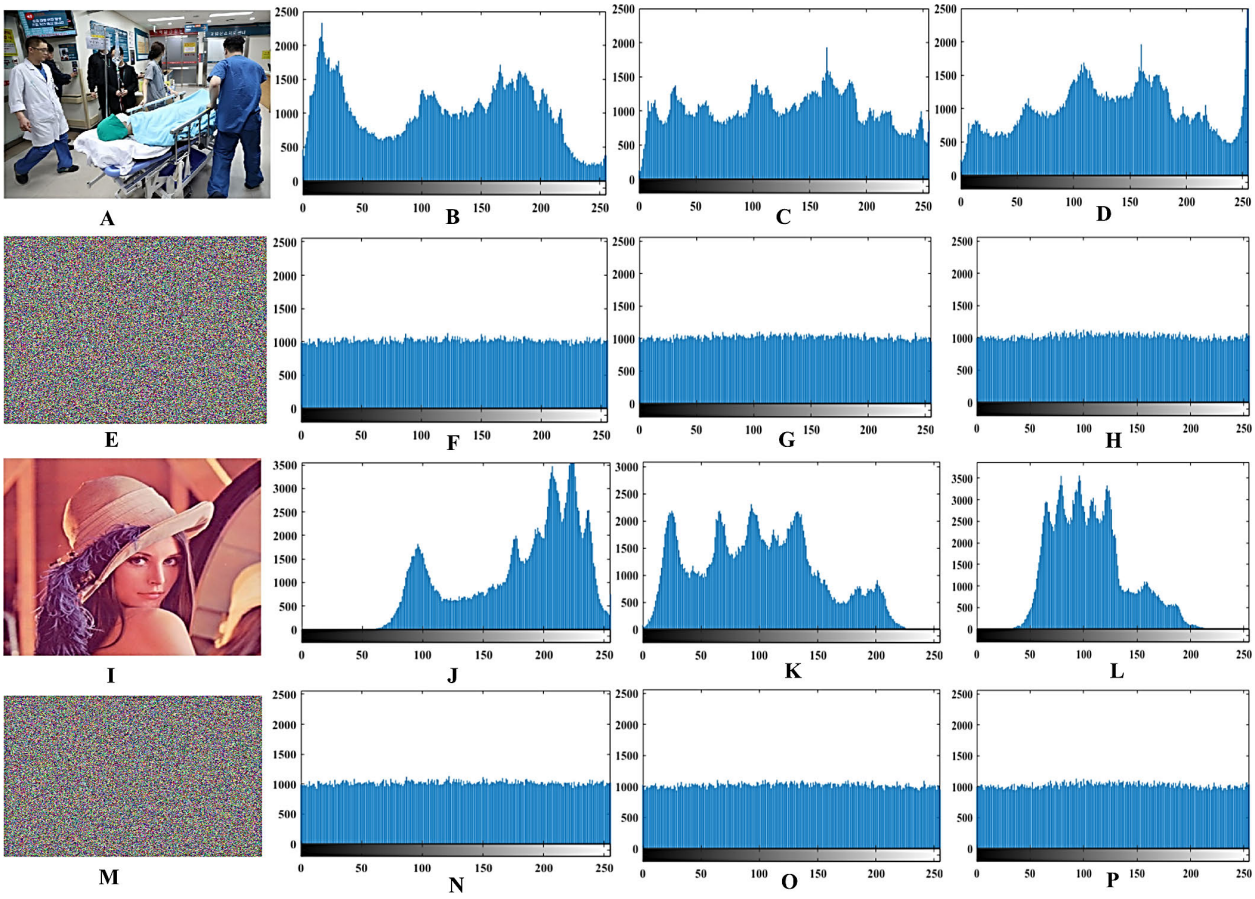


FIGURE 7. Simulation results of keyframe and test images of CTC-IES approach.

many other advanced methods of image encryption. We cited as a reference directly each finding reported by the author of the highly competitive encryption algorithms to perform a fair comparison.

A. COMPUTATIONAL COMPLEXITY AND SPEED TEST

This section introduces the computational complexity and speed of the projected cryptosystem as well as comparing the speed test with the other cryptosystems in the Table 5. The time-ingesting fragment of any chaotic map constructed encryption process is the combination of chaotic sequence generation, permutation, and diffusion procedures. Keeping in mind the smart healthcare IoT system, we emphasized to manage a low computational mechanism for producing fast communication speed by the adoption of the CTC-IES mechanism. In which generation of a sequence is very quick, processing of bitwise XOR and block scrambling with minimum computational time. We demonstrate average encryption time results for a set of the different size keyframes. The numerical value produced after encryption of the keyframes is shown in Table 5 and compared with the earlier color image encryption mechanism. This scheme's runtime is fast, attempting to make it more appropriate for real-time applications, including such as secure smart healthcare IoT system. The proposed

TABLE 5. Encryption time complexity and comparison with other schemes.

Method	Encryption time of 256x256 images (Keyframes)	Encryption time of 512x512 images (Keyframes)	Encryption time of 1024x1024 images (Keyframes)
Proposed	0.1022-0.1452	0.2811-0.3119	1.2399-1.3454
[36]	0.080-0.082	0.327-0.333	NA
[11]	0.1616	0.6708	2.821
[30]	0.0949	0.4010	1.9857
[33]	0.6212	NA	NA
[27]	1.28	NA	NA
[45]	0.3340	1.3357	5.3223
[46]	0.224	0.9731	3.8377

CTC-IES takes minimum computational tasks and less time to encrypt keyframes images compare to other color image encryption methods like [11], [27], [30], [33], [36], [45], [46].

B. INFORMATION ENTROPY ANALYSIS

Information entropy analyses the amount of uncertainty as well as the randomness behavior of the pixels in the cipher

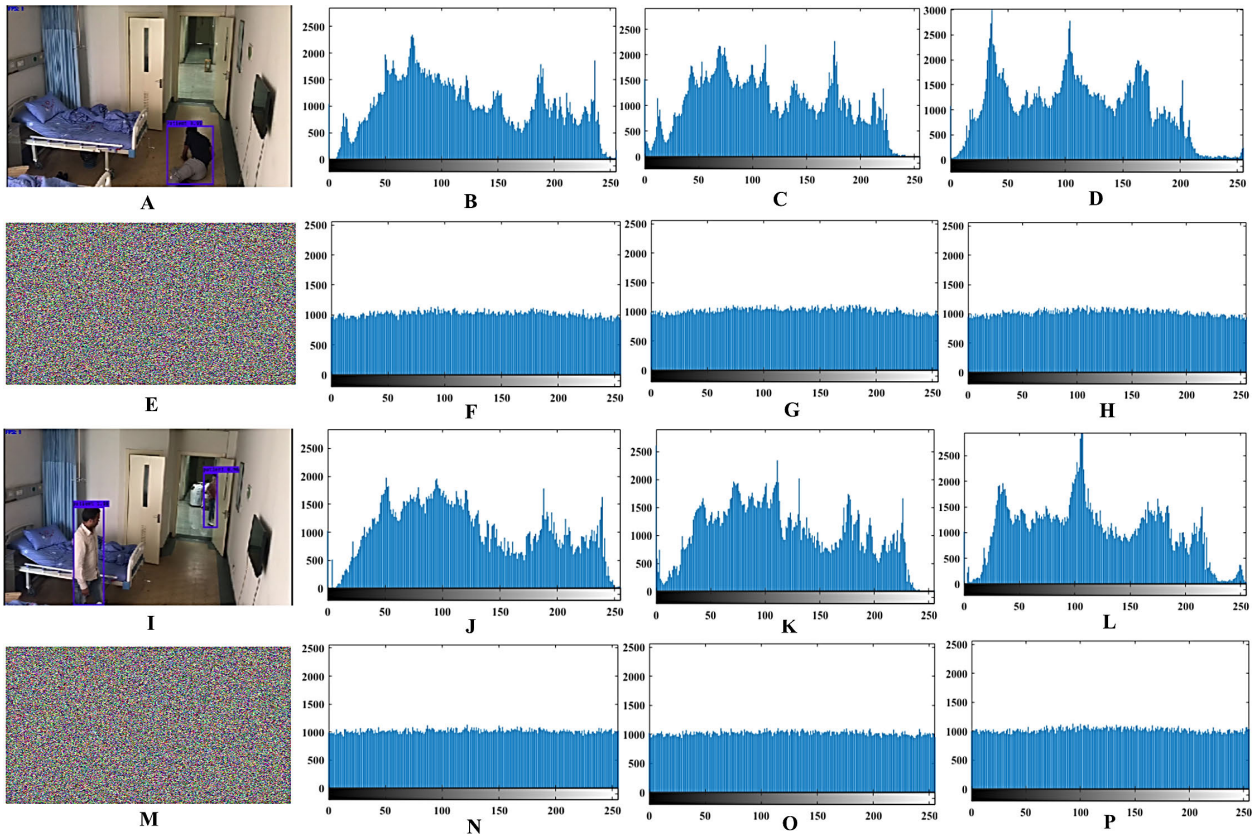


FIGURE 8. Simulation results of keyframe images of CTC-IES approach.

