Secure Smart Healthcare Monitoring in Industrial Internet of Things (IIoT) Ecosystem with Cosine Function Hybrid Chaotic Map Encryption

Jalaluddin Khan, Ghufran Ahmad Khan, Jian Ping Li, Mohamed Fahad AlAjmi, Amin Ul Haq, Shakir Khan, Naved Ahmad, Shadma Parveen, Mohammad Shahid, Sultan Ahmad, Mordecai Raji, Bilal Ahamad, Abdulrahman Abdullah Alghamdi, and Amjad Ali

1Department of Computer Science and Engineering, Koneru Lakshmaiah Education Foundation, Guntur, Andhra Pradesh 522502, India
2School of Computer Science and Engineering, University of Electronic Science and Technology of China, Chengdu 611731, China
3School of Information Science and Technology, Southwest Jiaotong University, Chengdu 611756, China
4Department of Pharmacognosy, College of Pharmacy, King Saud University, Riyadh 11451, Saudi Arabia
5College of Computer and Information Sciences, Imam Mohammad Ibn Saud Islamic University, Riyadh 11432, Saudi Arabia
6Head of Research Support Unit, AlMaarefa University, Riyadh 11597, Saudi Arabia
7School of Management and Economics, University of Electronic Science and Technology of China, Chengdu 611731, China
8Department of Computer Science and Information Engineering, National Taiwan University of Science and Technology, Taipei 10607, Taiwan
9Department of Computer Science, College of Computer Engineering and Sciences, Prince Sattam Bin Abdalaziz University, Alkharij 11942, Saudi Arabia
10College of Computing and Information Technology, Shaqra University, Shaqra 11961, Saudi Arabia
11Department of Computer Science and Software Technology, University of Swat, Saidu Sharif Swat 19200, Pakistan

Correspondence should be addressed to Jalaluddin Khan; jalal4amu@yahoo.com, Jian Ping Li; jpli2222@uestc.edu.cn, and Shadma Parveen; yourshadma@yahoo.com

Received 10 August 2020; Accepted 28 January 2022; Published 29 March 2022

Academic Editor: Habib Ullah Khan

The technological progression is raised as a hybrid ecosystem with the industrial Internet of Things (IIoT). Among them, healthcare is also broadly unified with the Internet of Things to develop an industrial forthcoming system. Utilizing this type of system can be facilitating optimum patient monitoring, competent diagnosis, intensive care, and including the appropriate operation against the existing critical diseases. Due to enormous data theft or privacy leakage, security, and privacy towards patient-based informative data, the preservation of personal patients’ informative data has now become a necessity in the digitized community. The produced article is underlined on handsomely monitoring, perceptively extracted keyframe, and further processed lightweight cosine functions using hybrid way chaotic map keyframe image encryption. Initially, a regular concept of extracted keyframe is deployed to salvage meaningful detected frames by transmitting an alert autonomously to the administration. Then, lightweight cosine function for encryption is employed. This encryption incorporates keyframe exceedingly secure and safe from the outside world or any adversary. Our proposed methodology validates effectiveness throughout the IIoT ecosystem. The produced outcome is highly acceptable and has minimum execution time, robustness, and reasonably adopted cost-effective, secure parameter than any other (keyframes) image encryption methods. Furthermore, this methodology has optimally reduced bandwidth, essential communicating price, transmission cost, storage, and immediately judicious analysis of each occurred activity from the outside world or any adversary to remain secure and confident about the real patient-based data in the smartly developed environment.
1. Introduction

Nowadays, the Internet of Things (IoT) has intensified its global omnipresence. The implementation of smart networks is supposed as an exposition of ubiquitous computing. The goal is to expand network edge enabling smart services with IoT system. These kinds of computing is the best way replacement of the upfront user intentness towards interconnected employed devices (sensor-enabled strategies). It deprived of human interaction and instigated industrial perspective such as industrial Internet of Things (IIoT) [1–8]. These applications are well-organized integral sensor-based IoT architecture which is behaving well-informed accosted systems, such as smart cities (SC), smart healthcare system (SHM), smart wireless-multimedia sensor network (SWMSN), smart homes (SH), remote monitoring on farm animals (RMFA), automobiles, drone monitoring system (DMS), smart industry surveillance system (SIS), agricultural crop monitoring system (ACMS), pain monitoring system (PMS), self-driving vehicles (SV), and smart transportation system (STS) [9–17]. These treasured research and innovation parturitions as a high processing skill set in terms of the intelligent operational IIoT ecology, which is well suited to meaningful communication through the environs.

WMMSN (wireless-multimedia surveillance networks) are among the top innovative contributor. It is an essential parameter towards IIoT empowered ecology that operates visual sensor data uniformly. It is also measuring all the possible views and nonstop capturing visual images. These laboring methodologies are generating enormous multimedia visuals with too much redundancy into the system [18–22]. Due to availability of huge redundant visuals into the intelligent system, it is observed consensus of the researchers that developed a mechanism which can process meaningful as well as informative visuals from the surveillance networks. Add the best way recorded for forthcoming usages. It is tracing behavior or activities (simple interaction or abnormal), diagnosis liveliness of the doctors, operation theater activities, patients handling ventures of the staff as well as nurses, and observing hygienic facilities in the whole industrial healthcare setup. The approaching mentioned problems. The optimum emphasis is to capture every probable abnormal activity detection by accurate analysis with well-organized supervision and video abstraction. The foremost motive behind this, transferring all the visuals through the communication medium before processing is not the best way because it contains more bandwidth as well as energies. Additionally, it is very hard (difficult) along with time-consuming to recognize and ingeniously extracted action-oriented intelligence from a high volume of surveillance visuals [23, 24].

Therefore, it is essential to employ a piece of machinery or methodology that can accumulate each valued visual information individually incorporating high processing skills set and communication capabilities of the smart-enabled IIoT sensors. The quality of these methodologies is intelligently selecting accurate views from any different locations or multiple views and smoothly captured. The closely informative pursuits or core-specific data in real-time with the sensors, as a result, accurately transfer that visual data to the expert witness. Additionally, the key importance is to take action from the specialist by the investigation of original gigantic enlightening visuals. Then, a conventional methodology including efficient monitoring (surveillance) is shown in Figure 1. The enhanced conceptual framework is apprehending each perilous movement for accurate recognition of any possible happened actions in a quite shrewdly and reporting immediate to enforce action promptly and reduces any miss happening into the entire system. This approach also provides healthier achievement regarding disciplined resource utilization and robustness, which is the essential requirement when monitoring smart healthcare systems with the (WMSNs) wireless multimedia sensor networks by proper investigation to resolve any technological, nature-based, and human malfunctioning defects [25, 26].

Concerning the tendency of visual transmission at wireless environments as a WMSN from start to endpoint, vice versa, these communications are coming in a vulnerable way with the enormous security threats. Consequently, it is highly recommended that the visual data in terms of keyframe image can be securely transferred to a base station with enhanced and secure guided way without any modification from any untrusted parties. Additionally, we are guessing that the utilized dedicated communication of visual data supposed to problems due to jammed (congested) spectrum allocation methods into WMSN medium. Furthermore, the unfolded report is an emphasis on solving mentioned problems by incorporating an intelligent and power-efficient system. That can easily handle in better way by gathering informative data or relevant information in real-time and prompt action taken against the happened events. By employing this, our methodology can be proficient in reducing the cost of the transmission as well as consumption of congested bandwidths. In addition, adapted methodology has the primary intent to enrich the security prototype, in which system is fully taking care, protecting WMSNs, and improving utilization towards concern authority. Technically proposed system engendered encrypted keyframe images when transferring extracted keyframes to concern authority for accomplishing high rate of security during entire communication inside the smart healthcare IIoT enabled setup.