images. It has been explained as in the Eq. (6),

$$H(m) = -\sum_{i=1}^{255} P(m_i) \log_2 P(m_i) \tag{6}$$

where H(m) is the entropy, $P(m_i)$ is the determined probability of the occurrence at m_i. In general, the information entropy is 8 for any ideal random keyframe image. The probabilities of any of the symbol's m_i are identical in an ideal discrete image. Therefore, the probability within each symbol m_i is 1/256.

$$\begin{aligned} H(m) &= -\sum_{i=1}^{255} P(m_i) \log_2 P(m_i) \\ &= -\sum_{1}^{255} \frac{1}{256} \log_2 \frac{1}{256} \\ &= -256 \times \frac{1}{256} \log_2 \frac{1}{2^8} \\ &= -\log_2 2^{-8} \\ &= -(-8) \log_2 2 \\ &= 8 \end{aligned}$$

The encrypted cipher image should continue to behave as an optimal random image after encryption. This means that an encrypted cipher image's information entropy value should be near to 8. The more it comes near to 8, the higher the pixel randomness, and the less information leakage into the smart healthcare IoT system. Table 6 illustrated the entropy analysis of individual color such as red (I_R), green (I_G) and blue (I_B) channels of extracted keyframe images using the proposed CTC-IES as well as some other referenced encryption schemes [11], [27], [28], [29], [32], [36] and [47]. From Table 6, we can determine that by using the proposed CTC-IES, the entropy results of each color channel (R, G, B) of keyframe encrypted images are very similar to 8. This demonstrates that the proposed CTC-IES is delivered the appropriate degree of security and randomness against the entropy attack which is most likely needed for any smart healthcare IoT system.

C. RESISTANCE TO DIFFERENTIAL ATTACK ANALYSIS

The differential attack is widely known as an effective security attack. The differential attack focuses on building a strong relationship between keyframe images and their subsequent encrypted cipher-images by observing how the variations in the keyframe images can affect encrypted cipher-images. If it maintains the diffusion feature, a keyframe image encryption scheme shows high efficiency in avoiding differential attacks.

The diffusion feature demonstrates that the cipher image could disperse a slight change throughout the plain image

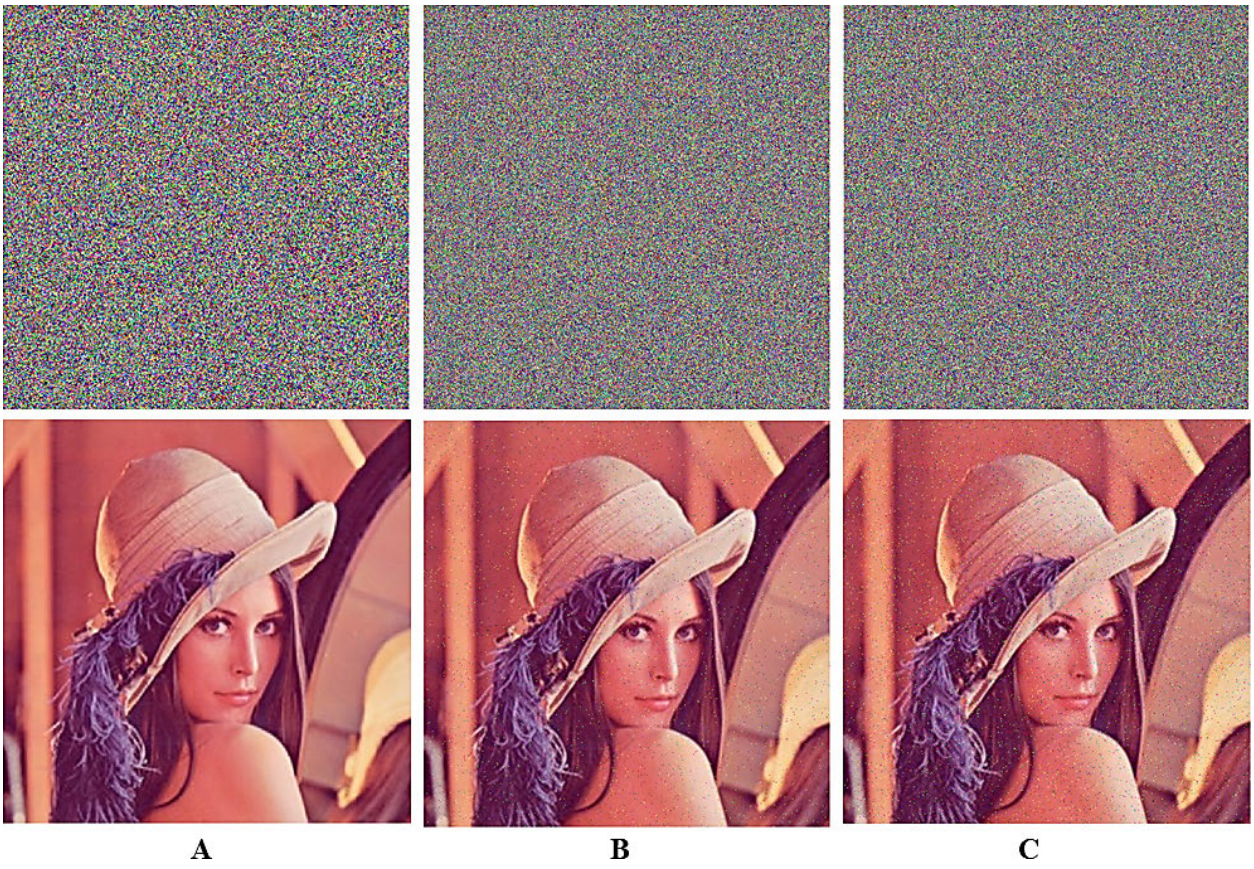


FIGURE 9. Decrypted image quality analysis: A) Encrypted and its decrypted image, B) 1%' salt & pepper' noise encrypted and decrypted image, C) 2%' salt & pepper' noise encrypted and decrypted image.

TABLE 6. Information entropy of keyframe encryption and comparison with other schemes.

Method	Images	Original Color Images			Encrypted Color Images		
		Red	Green	Blue	Red	Green	Blue
Proposed	Lena	7.2631	7.4940	6.9884	7.9980	7.9983	7.9991
	Optimize (Keyframe 1)	7.1582	7.2484	7.1348	7.9991	7.9981	7.9980
	P1 (Keyframe 2)	7.0966	7.1272	7.3605	7.9966	7.9919	7.9914
	P2 (Keyframe 3)	7.4591	7.2846	6.9962	7.9845	7.9810	7.9824
	P3 (Keyframe 4)	7.0818	6.7460	7.1210	7.9969	7.9919	7.9954
	P4 (Keyframe 5)	7.4521	7.3801	7.0091	7.9967	7.9921	7.9951
[11]	Keyframe3	7.7660	7.6599	7.7855	7.9975	7.9977	7.9979
[36]	Lena	7.2531	7.5940	6.9684	7.9994	7.9993	7.9993
[27]	Lena	7.2796	7.6321	6.9892	7.9973	7.9969	7.9971
[32]	Peppers	NA	NA	NA	7.9989	7.9991	7.9989
[28]	Lena	7.2775	7.5869	7.0133	7.9993	7.9994	7.9993
[29]	Boy	NA	NA	NA	7.9981	7.9983	7.9988
[47]	Lena	NA	NA	NA	7.9970	7.9972	7.9970

over the whole information or data. ''Fig 7 and 8'' are illustrated the innovative diffusion of the CTC-IES.