Core enrichment of the designed report is registered as follows:

(I) We proposed an effective architectural adjustment to monitor healthcare smartly with IIoT via utilizing cosine as a function targeted encryption based on chaotic hybrid map.

(II) The methodology emphasizes first to extract the most relevant or meaningful keyframes from the summarized video data into the keyframe extraction model.
(III) After that, we incorporated a well-organized probabilistic as well as lightweight cosine function for encryption. This encryption approach is conquering strong security against any adversary.

(IV) The methodology is applied to hybrid technologies such as Python, TensorFlow, YOLOv3 for the extraction of keyframes, and cryptographic simulation done by MATLAB. The extracted keyframe evaluation and security analysis ensured that our methodology is proficient for reducing the cost of transmission as well as the efficiency of consumption bandwidth.

(V) The produced report endorses the commanding characteristics of the patient-based privacy in terms of an encrypted matrix to avoid any adversary outbreak.

(VI) The produced report also approved that the numerous rigorous security threads can withstand.

The rest of the article is summarized and pursues as follows: Section 2 has articulated preliminary work briefly about the smart healthcare system, monitoring and surveillance system, video summarization, and RGB image encryption. Section 3 has incorporated a novel planned monitoring (surveillance) tactic in which model extraction of keyframe from visual sensors is briefly discussed, and it describes implementation of lightweight cosine function hybrid chaotic map encryption methodology. Section 4 has investigated its experimental outcomes and relative discussion. Section 5 has briefly encountered numerous rigorous security examination with each possible security-based parameter. Section 6 is an efficiently concluding move toward entire work as well as a future direction.

2. Preliminary Work

Recent huge progressions in the territory of WMSNs are owned as a smart intelligence-based healthcare setup. It elevates finest incorporation at the hospital management with relating to patient privacy, security, and safety in the industrial perspective. Targeted mensuration about confidentiality, safety, and security, it is important to examine visual intelligence data and maternal encryption methodology. That can validate the genuineness of the system designed for complete patient protection or towards health safety. Although providing relief to human lives, the huge surveillance information poses the challenging task of spending time and energy while the footage is being picked up. Consequently, some methodology or approaches are required to facilitate as well as provide the most relevant data as a summaries video, including extraction of meaningful keyframe within that summaries video instead of viewing the whole surveillance visual data. The video summary received considerable study coverage over the past two decades. In a very concise way, it helps to abbreviate one long video or different images, such as video skimming as well as a static storyboard. Khan et al. reported on [27] an effective, co-evolutionary neural network-based summary procedure for
a resource-constrained system of the surveillance videos, in which the shot segmentation process is incorporated by utilizing deep features. That mechanism retains the interesting nature of the produced summary by utilizing image memorability as well as entropy properties. It also claimed that in each shot of the frame recorded highest score as a keyframe of the memorability as well as entropy. Hussein et al. [28] expressed his thought about MVS (multi-view video summarization), how it is challenging to accommodate gigantic volumes of data, light variation, redundancy, overlapping views as well as inter-view correlation as well. Their idea is to integrate MVS with a deep neural network as a two-tier method to adopt soft computing processes. Its first automated tier conducts segmentation of priority shots based on appearance and preserves them in a query table which is forwarded to all the cloud with further analysis. Its second tier captures deep properties from every frame of a series in the indexed table as well as transfers those to deep, long-term bidirectional memory to gain insightful odds and providing a summary.

Huang and Wang [29] explained the popularity of video summarization and its key point selection of the keyframes that can represent actual content as a video sequence. Their idea is to provide video summarization as well as motion of the video summarization. For achieving this, initially the capsule networks are accurately trained, such as extractor of spatiotemporal details, as well as focused on such spatiotemporal properties as an interframe movement curve is produced. A (TED) transition effect detection system is subsequently proposed to segment the video streams automatically into shots. At last, a self-attention framework is implemented for selecting keyframe sequences within videos. Therefore, selecting key static images as a summary of streaming content as well as measuring visual flows as a summary of video motion. Jie et al. [30] proposed an action-driven video synthesis paradigm focused on reinforcing learning. The framework is divided mainly into two sections: video cut through action parsing and video description focused on reinforcement learning. Within the first section, a chronological multi-instance learning framework is equipped using weekly interpreted data to crack the issue of the time-consuming maximum annotation as well as the uncertainty of the weak annotation. Throughout the second section, it built a deep recurrent video summarization model constructed on the neural network that selects the most recognizable frames compared with other behavior. In the meantime, the consistency of the mainframes extracted may be assessed by the correctness of the categorization. Yuan et al. [31] introduced a new (DSSE) deep side semantic embedding prototype to produce video summaries using the free side details. The DSSE establishes an implicit subspace through correlating the two unimodal autoencoders’ hidden layers. Respectively, that embedded the side information and video frames. Furthermore, by dynamically reducing the loss of semantic meaning and the loss of the two unimodal autoencoders in function reconstruction, the comparable general facts between side information and video frames can be more thoroughly understood. Hence, its semantic significance can be evaluated quite efficiently. Ultimately, semantically relevant portions are picked from videos by eliminating its lengths to the side details and the latent subspace is constructed.

The cryptographic encryption of the digital images can be extensively recognized into two major groups. One of them is color image encryption, and another one is grayscale image encryption. The encryption methodology of a grayscale image is only based on one plane. But it can be prolonged by incorporating different color planes like red, green, and blue to adopt completely color image encryption procedures. Digital security is a vital problem limiting IIoT applications as well as cyber-physical systems’ wider acceptance. In these regards, focusing various cryptographic concepts earlier, Wang et al. [32] expressed their methods to incorporate quantized logistic map-based stream encryption among the (WBAN) wireless body area networks. WBANs are committed to the transmission and processing of human-grown biomedical information. This encryption mechanism uses a chaotic method to execute the process for encryption. The assessment results demonstrate that the suggested encryption framework seems to have the advantages of success with high-security defense. Al-Khedhairi et al. [33] reported their hybrid cryptosystem for achieving three goals. One of which is to implement a new (2D) two-dimensional fractional-order map with very dynamic chaotic behavior as well as a unique true value of Lyapunov exponents across a wide variety of variables, particularly in comparison to other 2D maps. Secondly, for the first time, it is suggested a new robust, stable encryption system integrating the related chaotic pseudo-orbits of the suggested map with those of the benefits of elliptic curves through public-key cryptography while implemented to color images. At lastly, the hybrid structure is confident of verifying secure exchange of hidden keys as well as extremely obscure and concealing information communications. Zhang et al. [34] described an effective S-box, secure hash algorithm MD2, and fractional-order logistic map-based image encryption. Furthermore, the authors emphasize that the proposed algorithm is focused on a logistic fractional-order map which had benefits in their improved potential to withstand specific cryptanalyst attacks with reduced execution times. Huang et al. [35] articulated about the procedure for the color-based image encryption wherein permutation-diffusion happened concurrently. In addition, it is cooperating strangely among the color image matrixes. Accordingly, this approach is added security characteristics through high competence.