The two metrics NPCR (Number of Pixel Change Rate) and UACI (Uniform Average Change Intensity) by which can examine how an image encryption scheme can withstand differential attacks [48]. The variety of different pixels is counted by the NPCR, even though the UACI determines the average pixel difference between the two images. If C_1 and C_2 are the two encrypted cipher images which have only one bit of difference in their keyframe images, then their NPCR,

TABLE 7. NPCR and UACI of keyframe encryption and comparison with other schemes.

Method	Images	NPCR of Color Images			UACI of Color Images		
		Red	Green	Blue	Red	Green	Blue
Proposed	Lena	99.6296	99.6174	99.6473	33.6027	33.4997	33.5516
	Optimize (Keyframe 1)	99.6273	99.6067	99.5914	33.368	33.3375	33.3449
	P1 (Keyframe 2)	99.6223	99.6071	99.5869	33.3316	33.2227	33.3957
	P2 (Keyframe 3)	99.6136	99.6136	99.5960	33.4406	33.3564	33.2764
	P3 (Keyframe 4)	99.6180	99.5987	99.6059	33.3962	33.4095	33.3788
	P4 (Keyframe 5)	99.6242	99.6156	99.6212	33.3212	33.3371	33.3201
[11]	Keyframe1	99.5881	99.6283	99.5999	33.3848	33.4955	33.4559
[27]	Lena	0.9960	0.9961	0.9961	0.3356	0.3345	0.3349
[32]	Peppers	99.8473	99.8387	99.8479	33.3297	33.3289	33.3378
[36]	Lena	99.6296	99.6174	99.6473	33.6027	33.4997	33.5516
[29]	Boy	99.6338	99.6094	99.5795	33.2918	33.6839	33.3533

as well as UACI values, can be determined with the help of equation (7), (8) and (9) as follows:

$$NPCR = \frac{\sum_{i,j} D(i,j)}{M \times N} \times 100\% \tag{7}$$

$$D(i,j) = \begin{cases} 0 & if\ C_1(i,j) = C_2(i,j) \\ 1 & if\ C_1(i,j) \neq C_2(i,j) \end{cases} \tag{8}$$

$$UACI = \frac{1}{M \times N}\left[\sum_{i,j} \frac{|C_1(i,j) - C_2(i,j)|}{255}\right] \times 100\% \tag{9}$$

where MxN is the size of the keyframe matrix, and D(i,j) is providing a calculation of pixel changing between the two encrypted cipher images. Table 7 illustrated the NPCR as well as UACI results of keyframe images using the proposed CTC-IES algorithm and compared it with earlier articles [11], [27], [29], [32] and [36]. We can see NPCR values are very close to 100, and UACI is the one-third of the hundreds. It is demonstrated that each encryption is purely different randomize images by which differential attack misses its effectiveness. This results also indicate that our proposed cryptosystem is competently secure and can ensure that, now the attacker is unable to get any information between the original keyframe and ciphered images to resist the differential attacks.

Testing the NPCR and UACI values for the examining randomness, suppose C_1 and C_2 are the two encrypted cipher images with MxN size. The hypothesis test of NPCR (C_1, C_2) with α-level consequence are as follows [48] in Eq.(10):

$$\begin{cases} H_0 : \text{NPCR}(C_1, C_2) = \mu_{NPCR} \\ H_1 : \text{NPCR}(C_1, C_2) < \mu_{NPCR} \end{cases} \tag{10}$$

It is assumed when $NPCR(C_1, C_2) < \mu_{NPCR}$, H_0 is rejected. Which is the essential value of the NPCR test. Alternatively, the H_0 test is approved. The critical value $NPCR^*_\alpha$ is explained as [48] in Eq. (11):

$$NPCR^*_\alpha = \mu_{NPCR} - \frac{\sigma_{NPCR}}{\Phi(\alpha)} = \left(F - \frac{\sqrt{\frac{F}{MN}}}{\Phi(\alpha)}\right) / (F+1) \tag{11}$$

where $\Phi(\alpha) = \frac{1}{\sqrt{2\pi}} \exp\left(-\frac{\alpha^2}{2}\right)$ is the Cumulative density function of SD (Standard Normal Distribution) N (0,1) and F is the gray level image which is studied in this paper as a value of 255.

$$\begin{cases} H_0 : \text{UACI}(C_1, C_2) = \mu_{UACI} \\ H_1 : \text{UACI}(C_1, C_2) < \mu_{UACI} \end{cases}$$

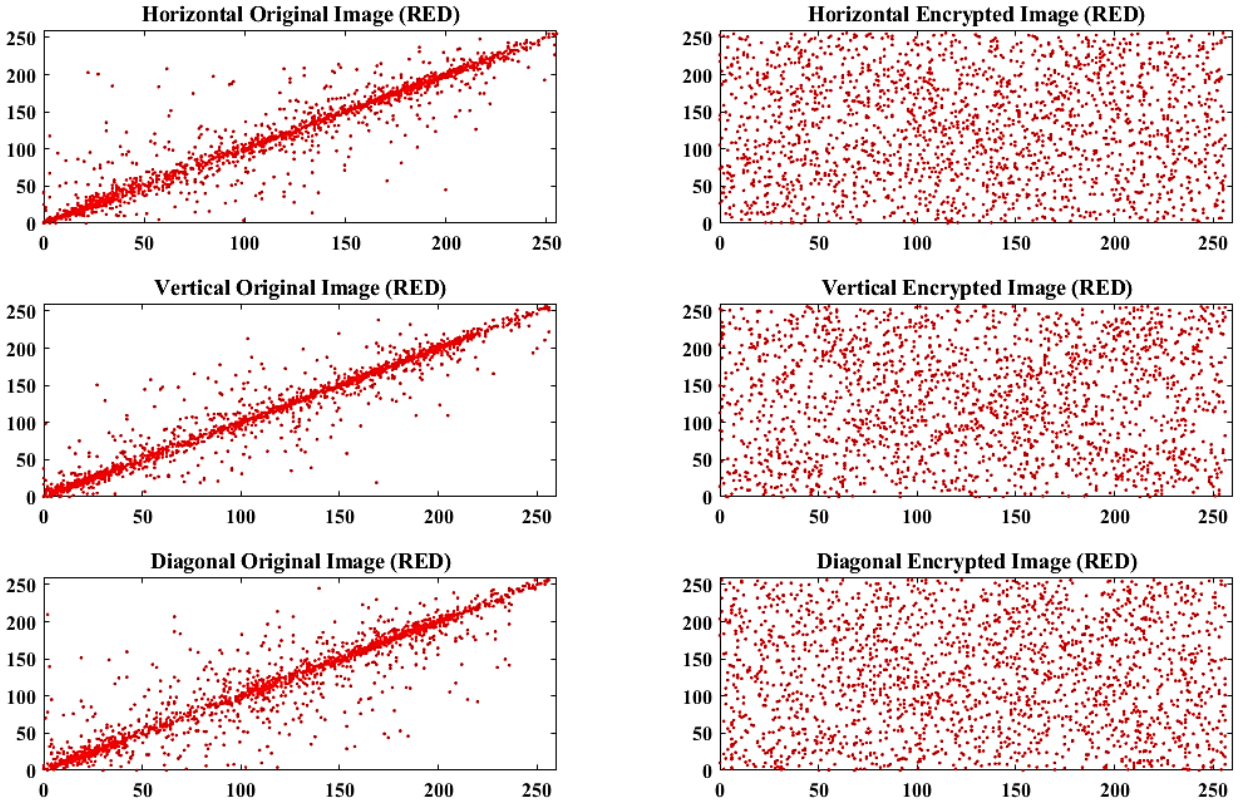


FIGURE 10. Distribution of two neighboring pixels (horizontally, vertically, and diagonally) in the plain keyframe and encrypted keyframe image (red component).

When UACI $(C_1, C_2) \notin \left(UACI_\alpha^{*-}, UACI_\alpha^{*+}\right)$, H_0 is rejected. Which is the essential value of the NPCR test. Alternatively, the H_0 test is approved [49]. The critical value of $UACI_\alpha^{*-}$ and $UACI_\alpha^{*+}$ are explained as [48] in Eq. (12-15):

$$UACI_\alpha^{*-} = \mu_{UACI} - \frac{\sigma_{UACI}}{\Phi\left(\frac{\alpha}{2}\right)} \tag{12}$$

$$UACI_\alpha^{*+} = \mu_{UACI} + \frac{\sigma_{UACI}}{\Phi\left(\frac{\alpha}{2}\right)} \tag{13}$$

$$\mu_{UACI} = \frac{F+2}{3F+3} \tag{14}$$

$$\sigma_{UACI} = \sqrt{\frac{(F+2)\left(F^2+F+3\right)}{18\,(F+1)^2\,MNF}} \tag{15}$$

Tables 8 and 9, respectively, displayed the NPCR and UACI test results level $\alpha = 0.05$.

TABLE 8. NPCR random test.

Algorithm	Image Size	NPCR	$NPCR_{0.05}$	NPCR Test
Proposed CTC-IES	512X512	99.6084	99.5816	Pass

TABLE 9. UACI random test.

Algorithm	Image Size	UACI	$UACI_{0.05}^{*-}$	$UACI_{0.05}^{*+}$	UACI Test
Proposed CTC-IES	512X512	33.3397	33.2018	33.4891	Pass

D. STATISTICAL ATTACK ANALYSIS

1) HISTOGRAM ANALYSIS

The histogram is a type of representation of a graph that is showing the pixel value distribution in any of the keyframe images. Encrypted keyframe image histograms must have a uniform pattern of pixel values and are completely different from the original keyframe images histograms [29], [36]. "Fig 7 and 8" each subsection A to P displays the histograms of the original, encrypted and decrypted keyframe image in red I_R, green I_G, and blue I_B components. In the results, we noticed that the encrypted results of the keyframe or Lena image histogram differ from the original results of the keyframe or Lena image histogram. In these encrypted images, we also noted that the uniformity of the values. The uniformity of the histogram can be measured numerically by the calculation of a variance. The lower variance means higher uniformity and higher variance means lover uniformity. It can be mathematically calculated by the Eq. (16): where n is the grayscale value, x_i and x_j are the pixels

$$\text{variance}\,(x) = \frac{1}{n^2}\sum_{i=1}^{n}\sum_{j=1}^{n}\frac{\left(x_i - x_j\right)^2}{2} \tag{16}$$

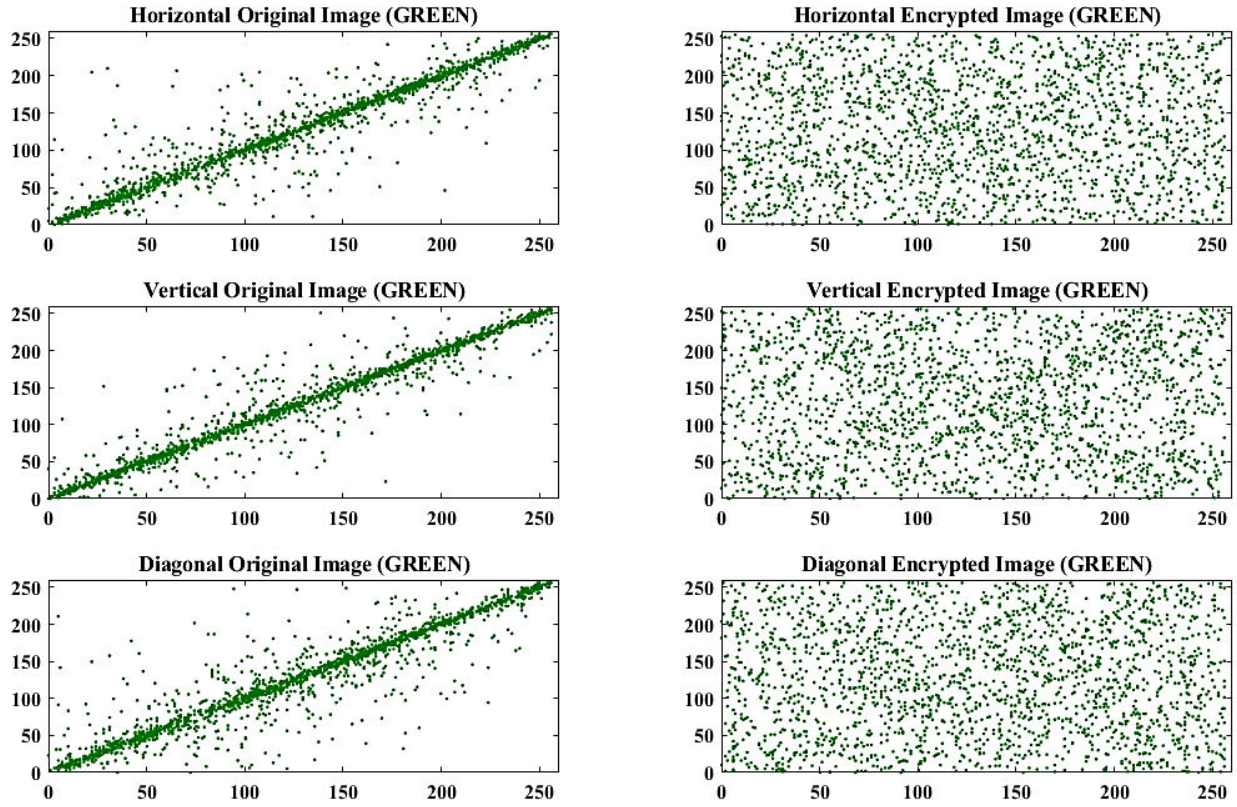


FIGURE 11. Distribution of two neighboring pixels (horizontally, vertically, and diagonally) in the plain keyframe and encrypted keyframe image (green component).

values of i^{th}, j^{th} gray scale [36], [50], [51]. Therefore, even if the attacker decrypts a certain section, it will still be problematic to decrypt the entire data. Similarly, the observation of original as well as an encrypted histogram of each red I_R, green I_G, and blue I_B component remains the same which is indicating that no information loss occurs during the transmission. The histogram analysis thus demonstrates that the proposed CTC-IES algorithm avoids the numerical or statistical attacks and thereby confirmations consistency, integrity in the communication.

2) CORRELATION ANALYSIS

The coefficient of correlation measures the sum of linear correlation in the images between the two adjacent pixels. In realistic images, there is a high correlation among the horizontal, diagonal and vertical directions between the pixels and their neighboring pixels. The purpose of the CTC-IES algorithm is to smash the correlation among the neighboring pixels along with horizontal, diagonal and vertical directions so that the keyframe image is reached around zero correlation with maximum unpredictability and randomness [29], [52]. The following Eq. (17-22) for calculating the correlation coefficient CC_{xy} between the two neighboring pixels are as follows:

$$CC_{xy} = \frac{\text{Covariance}\,(x, y)}{\sqrt{D\,(x)\,D\,(y)}} \tag{17}$$

$$\text{Covariance}\,(x, y) = \frac{1}{N}\sum_{i=1}^{N}\left(x_i - E\,(x)\right)\left(y_i - E\,(y)\right) \tag{18}$$

$$D\,(x) = \frac{1}{N}\sum_{i=1}^{N}\left(x_i - E\,(x)\right)^2 \tag{19}$$

$$D\,(y) = \frac{1}{N}\sum_{i=1}^{N}\left(y_i - E\,(y)\right)^2 \tag{20}$$

$$E\,(x) = \frac{1}{N}\sum_{i=1}^{N} x_i \tag{21}$$

$$E\,(y) = \frac{1}{N}\sum_{i=1}^{N} y_i \tag{22}$$

The value of the coefficient of correlation is between -1 and 1. Case 1: If it is bigger than 0, it reveals a positive correlation, Case 2: if it is lower than 0, it reveals negative correlation, Case 3: and when it is equivalent to 0, it reveals no correlation and non-correlation between neighboring pixels [29], [36] and [53]. For an original keyframe image, the correlation coefficient (CC) values come across to -1 or $+1$, but for the best result of encryption algorithms, to resist statistical effects, the value of the correlation coefficient should be nearly zero for encrypted images [36]. In this report, approx.