Almalkawi et al. [36] incorporated a lightweight image encryption method in which a hybrid kind of chaotic maps (logistic and henon) are used to encrypt the image matrix. His idea is to split digital images into blocks and effectively compress those blocks for reducing the size of the image matrix. After that they applied a logistic map for the creation of the key. The permutation and substitution operations are performed to attain shuffling and transportation of the image pixels. The henon chaotic map is implemented to adjust the pixel positions throughout the diffusion process to improve the necessary level of protection and to resist different security threats. Chai et al. [37] explained an RGB
image crypto-method founded on chaos as well as DNA oriented encryption. Firstly, his idea is to crumble color image as a red, green, blue channel. After that, intra-inter component permutation methods are reliant on a plain image which is functioned to scuffle them. Additionally, transformed and rejoined permuted classification in DNA matrix. Lastly, ornamental security employed a twice confusion process through scrambling images in receipt of encrypted images. They were creating pseudorandom chaotic orders, and the author accumulated a four-wing hyperchaotic process in the methodology. Wang and Li [38] proposed an innovative amalgamated chaotic color image encryption by using logistic and tent maps for preliminary key scanning. This method utilizes a chaotic hybrid map together via a structured logistic map and tent map. Afterward, it receives the necessary specification for Arnold mapping via a functionality transformation required to scramble that image matrix. The diffusion process utilized a chaotic neural network via Hopfield to produce a chaotic sequence of self-diffusion. At that time, the key is also created by a parameter reconstruction. Eventually, the mashed image is operated XOR with a key to acquire the penultimate encrypted cipher image. Hamza et al. [39] expressed an effective predictive cryptosystem to preserve the confidentiality of keyframes and the privacy of the patients. An innovative PRNG (pseudorandom number sequence) focused on chaos, concentrating on merging as well as cascading the positions of two of those same chaotic maps. By attaining safe and privacy-conserving communication, the medical professionals diagnosis and achieved these keyframes through limited bandwidth of energies and communication. Investigational testing from various viewpoints is done to ensure a high level of protection with more effective implementation relative to current methods. Hua et al. [40] proposed a CTBC (cosine-transform-based chaotic) system, in which two chaotic seed maps are used as a chaotic hybrid map to produce dynamic and a complex pattern of sequences. The encryption mechanism takes high-efficiency scrambling to isolate neighboring pixels and operates arbitrary pattern substitution to disperse a very small shift in the images towards all pixels of cryptographic matrix. Additionally, the summative assessment shows that arbitrary pattern substitution methods are reliant on a plain image which is functioned to scuffle them. Furthermore, the implemented architecture executes effective image encryption with the introduction of discrete random fractional transformation (DFRT). Kaur et al. [43] incorporated pseudodominated genetic algorithm processing and specific chaotic image encryption techniques. It is introduced to change the 5D chaotic map hyperparameters. Firstly, the incoming image is broken down into thread bands that used a dual-tree dynamic wavelet transform (DTCWT) to perform the TFCM. Therefore, these thread bands are diffused, and the hidden key is used from just the engineered 5D chaotic diagram. An inverse DTCWT is gradually enforced to get the ultimate encrypted image. Broumandnia [44] implemented 3D modular chaotic mapping that enhanced key size and acceleration for encryption of RGB images. To extend key space color picture encryption with modular arithmetic, he provided reasonable success with the study of the histograms as well as a correlation of the adjacency pixels. This method is used the confusion and diffusion function with the image encryption measures implemented in substitution and permutation.

Mondal et al. [45] introduced a highly efficient image encryption system for safe interaction and preservation of images. The framework is concentrated on a map of the chaotic skewed tent as well as cellular automata (CA). The synthesis for both chaotic maps with CA respectively provides a model which a larger key size as well as quicker generator PRNS. The results of the experiment indicate good effects of encryption that can also withstand every kind of identified attack. The proposed concepts followed an additional parametric observation presented with the distinguished modification, which reflects a relatively faster encryption methodology at [46].

3. Proposed Work

The mounting standard of autonomous monitoring is highly progressed manufacturing-based visual sensor and technological progression of IIoT. It is bringing effective management tools that can make accurate as well as easy analysis of the digital world. It can also perform constant adoption of cumulative monitoring networks. This can be well-known as a smart setup of healthcare. These technological ecologies are empowered to be analyzed autonomously in an intelligent way in real-time of visual data (video source). VSN (visual sensor networks) have the capability to interact smartly and agreeing to conduct critical as well as very complex visual data processing in real-time through the processing capacities and increased storage. For multi-view observation videos recorded in the healthcare communities. Its computing competencies can be utilized to evaluate streaming video footage to categorize keyframes as well as afterward eliminate obsolete and meaningless visual data, thereby reducing the parameters for minimizing bandwidth. The advanced communication skills of sensor nodes can also be
utilized to cooperatively accomplish comprehensive scene assessment to produce real-time multi-view overviews of monitoring keyframes.

Highly intelligence-based sensors can be utilized to yield a mechanized response. Subsequently, anomalous events are spotted such as the need of the patients in emergencies, discomforting from high and low blood pressure among the patients, and feeling symptoms like heart attack among the cardio patients, unbearable pain among the patients, and required help by shouting, monitoring high-risk patients’ activities like special care of cancerous patients treating in the special wards [47]. Besides, the core emphasis of our methodology, it is incorporating a very well-designed lightweight keyframe image encryption among the extracted keyframe. A well-organized, highly acceptable proposed smart setup healthcare IIoT is presented in Figure 1. Further coming sections are enforcing the best guidelines for achieving required results and its essential personifications.

3.1. Concept of Extracted Keyframes from Visual Information.

In the concept of keyframe extraction, visual information is transversely produced by installing visual sensors and retrieved from VPH (visual-processing hub). This is retrieved in terms of video frames into the entire smart setup which consists a massive amount of visual data. These visual data transports are unrealistic in terms of distance covering (more data traveling) in entire networks due to bandwidth and limitations of energy constraints in the wireless multimedia sensor networks. To handle these problems, many researchers have employed some technique to control and limits such a massive video information flow. Regarding this, researchers are adopted distinct compression schemes [48, 49] as well as video summary approaches to minimize a huge amount of visual contents at the visual-processing hub. So as to the appropriate frames, videos are traveled towards base stations [23]. Considering energies and bandwidth constraints, we employed an energy responsive keyframe extraction methodology to diminish data redundancy [50].

Our extraction methodology consists a lightweight keyframe extraction with an improved YOLOv3 algorithm [51]. In this methodology, our main emphasis is on extracting relevant keyframe from the summarized video, which is coming through installed wireless multimedia surveillance networks in the smart healthcare system. This algorithm adopted a backbone network which is called Darknet-53 [52].

In Figure 2, the up-sampling network, as well as detection layer, is recognized as a YOLO layer. YOLOv3 is completely dependent on Darknet-53 to extract keyframes from the visual input data. As an essential component, each network is using a residual. Each five layers of residual are selected differently in terms of depth and scale to perform residual among the produced output at diverse layer. All the convolutional in the number showed 53 with a residual block in terms of pair 3×3 and 1×1 layer. The spatial resolution is 1/32 smaller compare to visual input data at the final feature map size. YOLOv3 recognizes as a three-scale layer of YOLO which is basically answerable for the detection of the object at a different layer of scale. The First YOLO layer is based on grid resolution. It contains 1/32 of the visual input data and detecting big objects. The last layer has 1/8 resolution, and that can effectively detect a small extent of objects. Between the layers, one known as the up-sampling layer, and the other are several convolution layers that exist [53]. The resolution of this algorithm is initially set by default 416 × 416, and the algorithm is also favored height, as well as width, must be equal in size. But no essential to modify resolution before inputting images. We had designed appropriately in a manner to adjust the resolution of each image automatically when its obligatory.

The proposed extraction approach is administering a conceptual description at Figure 2. The whole setup includes a combination of four training modules. Firstly, the interaction of visual contents towards training module is defined. This module has been defined to train data with the help of the model module. Secondly, model module is responsible for modeling data towards received from first module. This module has capability to further model if there are some deficiencies from earlier process. Thirdly, modeled data are approaching to prediction module for accurate prediction. At the last foresight, prediction module is transferred data to detection module. Finally, the output comes as a human presence (patients and staff) via recorded video summary in terms of keyframe. A lightweight YOLOv3 algorithm [51] is quite efficient to detect visual data, either videos or images, in a real-time manner.

For the proposed extraction of keyframe, we properly trained the model in the Darknet-53 platform [52]. Additionally, this model is also renewed into the TensorFlow atmosphere. Attaining high precision, which is much required for the experimental work, we trained this model with a vast collection of image datasets. One of them is a wider-face dataset [54]. Originally this model is initially set floating-point as a by default. Therefore, it is transformed in the fixed-point model through TensorFlow. By converting the model, this model behaves computationally competent approach. It is effortlessly incorporated into the smart healthcare system. This can also suit any such small devices such as visual sensors that consume processing, bandwidth constraints, and energy. We effectively tested the model of the extraction by utilizing Face Database (FDB) [55].

Our incorporated methods are proposed to increase gratitude precision at encourager real-time exhibiting YOLOv3s bounding box, which is a more appropriate symbol of SSD (single-stage detection). The experimental results of the average accuracy are received 88–90% with 1–16 files per second (FPS). This model is operated at the environment of Intel (R) Core i5-6500 Microprocessor, CPU (Central Processing Unit) 3.20 GHz, RAM 8 GB, functioned Windows 10 Operating System. That is highly suitable concerning patient-based monitoring into smart setup healthcare IIoT-enabled architecture which is revealed extracted keyframe in Figure 2. This also indicates that the patient is correctly detected in terms of high precision as well as inside the bounding boxes. The process of extraction is incorporated among the patients for testing numerous clinical wards with the proper settings. After significantly produced keyframe from the model of extraction, the
3.2. Lightweight Cosine Functions with Operation of Hybrid Chaotic Map Keyframe Encryptions. This subdivision acquaints with examines the planned cosine function of chaotic sequence (CCS) [40]. It is physiognomies along with effective encryption methodology into the smart healthcare IIoT ecosystem. It is caused by keyframes from the video streaming data by the visual sensor. Our approach is handling first to generate PRNG from CCS with the incorporation of a secret key into the keyframe images. Secondly, it performed confusion as well as diffusion operation into the keyframe image as an engagement of bitwise XOR and highly efficient scrambling algorithms [40] as shown in Figure 3. This methodology is achieved by fast RGB keyframe encryption, randomized complex sequences, and highly encrypted cipher keyframe data. This cipher matrix is impossible to recognize an adversary to detect actual keyframe images. This can also confine the approachability of the information required in a typical cryptosystem. These keyframes are emanating from the monitoring of video streaming, which is done in terms of RGB format with highly resolution visual sensors installed at smart setup of IIoT enabled healthcare.

3.2.1. Preliminaries about Cosine Function. The CCS has incipiently pleaded each existing drawback that frail in chaos as well as tendencies of the weakness in the chaotic maps. This can be explained better in terms of used mathematical notations as below:

\[ X_{i+1} = \cos(\pi(Cos\ Seed\ Map\ 1 + Cos\ Seed\ Map\ 2 + \beta)) \tag{1} \]

where Chaotic Seed Map 1 and Chaotic Seed Map 2 are known as two different used chaotic maps. That are also well known as a combination of seed map with some control parameter and constant shifting \( \beta \) (set as \( \beta = -0.50 \)).

Equation (1) enlightens that CCS integrates with two seed maps output with adding constant shifting operator to get cosine transformation in terms of output. Mixing with two seed maps are the outcomes of a complex and efficient sequence generation in the cosine function-based hybrid chaotic sequence (CCS). Using two seed maps can also provide flexibility in terms of making countless fresh chaotic maps employing different configurations of prevailing maps. There are so many chaotic seed maps available that can be a better alternative as a complex sequence provider with the consideration or nature of the requirement. Some of them are mentioned below throughout:

- **Logistic Map:**
  \[ X_{i+1} = L(r, x_i) = 4rx_i(1 - x_i). \tag{2} \]

- **Arnold Map:**
  \[ X_{i+1} = (\Gamma: (x, y) \rightarrow (2x + y, x + y) \text{mod} 1). \tag{3} \]

- **Tent Map:**
  \[ X_{i+1} = \mu(r, x_i) = \begin{cases} 2rx_i & \text{if } x_i < 0.5 \\ 2r(1 - x_i) & \text{if } x_i \geq 0.5, \end{cases} \tag{4} \]

- **Chirikov Taylor Map:**
  \[ X_{i+1} = \begin{cases} P_{n+1} = P_n + K \sin\theta_n(\theta_n), \theta_n, \theta_n \text{mod} 2\theta, \end{cases} \tag{5} \]

- **Sine Map:**
  \[ X_{i+1} = S(r, x_i) = r\sin(\pi x_i) \tag{6} \]

- **Zaslavskii Map:**
  \[ X_{i+1} = \begin{cases} x_{n+1} = [x_n + \nu(1 + \mu y_n) + \epsilon \nu \cos(2\pi x_n)] \text{mod } 1 \\ y_{n+1} = e^{-\gamma} (y_n + e \cos(2\pi x_n)), \mu = (1 - e^{-\gamma}) \gamma, \end{cases} \tag{7} \]

- **Henon Map:**
  \[ X_{i+1} = \begin{cases} x_{n+1} = 1 - ax_n^2 + y_n \\ y_{n+1} = bx_n, \end{cases} \tag{8} \]

Arranging the above chaotic seed maps in terms of hybrid nature such as Equation 1. The incorporated cosine function-based hybrid chaotic sequences compile on the following:

- **Cosine-transform:** Pair 1.
$X_{i+1} = \{\cos(\pi(4x_i(1-x_i) + (1-r)\sin(\pi x_i) - 0.5))\}$.  

(9)

Cosine-transform: Pair 2.

$X_{i+1} = \{\cos(\pi(r\sin(\pi x_i) + 2(1-r)x_i - 0.5))$ for $x_i < 0.5$

$\cos(\pi(r\sin(\pi x_i) + 2(1-r)(1-x_i) - 0.5))$ for $x_i < 0.5$,

(10)

Cosine-transform: Pair 3.

$X_{i+1} = \{\cos(\pi(2x_i + 4(1-r)(1-x_i) - 0.5))$ for $x_i < 0.5$

$\cos(\pi(2x_i + 4(1-r)x_i(1-x_i) - 0.5))$ for $x_i < 0.5$,

(11)

where $r \in [0, 1]$, $a$ replaces $r$ and $b$ swaps $1-r$. Equations (9)–(11) are the same as our standard notations, as mentioned in equation (1). The proposed method is used equation (10) STC maps (Sine Tent Cosine) as the actual combination of the CCS in the entire paper, which is the adaptation of Sine and Tent seed maps.

3.2.2. Structural Setup towards Producing Key. The reliable key state controls the series of STC at primary states. Concerning the ideal state of key, the researchers emphasized on [56]. It is highly counseled to withstand diverse sorts of attacks whenever the key size of every chaos-based cryptographic protocol corresponds to the $2^{100}$ proportions. Concerning the effective length, which can provide freedom to maintain a higher security aspect, the key space of STC-IES used 256-bit long proportion that can be represented as $2^{256}$. It is made of five key components such as $K = [X_0, Y_0, U, g, d]$, in which preliminary states are addressed with $(X_0, Y_0)$. $U$ is the best represented component as a constraint of disorder that befuddle the preliminary states, $g$ is the coefficient of preliminary states, and $d$ comprises four-parameter of disturbance coefficients represented as $[d_1, d_2, d_3, d_4]$. Individually of each $X_0, Y_0, U, g, d_1, d_2, d_3$, and $d_4$ are a set of 32-bit length proportion. The float variables are $X_0, Y_0, U$, within the range of $[0, 1]$ and individually represented as the 32-bit stream as follows:

Float number $\sum_{i=1}^{32} Binary_i \times 2^{-i}$, where $g, d_1, d_2, d_3$, and $d_4$ are the coefficients of integer, which can be generated as follows: integer values $\sum_{i=1}^{32} Binary_i \times 2^{i-1}$.