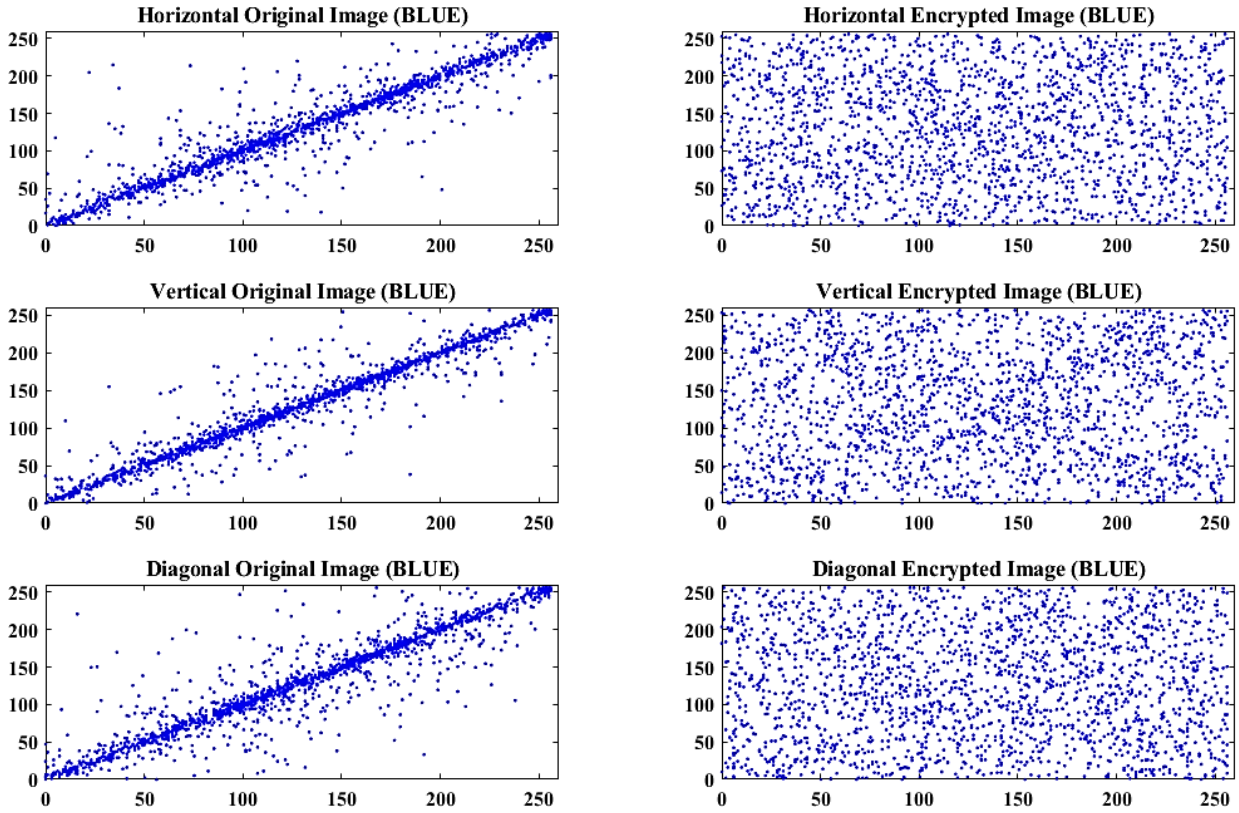


FIGURE 12. Distribution of two neighboring pixels (horizontally, vertically, and diagonally) in the plain keyframe and encrypted keyframe image (blue component).

Ten thousand sets of two neighboring pixels are selected randomly through vertical, horizontal, and diagonal angles to calculate the coefficient of correlation of two neighboring pixels. Table 8 displays the correlation coefficient outcomes of keyframe images using the proposed CTC-IES, as well as compared with earlier articles correlation coefficient results like [11], [27], [32], [36], [54] and [55]. The findings of Table 10 demonstrate that the coefficient of correlation of two neighboring pixels of original keyframe images in vertical, horizontal, and diagonal directions is almost equal to 1. However, the coefficient of correlation of two neighboring pixels of encrypted images in all three directions is approximately 0 (zero). The results of the analysis in Table 10 and "Fig10-12" are also showing the highest quality of breaking the correlation connection among the neighboring pixels in the original keyframe images by the using proposed CTC-IES than the other schemes and its compared with other encrypted methods such as [11], [27], [32], [36], [54] and [55]. We noticed in the "Fig 10-12" that the neighboring pixels in the original keyframe images are strongly (highly) correlated in vertical, horizontal, and diagonal directions, whereas the neighboring pixels are correlated weekly in the all three directions in the encrypted keyframe images. This demonstrates that the proposed CTC-IES is highly resistant to a statistical attack in the smart healthcare IoT ecosystem.

E. SECRET KEY ANALYSIS

The key size should be appropriate for any cryptographic algorithm. The CTC-IES key space is 2^{256}, which meets the key performance necessities and it is highly effective in avoiding different types of security attacks [30], [43], [56]. Moreover, including its secret key, the proposed algorithm should be highly sensitive by seeing the key structure in the "Fig 5". Otherwise, inaccurate secret keys with minute differences can also decrypt the original keyframe image information correctly, which can make the entire crucial key space smaller than those of the theoretical one [30], [43], [56]. Table 11 compares with the relative key space from different methods such as [11], [27], [32], [57], [58] and [59] with our proposed scheme. It shows that proposed CTC-IES provides comparatively better range of key space to generate complex chaotic behavior, therefore, CTC-IES has sufficient key space to avoid all types of brute force attacks in the smart healthcare IoT ecosystem.

TABLE 10. CC of two adjacent pixels, original, encrypted and comparison with other schemes.

Method	Images		Original Color Images			Encrypted Color Images		
			H	V	D	H	V	D
Proposed	Lena	R	0.9885	0.9953	0.9824	-0.0030	1.8172e-04	-5.213e-04
		G	0.9870	0.9920	0.9810	0.0021	-0.0030	-0.0019
		B	0.9875	0.9940	0.9818	-0.0011	-0.0012	-0.0028
	Optimize (Keyframe 1)	R	0.9631	0.9763	0.9429	0.0026	4.0123e-04	-0.0031
		G	0.9645	0.9780	0.9430	0.0031	6.1964e-04	0.0015
		B	0.9625	0.9750	0.9425	0.0015	4.6385e-04	7.3577e-04
	P1 (Keyframe 2)	R	0.9579	0.9906	0.9510	0.0027	-0.0013	0.0034
		G	0.9560	0.9916	0.9520	-3.3575e-05	-0.0027	9.5037e-04
		B	0.9570	0.9910	0.9508	-0.0012	-0.0025	0.0025
	P2 (Keyframe 3)	R	0.9552	0.9924	0.9495	-8.4643e-05	-0.0013	0.0030
		G	0.9540	0.9915	0.9470	2.5539e-05	-0.0016	9.6791e-04
		B	0.9535	0.9910	0.9460	4.6623e-05	-9.5287e-04	0.0025
	P3 (Keyframe 4)	R	0.9575	0.9933	0.9523	0.0015	-0.0010	0.0047
		G	0.9560	0.9910	0.9500	0.0012	7.5183e-04	0.0020
		B	0.9550	0.9885	0.9490	-8.3211e-04	-0.0020	0.0036
	P4 (Keyframe 5)	R	0.9493	0.9880	0.9384	0.0051	-0.0033	0.0015
		G	0.9470	0.9789	0.9280	0.0015	-0.0018	-0.0016
		B	0.9410	0.9800	0.9301	0.0017	-0.0044	0.0011
[11]	Keyframe1	R	0.9716	0.8707	0.8569	0.0035	0.0055	8.034e−04
		G	0.9660	0.8459	0.8288	−0.0026	−0.0044	0.0016
		B	0.9663	0.8464	0.8292	0.0025	−3.594e−04	0.0034
[54]	Keyframe	R	0.9937	0.9901	0.9854	0.0012	−0.0027	0.0002
		G	0.9909	0.9834	0.9877	−0.0007	0.0021	−0.0010
		B	0.9931	0.9824	0.9901	0.0015	−0.0010	0.0007
[27]	Lena		0.9603	0.9325	0.9084	−0.0027	0.0033	−0.0035
[32]	Peppers		NA	NA	NA	−0.0011	0.0013	0.0015
[36]	Lena		0.9778	0.9886	0.9695	0.0031	0.0005	−0.0041
[55]			0.9705	0.9927	0.9768	−0.0074	0.0032	−0.0121

TABLE 11. Key space comparison.