These preliminary stages can be additionally calculated by the way of proclaimed setup of encryption operation form as follows:

$$
\begin{cases}
X'_0 = (X_0 + g + U \times d_i) \mod 1, \\
Y'_0 = (r_0 \times g + U \times d_i) \mod 1.
\end{cases}
$$

(12)

The STC map is generated uniformly scattered chaotic sequences, which is shown in Figure 4 through Table 1 for the process of bitwise XOR and highly efficient scrambling at the preliminary stages $(X_i, Y_i)$.

3.2.3. Steps of Lightweight STC-IES. The proposed STC-IES approach is the keyframe encryption as well as decryption algorithm suggested in Tables 1–3, respectively. The key approach for producing encryption is demarcated as follows:

(I) Each generated keyframe image is first permuted by sine tent cosine (STC) chaotic sequence through a randomly generated secret key to accomplishing a more complex chaotic sequence. Additionally, keyframe is reshaped through recently created complex nature chaotic sequence. After that, splitting each keyframe image as a matrix form of its color RGB channel such as red, green, and blue, an operation is performed as a bitwise XOR and highly efficient scrambling.

(II) Each matrix of color keyframe is diffused by bitwise XOR by combining highly efficient scrambling algorithms to generate the cipher keyframe images.

(III) The cipher keyframe is confused through the highly efficient scrambling procedures [40] to obtain the caused encrypted keyframe image.

The decryption process approach is fully followed through the inverse of highly efficient scrambling procedures and inverse bitwise XOR methods, that is, consecutively decrypt encrypted cipher image at the original keyframe images. Tables 1–3 are confirmed pseudocode. It is used for bitwise XOR, STC sequence generation with the addition of highly efficient scrambling algorithms, one-to-one, where $S$ is the sine tent cosine (STC) chaotic sequence and the size of the keyframe image is $M \times N$. The produced secure key is used in entire cryptosystem and is formed with the random key generation procedures.
Figure 4: Bifurcation of tent map, sine map, and complex STC sequences [40].

Table 1: Algorithm 2, STC sequence generation.

| Step | Description |
|------|-------------|
| 1    | Reading secret key K (and allocate to x) |
| 2    | Read r |
| 3    | Resetting chaotic sequence |
| 4    | Starting for loop from m = 1:100 |
| 5    | \( X \leftarrow \cos(\pi \times (r \times \sin(\pi \times x) + 2 \times (1 - r) \times x - 0.5)) \) |
| 6    | end of the for loop |
| 7    | Starting for loop from m = 1:M × N |
| 8    | \( X \leftarrow \cos(\pi \times (r \times \sin(\pi \times x) + 2 \times (1 - r) \times (1 - x) - 0.5)) \) |
| 9    | \( S(m) = X \) |
| 10   | end of the for loop |
| 11   | STC generation |

Table 2: Algorithm 1, encryption process through bitwise XOR.

| Step | Description |
|------|-------------|
| 1    | Read size \((M \times N)\) RGB keyframe image |
| 2    | Resizing keyframe images |
| 3    | Generation of random number for getting key |
| 4    | Generating secret key by calling function |
| 5    | Generating STC sequence by calling function |
| 6    | Reshaping keyframe images with STC |
| 7    | Splitting RGB keyframe image in each 3 channels IR, IG, and IB |
| 8    | Bitwise XOR operation is performed in every channel |
| 9    | Performing highly efficient scrambling algorithm obtained keyframe channel from step 9 |
| 10   | Merging every scrambled keyframe channel |
| 11   | Encrypting cipher keyframe images C |

Table 3: Algorithm 2, highly efficient scrambling.

| Step | Description |
|------|-------------|
| 1    | Obtain block size \( H = \min([M/2], [N/2]) \) of color channels separately (operated keyframe of bitwise XOR) |
| 2    | Producing four STC sequences such as O, P, Q, and R |
| 3    | Sorting each four STC sequences such as sort \((O)\), sort \((P)\), sort \((Q)\), and sort \((R)\) and obtaining their corresponding indexes |
| 4    | Two matrices S and T are initialized with the square of block size \( H^2 \times H^2 \) |
| 5    | Starting loop, for \( j = 1: H^2 \) (\( H^2 \) square of the block size within \( M \times N \)) |
| 6    | Starting loop, for \( i = 1: H^2 \) |
| 7    | \( a = ((1 + IP(j) - 1)mod H^2) + 1 \) |
| 8    | \( b = ((i + IR(j) - 1)mod H^2) + 1, Si = IOa, ti = IQb \) |
4. Simulation Results and Discussion

This segment imposes as well as discourses the investigational consequences of the proposed STC-IES on MATLAB 2018a version software. It also analyzes security with the help of using test images from the eminent source USC-SIPI [57] repository database of digital images. An ideal and prominent encryption approach is always intelligent to encrypt dissimilar classes of images into highly secure cipher images. When an encrypted method is strongly enforced to reach an optimum security level in terms of cipher images, it is noticeable that any keyframe can only be retrieved by knowing the arcuate used top-secret key. Unless the known used secret key, not any information of the keyframe images can be extracted in smart healthcare IIoT-enabled system. Figure 5 is illustrated the encryption approach. It used USC-SIPI images A (as a test image). Image A is the pepper image, and its corresponding originated all the three-color frequency as mentioned at histogram R, G, and B, which is purely showing the maximum correlation of the pixels in each color channel. The encrypted cipher image of the pepper image B and its corresponding three-color channel histogram R, G, and B show uniform distribution in each color channel. Similarly, Image C is the keyframe image. It originated from all the color channels as shown in each color channel histogram R, G, and B, which originally showed maximum pixels of the correlation in individual color channels. The encrypted cipher image of the keyframe image is D. It is conforming that the entire three-color channel histogram R, G, and B are screening uniform distribution in the separate color channel.

Figure 5 is indicating that the proposed approach has a strongly encrypted methodology. Uniformly distributed pixels are also visible in the cipher image. It means this cipher image has adopted better encryption process; in this way, any intruder or attackers cannot effectively gain original keyframe information from cipher image. Therefore, STC-IES can easily convalesce every keyframe fully from consequently encrypted image data for the reason that all the handling process is completely reversible. Our methods have robust inefficiency, fast execution, and minimal computational overhead, employing bitwise XOR and highly efficient scrambling algorithms at a smart healthcare setup. Thus, this encryption methodology can be accomplished faster and efficiently in the IIoT ecosystem. To provide better security as well as privacy towards the patients in the respectively possible emergency requirement, Table 4 depicts the time complexity to encrypt keyframe, uses test images, and undergoes comprehensive comparison with the different types of available encryption algorithms.

The simulation and experimental cryptosystems are effectively conducted on the required platforms. For example, Intel (R) Core i5-6500 Microprocessor, CPU (Central Processing Unit) 3.20 GHz, RAM 8GB, operated Windows 10 Operating System. The demonstration of the fast keyframe encryption is exhibiting STC-IES from various image extent exemplified on the numerous results in terms of tabular form. It is always required to have a vintage high-quality of deciphered images because a noteworthy discrepancy of pixels into keyframe can disturb entire pixels into the encrypted images. Incorporation of the STC-IES can be a safeguard in terms of higher security aspects of the cipher images. A delicate modification of pixels into a ciphered encrypted image matrix can distress some pixels as a deciphered conclusion (results) into the decryption approach. In this crucial condition, if STC-IES encrypted data miss some pieces of information, the process of decryption can also easily recuperate tangible keyframe visual facts. Figure 6 demonstrates the quality-based approach after the decipherment process as soon as the STC-IES encrypted cipher images suffered from noises or various types of proportion data forfeiture. For example, in Figure 6(a), the decipherment methodology is fully recovered in pepper image and no data loss into encrypted cipher of pepper image are viewed. Even though the cipher images had also lost some data (info) or noise moreover, their deciphered findings incorporate most sensory information of the same individual pepper images, which can be presented in Figures 6(b) to 6(d). Accordingly, the employed STC-IES can fairly decrypt the superior quality in terms of encrypted cipher.