Algorithm	CTC-IES	[11]	[27]	[32]	[57]	[58]	[59]
Key space	2^{256}	10^{90}	3.9402×10^{185}	10^{168}	2^{128}	2^{100}	2^{128}

F. COMPARATIVE ANLYSIS WITH EXISTING SURVEILANCE SCHEMES

In this section, we are going to compare our proposed approach with earlier existing secure surveillance and image encryption schemes in the Table 12. Table 12 is demonstrated each and every key aspect of the surveillance as well as encryption scheme which is more comparable to measure robustness and secure parameter such as key space, speed, entropy, correlation coefficient NPCR and UACI values of the mechanism. The finding of the proposed approach is quite satisfactory and ideal values as illustrated by Table 12. In which our proposed method has gaining impetus in each mentioned area. We compared with other methods such as [11], [31], [23] and [24]. Each method has proposed good values and tried to cover confidentiality of the secure parameter of the image encryption. Although we compared relatively our results with various collection of images using different platforms and background functionality with many measured factors. Our proposed approach has fast speed in execution, comparable better entropy, lowest correlation coefficient, acceptable NPCR and UACI values. Which is firmly indicated that proposed work has highly acceptable

TABLE 12. Comparative analysis with existing surveillance schemes.

Algorithm	Image size	Key space	Speed	Entropy	CC_{xy}	NPCR	UACI
CTC-IES	512x512 [3]	2^{256}	0.2811-0.3119	7.9991	0.0015	99.6212	33.4406
[11]	512x512 [3]	10^{90}	0.6708	7.9998	0.0035	99.6125	33.4451
[31]	640x480 [3]	2^{372}	0.95/0.96	7.9994	0.0021	99.609	33.465
[23]	1024x1024 [3]	2^{300}	NA	7.91	0.003	99.5826	33.4213
[24]	Keyframe 0065	2^{711}	2.58	7.9998	0.0019	99.609	33.450

in the field of cryptographically secure surveillance on smart healthcare IoT ecosystem.

VI. CONCLUSION AND FUTURE WORK

IoT ecosystem is widely interconnected with medical healthcare system to provide best possible services including security and privacy of the patients. This paper is originally based on security and privacy issues into the IoT enabled smart healthcare system. Because of recent developments in IoT aided network we implemented a novel secure surveillance mechanism and probabilistic lightweight keyframes image encryption to provide security and privacy from any adversary. Keeping this in mind, this paper is firstly proposed, an efficient keyframe extraction mechanism from visual sensors by employing lightweight YOLOv3 algorithm. YOLOv3 algorithm is generated keyframes successfully and efficiently incorporated for testing with the large collection-oriented Face Database. The optimum result is received as an average accuracy of the keyframe extraction model which is 88-90% with 1-16 FPS (file per second). After completing keyframe extraction model, secondly proposed efficient probabilistic and lightweight keyframe image encryption. Cosine-transform-based chaotic sequence are used as a non-linear transform to generate and exhibit significantly complex new chaos behavior. Our fast keyframe image encryption are implied three rounds of diffusion-confusion operation. Bitwise XOR operation performed to encrypt in each channel of color images [I_R, I_G, I_B] separately with designed block scrambling to disperse adjacent-pixels into dissimilar positions rapidly in which keyframe images are ensuring adequately encrypted data as a cipher-image without recognizing actual keyframes in the smart healthcare system.

The various security analysis confirmed that the proposed mechanism has comparatively higher security aspect which is more likely competing with several other image encryption methods. It also demonstrates its success in minimizing bandwidth, space, transmission costs, and also diminishing the browsing timeframe of analysts coping with large quantities of surveillance information to make decisions on unusual incidents, such as any suspicious or normal activity detection and patients emergency suspicious action detection in the smart healthcare IoT system. This approach can be used for other similar real-time urgent response system such as fire detection, traffic control system, smart transportation system (STS), crime control detection in the smart city etc.

For future work, it can be carried out to integrate information from other systems, for many applications as well as further advance security aspect, access control, privacy measures in specific areas into the smart healthcare system. New direction can also be possible to implement dynamic secure key instead of implemented method for further enhancing security and privacy.

REFERENCES

[1] C. Stergiou, K. E. Psannis, B.-G. Kim, and B. Gupta, "Secure integration of IoT and cloud computing," *Future Gener. Comput. Syst.*, vol. 78, pp. 964–975, Jan. 2018.

[2] M. B. M. Noor and W. H. Hassan, "Current research on Internet of Things (IoT) security: A survey," *Comput. Netw.*, vol. 148, pp. 283–294, Jan. 2019.

[3] F. A. Teixeira, F. M. Pereira, H.-C. Wong, J. M. Nogueira, and L. B. Oliveira, "SIoT: Securing Internet of Things through distributed systems analysis," *Future Gener. Comput. Syst.*, vol. 92, pp. 1172–1186, Mar. 2019.

[4] M. Wazid, A. K. Das, R. Hussain, G. Succi, and J. J. P. C. Rodrigues, "Authentication in cloud-driven IoT-based big data environment: Survey and outlook," *J. Syst. Archit.*, vol. 97, pp. 185–196, Aug. 2019.

[5] A. M. Rahmani, T. N. Gia, B. Negash, A. Anzanpour, I. Azimi, M. Jiang, and P. Liljeberg, "Exploiting smart e-Health gateways at the edge of healthcare Internet-of-Things: A fog computing approach," *Future Gener. Comput. Syst.*, vol. 78, pp. 641–658, Jan. 2018.

[6] M. Gusev and S. Dustdar, "Going back to the roots—The evolution of edge computing, an IoT perspective," *IEEE Internet Comput.*, vol. 22, no. 2, pp. 5–15, Mar. 2018.

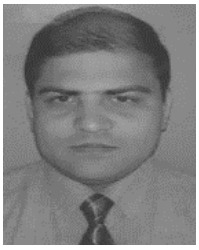
[7] L. Maglaras, L. Shu, A. Maglaras, J. Jiang, H. Janicke, D. Katsaros, and T. J. Cruz, "Editorial: Industrial Internet of Things (I2oT)," *Mobile Netw. Appl.*, vol. 23, no. 4, pp. 806–808, Aug. 2018.

[8] T. T. Allen, Z. Sui, and N. L. Parker, "Timely decision analysis enabled by efficient social media modeling," *Decis. Anal.*, vol. 14, no. 4, pp. 250–260, Dec. 2017.

[9] J. Khan, H. Abbas, and J. Al-Muhtadi, "Survey on mobile user's data privacy threats and defense mechanisms," *Procedia Comput. Sci.*, vol. 56, pp. 376–383, Jul. 2015.

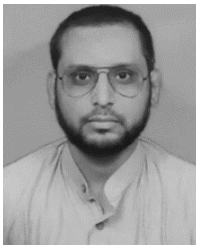
[10] D. Mishra, P. Vijayakumar, V. Sureshkumar, R. Amin, S. K. H. Islam, and P. Gope, "Efficient authentication protocol for secure multimedia communications in IoT-enabled wireless sensor networks," *Multimed. Tools Appl.*, vol. 77, no. 14, pp. 18295–18325, 2018.

[11] K. Muhammad, R. Hamza, J. Ahmad, J. Lloret, H. Wang, and S. W. Baik, "Secure surveillance framework for IoT systems using probabilistic image encryption," *IEEE Trans. Ind. Informat.*, vol. 14, no. 8, pp. 3679–3689, Aug. 2018.
[12] L. Da Xu, W. He, and S. Li, "Internet of Things in industries: A survey," *IEEE Trans. Ind. Informat.*, vol. 10, no. 4, pp. 2233–2243, Nov. 2014.
[13] R. Borawake-Satao and R. Prasad, "Mobility aware multi-objective routing in wireless multimedia sensor network," *Multimed Tools Appl.*, vol. 78, no. 23, pp. 32659–32677, Dec. 2019.
[14] M. Sajjad, I. Mehmood, and S. Baik, "Sparse representations-based super-resolution of key-frames extracted from frames-sequences generated by a visual sensor network," *Sensors*, vol. 14, no. 2, pp. 3652–3674, Feb. 2014.
[15] Y. Sun, "Analysis for center deviation of circular target under perspective projection," *Eng. Comput.*, to be published.
[16] I. Mehmood, M. Sajjad, W. Ejaz, and S. W. Baik, "Saliency-directed prioritization of visual data in wireless surveillance networks," *Inf. Fusion*, vol. 24, pp. 16–30, Jul. 2015.
[17] Q. Wu, M. Tao, D. W. Kwan Ng, W. Chen, and R. Schober, "Energy-efficient resource allocation for wireless powered communication networks," *IEEE Trans. Wireless Commun.*, vol. 15, no. 3, pp. 2312–2327, Mar. 2016.
[18] J. Ding, L. Jiang, and C. He, "User-centric energy-efficient resource management for time switching wireless powered communications," *IEEE Commun. Lett.*, vol. 22, no. 1, pp. 165–168, Jan. 2018.
[19] Z. Ji, Y. Zhang, Y. Pang, and X. Li, "Hypergraph dominant set based multi-video summarization," *Signal Process.*, vol. 148, pp. 114–123, Jul. 2018.
[20] Z. Ji, Y. Zhang, Y. Pang, X. Li, and J. Pan, "Multi-video summarization with query-dependent weighted archetypal analysis," *Neurocomputing*, vol. 332, pp. 406–416, Mar. 2019.
[21] M. Fei, W. Jiang, and W. Mao, "Memorable and rich video summarization," *J. Vis. Commun. Image Represent.*, vol. 42, pp. 207–217, Jan. 2017.
[22] X. Song, L. Sun, J. Lei, D. Tao, G. Yuan, and M. Song, "Event-based large scale surveillance video summarization," *Neurocomputing*, vol. 187, pp. 66–74, Apr. 2016.
[23] R. Hamza, A. Hassan, T. Huang, L. Ke, and H. Yan, "An efficient cryptosystem for video surveillance in the Internet of Things environment," *Complexity*, vol. 2019, pp. 1–11, Dec. 2019.
[24] R. Hamza, K. Muhammad, Z. Lv, and F. Titouna, "Secure video summarization framework for personalized wireless capsule endoscopy," *Pervasive Mobile Comput.*, vol. 41, pp. 436–450, Oct. 2017.
[25] L. Li, G. Wen, Z. Wang, and Y. Yang, "Efficient and secure image communication system based on compressed sensing for IoT monitoring applications," *IEEE Trans. Multimedia*, vol. 22, no. 1, pp. 82–95, Jan. 2020.
[26] L. Huang, S. Cai, X. Xiong, and M. Xiao, "On symmetric color image encryption system with permutation-diffusion simultaneous operation," *Opt. Lasers Eng.*, vol. 115, pp. 7–20, Apr. 2019.
[27] X. Chai, X. Fu, Z. Gan, Y. Lu, and Y. Chen, "A color image cryptosystem based on dynamic DNA encryption and chaos," *Signal Process.*, vol. 155, pp. 44–62, Feb. 2019.
[28] X.-Y. Wang and Z.-M. Li, "A color image encryption algorithm based on Hopfield chaotic neural network," *Opt. Lasers Eng.*, vol. 115, pp. 107–118, Apr. 2019.
[29] A. Broumandnia,"The 3D modular chaotic map to digital color image encryption," *Future Generation Comput. Syst.*, vol. 99, pp. 489–499, Oct. 2019.
[30] Z. Hua, Y. Zhou, and H. Huang, "Cosine-transform-based chaotic system for image encryption," *Inf. Sci.*, vol. 480, pp. 403–419, Apr. 2019.
[31] R. Hamza, Z. Yan, K. Muhammad, P. Bellavista, and F. Titouna, "A privacy-preserving cryptosystem for IoT E-healthcare," *Inf. Sci.*, to be published.
[32] M. Y. Valandar, M. J. Barani, and P. Ayubi, "A fast color image encryption technique based on three dimensional chaotic map," *Optik*, vol. 193, Sep. 2019, Art. no. 162921.
[33] M. Alawida, A. Samsudin, J. S. Teh, and R. S. Alkhawaldeh, "A new hybrid digital chaotic system with applications in image encryption," *Signal Process.*, vol. 160, pp. 45–58, Jul. 2019.
[34] M. Asgari-Chenaghlu, M.-A. Balafar, and M.-R. Feizi-Derakhshi, "A novel image encryption algorithm based on polynomial combination of chaotic maps and dynamic function generation," *Signal Process.*, vol. 157, pp. 1–13, Apr. 2019.
[35] B. Mondal, S. Singh, and P. Kumar, "A secure image encryption scheme based on cellular automata and chaotic skew tent map," *J. Inf. Secur. Appl.*, vol. 45, pp. 117–130, Apr. 2019.
[36] K. A. K. Patro and B. Acharya, "An efficient colour image encryption scheme based on 1-D chaotic maps," *J. Inf. Secur. Appl.*, vol. 46, pp. 23–41, Jun. 2019.
[37] L. Gong, K. Qiu, C. Deng, and N. Zhou, "An image compression and encryption algorithm based on chaotic system and compressive sensing," *Opt. Laser Technol.*, vol. 115, pp. 257–267, Jul. 2019.
[38] J. Wu, B. Cheng, M. Wang, and J. Chen, "Energy-aware concurrent multipath transfer for real-time video streaming over heterogeneous wireless networks," *IEEE Trans. Circuits Syst. Video Technol.*, vol. 28, no. 8, pp. 2007–2023, Aug. 2018.
[39] J. Redmon and A. Farhadi, "YOLOv3: An incremental improvement," Comput. Vis. Pattern Recognit., Cornell Univ., Ithaca, NY, USA, Tech. Rep. 1804.02767, 2018.
[40] J. Redmon. (2016). *Darknet Open Source Neural Network Framework*. Accessed: Sep. 18, 2019. [Online]. Available: https://github.com/pjreddie/darknet
[41] Tzu Chi University Hong Kong Multimedia Laboratory, Department of Information Engineering. Accessed: Sep. 18, 2019. *WIDER FACE: A Face Detection Benchmark*. [Online]. Available: http://shuoyang1213.me/WIDERFACE/
[42] K. Delac and M. Grgic. *Face Recognition Homepage*. Accessed: Sep. 18, 2019. [Online]. Available: http://www.face-rec.org/databases/
[43] G. Alvarez and S. Li, "Some basic cryptographic requirements for chaos-based cryptosystems," *Int. J. Bifurcation Chaos*, vol. 16, no. 8, pp. 2129–2151, Aug. 2006.
[44] Digital Test Image. *USC-SIPI Image Database for Research in Image Processing, Image Analysis, and Machine Vision*. Accessed: Sep. 19, 2017. [Online]. Available: http://sipi.usc.edu/database/
[45] P. Ping, F. Xu, Y. Mao, and Z. Wang, "Designing permutation-substitution image encryption networks with Henon map," *Neurocomputing*, vol. 283, pp. 53–63, Mar. 2018.
[46] A.-V. Diaconu, "Circular inter-intra pixels bit-level permutation and chaos-based image encryption," *Inf. Sci.*, vols. 355–356, pp. 314–327, Aug. 2016.
[47] R. Parvaz and M. Zarebnia, "A combination chaotic system and application in color image encryption," *Opt. Laser Technol.*, vol. 101, pp. 30–41, May 2018.
[48] Y. Wu, J. P. Noonan, and S. Agaian, "NPCR and UACI randomness tests for image encryption," *Cyber J., Multidisciplinary J. Sci. Technol., J. Sel. Areas Telecommun.*, pp. 31–38, 2011.
[49] T. T. Allen, Z. Sui, and K. Akbari, "Exploratory text data analysis for quality hypothesis generation," *Quality Eng.*, vol. 30, no. 4, pp. 701–712, Oct. 2018.
[50] X. Chai, Y. Chen, and L. Broyde, "A novel chaos-based image encryption algorithm using DNA sequence operations," *Opt. Lasers Eng.*, vol. 88, pp. 197–213, Jan. 2017.
[51] Z. Sui, "Social media text data visualization modeling: A timely topic score technique," *Amer. J. Manag. Sci. Eng.*, vol. 4, no. 3, p. 49, 2019.
[52] Y. Zhang, X. Wang, L. Liu, and J. Liu, "Fractional order spatiotemporal chaos with delay in spatial nonlinear coupling," *Int. J. Bifurcation Chaos*, vol. 28, no. 2, Feb. 2018, Art. no. 1850020.
[53] J. Zhang, D. Fang, and H. Ren, "Image encryption algorithm based on DNA encoding and chaotic maps," *Math. Probl. Eng.*, vol. 2014, pp. 1–10, Dec. 2014.
[54] R. Hamza, Z. Yan, K. Muhammad, P. Bellavista, and F. Titouna, "A privacy-preserving cryptosystem for IoT E-healthcare," *Inf. Sci.*, to be published.
[55] C.-L. Li, H.-M. Li, F.-D. Li, D.-Q. Wei, X.-B. Yang, and J. Zhang, "Multiple-image encryption by using robust chaotic map in wavelet transform domain," *Optik*, vol. 171, pp. 277–286, Oct. 2018.
[56] N. P. Smart. ECRYPT—CSA. *Algorithms, Key Size and Protocols Report (2018)*. Accessed: Oct. 18, 2019. [Online]. Available: http://www.ecrypt.eu.org/csa/documents/D5.4-FinalAlgKeySizeProt.pdf
[57] X. Chai, Z. Gan, K. Yang, Y. Chen, and X. Liu, "An image encryption algorithm based on the memristive hyperchaotic system, cellular automata and DNA sequence operations," *Signal Process., Image Commun.*, vol. 52, pp. 6–19, Mar. 2017.
[58] G. Ye and X. Huang, "An efficient symmetric image encryption algorithm based on an intertwining logistic map," *Neurocomputing*, vol. 251, pp. 45–53, Aug. 2017.
[59] A. Y. Niyat, M. H. Moattar, and M. N. Torshiz, "Color image encryption based on hybrid hyper-chaotic system and cellular automata," *Opt. Lasers Eng.*, vol. 90, pp. 225–237, Mar. 2017.