5. Security Analysis

With the intention of validating STC-IES preeminence, this unit scrutinizes efficient security in terms of resulting aspects with minimal encryption speed assessment, histogram analysis, information entropy analysis, differential attack analysis, correlation analysis, analysis of produced key, and comprehensive comparative analysis among surveillance systems. To supplementary exemplify the effectiveness of STC-IES, we equate our approach with the
other available advanced image encryptions. We cited directly, respectively, finding in terms of references reported at esteemed scientific journals by the author for the fair comparison at the area of highly noticeable image-based encryption algorithms.

5.1. Encryption Speed Assessment. This segment is familiarized with minimal computational-based overhead and speed assessment displayed in Table 4. The time computation segment of any encrypted system depends on the generation of chaotic sequences with the proper handling of permutation and diffusion methods in the operating algorithms, eEnforcing smart healthcare enabled IIoT system. We accentuated to achieve minimal computational overhead for constructing relatively better communication in speed with the adoption of the STC-IES mechanism. We observed that the generation of complex sequences is relatively quick in nature. The operation of bitwise XOR with highly efficient scrambling is operating in minimal computational time. The proposed approach is demonstrated as an average encryption time assessment for each set of various sizes of the keyframes. The production of numerical values of the encrypted keyframes is presented in Table 4 and compared with other past color image encryption methodology such as [20, 37, 40, 58–62]. Our proposed approach

| Method   | Encryption time (E.T) 256×256 keyframes (images) | Encryption time (E.T) 512×512 keyframes (images) | Encryption time (E.T) 1024×1024 keyframes (images) |
|----------|--------------------------------------------------|--------------------------------------------------|--------------------------------------------------|
| Proposed | 0.0670–0.08470                                   | 0.2205–0.2541                                    | 1.0079–1.1095                                    |
| [20]     | 0.1616                                           | 0.6708                                           | 2.821                                            |
| [37]     | 1.28                                             | NA                                               | NA                                               |
| [40]     | 0.0949                                           | 0.4010                                           | 1.9857                                           |
| [58]     | 0.080–0.082                                      | 0.327–0.333                                      | NA                                               |
| [59]     | 0.6212                                           | NA                                               | NA                                               |
| [60]     | 0.3340                                           | 1.3357                                           | 5.3223                                           |
| [61]     | 0.224                                            | 0.9731                                           | 3.8377                                           |
| [62]     | 1.7874 (En & Dec)                                | NA                                               | NA                                               |
is fast in running and has minimum computational effort, which enforces for real-time application setup like a smart healthcare IIoT-enabled architecture.

5.2. Histogram Analysis. Keyframe histogram is the best illustration of a typical graphical representation of the pixel rate distribution in the keyframe images. The keyframe/encrypted cipher keyframe image histogram contains the statistical data by which evaluation of the robustness recognizes the statistical data analysis. Really, histogram reports about the distribution of a keyframe’s grey-level values, and relatively smooth distribution will expose the loopholes in the method that attackers can use to initiate a preferred-ciphertext attack using statistical analysis. However, for reliable cryptography, the dispersal of histograms must be uniform. Figure 5 demonstrates the histograms of the keyframe and its ciphered images, which can pictorially recognize that the arrangement amongst pixel correlation at ciphered-keyframe images has fairly unvarying color frequencies. Still, there are a few variations in the original keyframe image [44, 58, 63].

The histogram deviation is used to measure an encrypted image, and this also contributes to significant analysis. Suppose the quantity of variation in the encrypted cipher keyframe image is small, the greater its uniformity. Two encrypted keyframe images are produced using different surreptitious keys, even with similar image data. It shows better homogeneity, uniformity, of the encrypted keyframe images if the differences are similar enough. Figure 5 demonstrates color test image histograms, wherein it is clearly verified, specifically color frequency histogram representation and its encrypted image histogram accurately. We perceived that each color channel of the test images and keyframe images shows their natural behavior before encryption, and after encryption, each color channel behaves uniformly in nature. The uniform behavior of the histogram can be calculated numerically of a variance. The uniform behavior of a histogram is purely dependent on the variance. Lower variance is recognized as the higher nature of uniformity. The higher variance is lower uniformity. The variance of the histogram can be statistically obtained by Eq (13), in which grayscale numerical value is \( n \), \( Y_i \), and \( Y_j \) stands for the values of the pixels at the \( i_{th} \), \( j_{th} \) gray levels [58, 64]:

\[
\text{Variance} (y) = \frac{1}{n^2} \sum_{i=1}^{n} \sum_{j=1}^{n} \frac{(y_i - y_j)^2}{2} .
\] (13)

Consequently, in such a scenario, if any attacker decrypts any piece of the image, assuredly, the attacker cannot find the entire original data because the proposed method has a powerful encryption methodology that keeps away any data leakage. In the same way, with the observation of the keyframe channels as well as encrypted keyframe channels remains identical keyframe, it is signifying no data loss during the communication into smart healthcare IIoT enabled system occurs. Therefore, the histogram analysis equally justifies that the proposed STC-IES methodology strongly avoided any statistical or numerical attacks. It also provided a statement for the integrity, including consistency during the transmission at smart setup healthcare system.

5.3. Information Entropy Analysis. The methodology of analyzing the amount of uncertainty and randomness behavior among the cipher images’ correlated pixels is called information entropy. It can be well demarcated as
\[ H(n) = \sum_{i=1}^{255} P(n_i) \log_2 P(n_i), \]  

\[ H(n) = -\sum_{i=1}^{255} P(n_i) \log_2 P(n_i) = -\sum_{i} \frac{1}{256} \log_2 \frac{1}{256} = -\frac{256}{256} \sum_{i} \log_2 \frac{1}{256} = -\log_2 2^{256} = -(-8) \log_2 2 = 8. \]

After encryption, the encoded cipher image must continue to act as the best possible random image. This is validated that encrypted keyframe information entropy should be around numerical value 8, significantly proved from equation (14). The following is also demonstrated: the information entropy around 8 is highly random in nature and very low information leakage is present in our proposed smart healthcare IIoT-enabled system. Table 5 demonstrates information entropy of color channels with its extracted as well as encrypted keyframes (1–6). It is also relatively compared in Table 6 with earlier referenced encryption methodology such as [20, 50, 65–70]. Tables 5 and 6 exemplified by the projected approach have shown healthier results in terms of information entropy for each color channel, which almost have numerical value 8 as an encrypted keyframe image. This indicates that the proposed STC-IES methods deliver quite a suitable notch of security, privacy, and randomness behavior in contradiction to the information entropy attack. That is the furthestmost requirement for the appropriate way of handling secure concern smart healthcare IIoT-enabled system.

5.4. Differential Attack Analysis. The differential attack is a well-known attack into keyframe image encryption. This attack is used as an active security attack. It focuses on associating a sturdy relationship among keyframes per their ensuing encrypted images via perceiving transformations at a keyframe. It can annoy encrypted data. If it preserves diffusion in an ideal way, the keyframe encryption methodology expresses high usefulness in the sidestepping differential attack. This diffusion process proves that the encrypted-cipher keyframe possibly will scatter a minor alteration throughout the keyframe image over the entire statistics or data. The proposed STC-IES mechanism is appropriately demonstrated as an innovative way diffusion process in Figure 5.