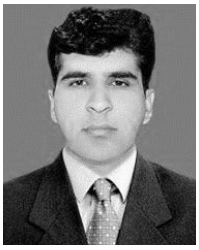
JALALUDDIN KHAN received the M.S. degree in computer science from Aligarh Muslim University Aligarh, India. He is currently pursuing the Ph.D. degree from the School of Computer Science and Engineering, University of Electronic Science and Technology of China (UESTC) Chengdu China. He has an impressive academic, research, and professional experience from Kingdom of Saudi Arabia. He was a Lecturer in Deanship of Skills Development and a Researcher with the Center of Excellence in Information Assurance (COEIA), King Saud University, Riyadh, Saudi Arabia. His research areas include the IoT, security and privacy, E-Health and telemedicine, machine learning, and medical big data concerned technologies. He is currently focusing the IoT security with medical data. He has authored some research articles. He is accompanying with the Wavelets Active Media Technology and Big Data Lab under supervision with Prof. J. P. Li and with a collaborated way with other researchers in UESTC.

JIAN PING LI is currently a Chairman of the Computer Science and Engineering College and Model Software College, University of Electronic Science and Technology, China. He is also the Director of the International Centre for Wavelet Analysis and its Applications. He is a National Science and Technology Award Evaluation Committee, National Natural Science Foundation Committee of Chin, The Ministry of Public Security of the People's Republic of China such as technical adviser and a dozen academic and social positions. He is the Chief Editor of International Progress on Wavelet Active Media Technology and Information Processing. He is also an Associate Editor of *International Journal of Wavelet Multimedia* and *Information Processing*.



BILAL AHAMAD received the master's degree in computer science from Jamia Hamdard University, New Delhi, India, in 2008. He is currently a Lecturer with the Department of Computer Science, College of Computing and Information Technology, Shaqra University, Saudi Arabia. He has an extra ordinary academic, research, and professional experience in Computer Science and Software Programming. His research interests include information security, software security, web application security data mining, machine learning, medical big data, and connected technologies.

SHADMA PARVEEN received the M.S. degree in e-commerce from Dr. Ram Manohar Lohia Awadh University, Faizabad. She is currently pursuing the Ph.D. degree from the School of Management and Economics, University of Electronic Science and Technology of China (UESTC), Chengdu, China. She has a vast Academic, Technical, and Professional Experience in India. She is currently a Lecturer with the Ram Tirath Degree College, Siddartha University, Utraula Balrampur, India. She is also associated with the Wavelets Active Media Technology and Big Data Lab. She has authored some research articles. Her research areas include management science, economics, statistical analysis of e-waste, deep learning, machine learning, and the Internet of Things.



AMIN UL HAQ received the M.S. degree in computer science. He is currently pursuing the Ph.D. degree with the School of Computer Science and Engineering, University of Electronic Science and Technology of China, Chengdu, China. He has a vast academic, technical and professional experience in Pakistan. He is currently a Lecturer with Agricultural University, Peshawar, Pakistan. He is also associated with Wavelets Active Media Technology and Big Data. He has authored some research articles. His research areas include machine learning, medical big data, the IoT, E-health and telemedicine, concerned and technologies and algorithms.

GHUFRAN AHMAD KHAN received the M.S. degree in computer science from Aligarh Muslim University, Aligarh, India. He is currently pursuing the Ph.D. degree from the School of Information Science and Technology, Southwest Jiaotong University, Chengdu, China. He has huge Academic and Technical Experience in India. He has authored some research articles. His research areas include machine learning, data mining, rough set theory, and deep learning.

ARUN KUMAR SANGAIAH received the M.E. degree from Anna University and the Ph.D. degree from VIT University, Vellore, India. In 2016, he was a Visiting Professor with the School of Computer Engineering, Nanhai Dongruan Information Technology Institute, China, for 6 months. In addition, he has been appointed as a Visiting Professor with Southwest Jiaotong University, Chengdu; Changsha University of Science and Technology, China; Dongguan University of Technology, Guangdong; and Hwa-Hsia University of Technology, Taiwan. Further, he has visited many research Centers and Universities in China, Japan, Singapore and South Korea for join collaboration towards research projects and publications. He is currently a Professor with the School of Computing Science and Engineering, VIT University. His publications are distributed as follows: 200 articles indexed in ISI-JCR (Q1 :90, Q2:30, Q3 :40, Q4 :50) and 21 articles indexed in Scopus. In addition, he has authored/edited eight books (Elsevier, Springer, and others) and edited 50 special issues in reputed ISI journals, such as the *IEEE Communication Magazine*, the IEEE TII, the IEEE IoT, *ACM transaction on Intelligent Systems and Technology*, and so on. His areas of research interest include E-learning, machine learning, software engineering, computational intelligence, and the IoT. Dr. Sangaiah's outstanding scientific production spans more than 250 contributions published in high standard ISI journals, such as the *IEEE Communication Magazine*, the IEEE Systems, and IEEE IoT. He has also registered one Indian patent in the area of Computational Intelligence. His Google Scholar Citations reached 4000+ with H-index: 32 and i10-index: 125. His Google Scholar Citations reached 4500+ with H-index: 24 and i10-index: 69. He has received many Awards that includes, India-Top-10 researcher award, Chinese Academy of Science-PIFI overseas visiting scientist award, and so on. He is also responsible for Editorial Board Member and an Associate Editor of many reputed ISI journals.