The differential attacks can be best examined among encryption methodologies to withstand attacks with the two well-known metrics such as NPCR (number of pixel change rate) and UACI (uniform average change intensity) [74]. NPCR calculates the change percentage amongst the pixel positions within an encrypted cipher keyframe by adjusting one pixel’s worth at keyframe or original image. UACI possible information entropy’s numerical value recognizes as 8 for the ideal scenario at each random keyframes or image. In an ideal, discrete image, probabilities of any containing \( n_i \) signs are identical. The probability among each \( n_i \) symbol is, therefore, 1/256:

\[ \text{NPCR} = \frac{\sum_{i,j} G(i,j)}{M \times N} \times 100\%, \]
\[ G(i, j) = \begin{cases} 0 & \text{if } C_1(i, j) = C_2(i, j) \\ 1 & \text{if } C_1(i, j) \neq C_2(i, j) \end{cases}, \]
\[ \text{UACI} = \frac{1}{M \times N} \left[ \sum_{i,j} \frac{|C_1(i, j) - C_2(i, j)|}{255} \right] \times 100\%. \]

The magnitude of the keyframe matrix is denoted as \( M \times N \). Equation (17) is calculated \( G(i, j) \), which is pixel transformation between corresponding encrypted keyframe images. Table 7 illustrates the best possible NPCR and UACI produced values from keyframe in the proposed STC-IES algorithm, and reasonable comparison is shown in Table 8 through previously referenced encryption algorithms such as [20, 50, 71–73, 75]. The results indicate that the produced result of NPCR is very near to a hundred and produced the result of UACI approaching very near to one-third of the hundred. This is purely demonstrates encryption methodology of STC-IES. It incorporates effectively dissimilar randomize keyframe images as well as completely misses the effectiveness of differential attacks. In this manner, the planned cryptosystem ensured complete security and privacy from the attacker for not getting any information into smart healthcare IIoT-enabled system.

For example, investigation of ideal encryption and randomness nature of NPCR, UACI result into cryptosystem. Suppose the encrypted matrixes which size is \( M \times N \), C1, and C2 are encrypted cipher keyframes. An ideal encrypted cipher image is a certain image that cannot be discerned from a pseudorandom image. Simply cipher image is an arbitrary arena at the size of \( M \times N \), where integer \( i \in [1, M] \) and \( j \in [1, N] \), arbitrary pixels price \( C(i, j) \) identical nature and independently occurs isolated unvarying distribution taking place 0 to \( C \)’s principal buttressed numeral \( E \) such as \( \forall j \in [1, N], \forall i \in [1, M], \exists C(i, j) \sim i.i.d U(0, E) \) [74].
Table 5: Information entropy of keyframe and test images.

| Methods       | Images          | Plain image | Encrypted image |
|---------------|-----------------|-------------|-----------------|
|               | R               | G           | B               | R       | G        | B       |
| Proposed      | Pepper          | 7.3388      | 7.4963          | 7.0583  | 7.9962   | 7.9831  | 7.9981  |
|               | Lake            | 7.3124      | 7.6429          | 7.2136  | 7.9876   | 7.9878  | 7.9977  |
|               | P001 (keyframe 1)| 7.8579      | 7.9484          | 7.9484  | 7.9971   | 7.9961  | 7.9892  |
|               | P002 (keyframe 2)| 7.7876      | 7.7255          | 7.6506  | 7.9989   | 7.9975  | 7.9956  |
|               | P003 (keyframe 3)| 7.7592      | 7.6845          | 7.6197  | 7.9978   | 7.9952  | 7.9959  |
|               | P004 (keyframe 4)| 7.7925      | 7.7459          | 7.7153  | 7.9984   | 7.9898  | 7.9959  |
|               | P005 (keyframe 5)| 7.7982      | 7.8063          | 7.7699  | 7.9988   | 7.9965  | 7.9959  |
|               | P006 (keyframe 6)| 7.7754      | 7.7022          | 7.6331  | 7.9899   | 7.9897  | 7.9966  |

Table 6: Information entropy comparison through relative approaches.

| Methods       | Images          | Plain image | Encrypted image |
|---------------|-----------------|-------------|-----------------|
|               | R               | G           | B               | R       | G        | B       |
| Proposed      | P002 (keyframe 2)| 7.7876      | 7.7255          | 7.6506  | 7.9989   | 7.9975  | 7.9956  |
| [20] Keyframe 6| 6.4410         | 6.3789      | 6.4770          | 7.9778  | 7.9778   | 7.9797  |
| [50] Keyframe 4| 7.0818         | 6.7460      | 7.1210          | 7.9969  | 7.9919   | 7.9954  |
| [65] House     | 7.4007         | 7.2312      | 7.4357          | 7.9985  | 7.9984   | 7.9985  |
| [66] Baboon    | 7.7326         | 7.7591      | 7.4557          | 7.9993  | 7.9993   | 7.9994  |
| [67] Girl      | 7.3490         | 7.1876      | 6.9857          | 7.9994  | 7.9995   | 7.9994  |
| [68] Image 2   | 4.7664         | 4.4860      | 5.0793          | 7.9021  | 7.9027   | 7.9023  |
| [69] G01       | 7.16399        | 7.16399     | 7.16399         | 7.99696 | 7.99696  | 7.99696 |
| [70] Pepper    | NA             | NA          | NA              | 7.9993  | 7.9993   | 7.9991  |

Table 7: NPCR and UACI of the keyframe and test images.

| Methods       | Images          | NPCR | UACI |
|---------------|-----------------|------|------|
|               | R               | G    | Blue | R    | G    | B    |
| Proposed      | Pepper          | 99.5520 | 99.5735 | 99.6532 | 33.3396 | 33.3363 | 33.4394 |
|               | Lake            | 99.4546 | 99.5453 | 99.6868 | 33.32473 | 33.2669 | 33.3329 |
|               | P001 (keyframe 1)| 99.6634 | 99.5383 | 99.5983 | 33.3782 | 33.3493 | 33.3483 |
|               | P002 (keyframe 2)| 99.5989 | 99.6682 | 99.5959 | 33.3498 | 33.3467 | 33.3467 |
|               | P003 (keyframe 3)| 99.5566 | 99.6536 | 99.5990 | 33.4086 | 33.3474 | 33.3364 |
|               | P004 (keyframe 4)| 99.6343 | 99.5888 | 99.6699 | 33.3366 | 33.3495 | 33.3498 |
|               | P005 (keyframe 5)| 99.6346 | 99.6456 | 99.6412 | 33.3332 | 33.3983 | 33.3351 |
|               | P006 (keyframe 6)| 99.4996 | 99.5978 | 99.5892 | 33.3596 | 33.5477 | 33.3499 |

Table 8: NPCR and UACI comparison through relative approaches.

| Methods       | Images          | NPCR | UACI |
|---------------|-----------------|------|------|
|               | R               | G    | Blue | R    | G    | B    |
| [20] Keyframe 4| 99.6009        | 99.5899 | 99.6311 | 33.4910 | 33.3394 | 33.4804 |
| [50] Keyframe 3| 99.6136        | 99.6136 | 99.5960 | 33.4406 | 33.3564 | 33.2764 |
| [66] Baboon    | 0.9962         | 0.9962 | 0.9962 | 0.2988 | 0.2844 | 0.3104 |
| [71] Frame 5   | 99.6070        | 99.5808 | 99.6307 | 33.4251 | 33.4013 | 33.5713 |
| [72] House 2   | 0.999908       | 0.999908 | 0.999923 | 0.332853 | 0.332929 | 0.332986 |
| [73] Lena      | 99.6258        | 99.6183 | 99.6182 | 33.4635 | 33.4877 | 33.4749 |
hypothesis assessment of NPCR \((C_1, C_2)\) by means of \(\beta\)-level consequence follows as [74] in
\[
\begin{align*}
H_0: \text{NPCR } (C_1, C_2) &= \xi_{\text{NPCR}} \\
H_1: \text{NPCR } (C_1, C_2) &< \xi_{\text{NPCR}}.
\end{align*}
\] (19)

It is implicit at what time \(\text{NPCR } (C_1, C_2) < \xi_{\text{NPCR}}\) [76], and \(H_0\) hypothesis assessment is purely rejected. That is the vital worth designed for challenging NPCR. On the contrary, \(H_0\) hypothesis assessment is acknowledged. The produced result of \(\text{NPCR}^*_\beta\) is critically enlightened [74] in the following equation:
\[
\text{NPCR}^*_\beta = \xi_{\text{NPCR}} - \frac{\eta_{\text{NPCR}}}{\Phi(\beta/2)} = \left( E - \frac{\sqrt{E/MN}}{\Phi(\beta/2)} \right) / (E+1),
\] (20)

where \(\Phi(\beta) = 1/\sqrt{2\pi} \exp(-\beta^2/2)\) [77–79] is well known as CD (cumulative density) function of SD (standard normal distribution) which has range amongst zero towards one, expressed through \(N\) [0, 1], and \(E\) represented as a gray image that is incorporated numerical value 255 in the current study:
\[
\begin{align*}
H_0: \text{UACI } (C_1, C_2) &= \xi_{\text{UACI}} \\
H_1: \text{UACI } (C_1, C_2) &< \xi_{\text{UACI}}.
\end{align*}
\] (21)

Once \(\text{UACI}(C_1, C_2) \notin (\text{UACI}^*_\beta^-, \text{UACI}^*_\beta^+)\) [80], \(H_0\) hypothesis assessment is virtuously rejected. That is the crucial worth designed for challenging NPCR. On the contrary, \(H_0\) hypothesis assessment is legalized. The produced results of \(\text{UACI}^*_\beta^-, \text{UACI}^*_\beta^+\) are critically explicated [74] in the following:
\[
\begin{align*}
\text{UACI}^*_\beta^- &= \xi_{\text{UACI}} - \frac{\eta_{\text{UACI}}}{\Phi(\beta/2)} \\
\text{UACI}^*_\beta^+ &= \xi_{\text{UACI}} + \frac{\eta_{\text{UACI}}}{\Phi(\beta/2)}.
\end{align*}
\] (22, 23)

\[
\begin{align*}
\xi_{\text{UACI}} &= \frac{E + 2}{3E + 3}, \\
\eta_{\text{UACI}} &= \frac{(E + 2)(E^2 + E + 3)}{18 (E + 1)^2 MN}. \\
\end{align*}
\] (24, 25)

Tables 9 and 10, correspondingly, exhibit assessment results from level \(\beta = 0.05\) of the NPCR and UACI.

### 5.5. Correlation Analysis

CC\(_{xy}\) correlation coefficient of the two neighboring pixels offered randomness information. That is a parameter for calculating a keyframe cipher’s robustness and can only be quantified utilizing equations (26)–(32). CC\(_{xy}\) analyses the total amount of linear correlation between both the adjoining pixels in the keyframe images. For authentic images, each direction of the keyframe images (diagonal, horizontal, and vertical) amongst pixel and the corresponding pixel is highly correlated. The STC-IES method’s primary function is likely to tinkle causal relationships between nearby pixels together at each direction, such as vertical (V), horizontal (H), and its diagonal (D). At the same time, keyframe data matrix achieved approximately zero correlation with the highest possible unpredictable nature and strangeness (randomness) [44, 81, 82]:

\[
\text{CC}_{xy} = \frac{\text{Covariance}(x, y)}{\sqrt{D(x)D(y)}},
\] (26)

\[
\text{Covariance}(x, y) = \frac{1}{N} \sum_{i=1}^{N} (x_i - E(x))(y_i - E(y)),
\] (27)

\[
D(x) = \frac{1}{N} \sum_{i=1}^{N} (x_i - E(x))^2,
\] (28)

\[
D(y) = \frac{1}{N} \sum_{i=1}^{N} (y_i - E(y))^2,
\] (29)

\[
E(x) = \frac{1}{N} \sum_{i=1}^{N} x_i,
\] (30)

\[
E(y) = \frac{1}{N} \sum_{i=1}^{N} y_i.
\] (31)

The scope for the coefficient’s performance is between +1 (a positive one) and −1 (a negative one), minor the value of the coefficient for encrypted cipher keyframe image, higher the quality of the cipher to battle any the statistical attack. Scenario 1: If CC\(_{xy}\) > 0, it exposes a positive correlation into the encrypted matrix. Scenario 2: If CC\(_{xy}\) < 0, it exposes negative correlation into the encrypted cipher matrix. Scenario 3: If CC\(_{xy}\) = 0, it exposes no correlation into the encrypted keyframe cipher matrix,

### Table 9: Randomness test of NPCR.

| Algorithms | Image shape | NPCR   | NPCR00.05 | NPCR tests |
|------------|-------------|--------|-----------|------------|
| STC-IES    | 512 × 512   | 99.6536| 99.6034   | Pass       |

### Table 10: Randomness test of UACI.

| Algorithms | Image shape | UACI   | UACI\(_{0.05}^–\) | UACI\(_{0.05}^+\) | UACI tests |
|------------|-------------|--------|-------------------|-------------------|------------|
| STC-IES    | 512 × 512   | 33.4086| 33.3463           | 33.4568           | Pass       |
Table 11: CCs of two bordering pixels, plain and ciphered images (including test images).

| Methods | Images      | Plain images | Encrypted images |
|---------|-------------|--------------|------------------|
|         | H           | V            | D                | H           | V            | D                |
| Pepper  | R           | 0.9786       | 0.9820           | 0.9694      | 5.1e-04      | 1.2e-04          | 0.0017           |
|         | G           | 0.9775       | 0.9990           | 0.9650      | 0.0017       | -6.7e-04         | -4.2e-04         |
|         | B           | 0.9760       | 0.980            | 0.9640      | 0.0031       | 1.6e-04          | 3.5e-05          |
|         | R           | 0.9677       | 0.9663           | 0.9502      | 7.6e-04      | -0.0016          | 0.0014           |
| Lake    | G           | 0.9620       | 0.9640           | 0.9540      | 9.4e-04      | -0.0011          | -2.4e-04         |
|         | B           | 0.9670       | 0.9650           | 0.9520      | 0.0022       | 4.5e-04          | 0.0031           |
|         | R           | 0.9630       | 0.9760           | 0.9427      | -0.0023      | 0.0017           | 5.5e-04          |
| Proposed| P001 (keyframe 1) | G          | 0.9620       | 0.9740       | 0.9410      | 9.6e-04          | 0.0023           | 5.3e-04          |
|         | G           | 0.9605       | 0.9750           | 0.9430      | 2.2e-06      | 0.0022           | -6.2e-04         |
|         | R           | 0.9578       | 0.9905           | 0.9511      | 2.3e-05      | -4.3e-04         | 0.0032           |
|         | G           | 0.9560       | 0.9900           | 0.9505      | 0.0028       | -9.1e-04         | 0.0033           |
|         | B           | 0.9570       | 0.9901           | 0.9500      | 5.2e-07      | -3.3e-04         | 0.0011           |
|         | R           | 0.9554       | 0.9926           | 0.9498      | 6.16e-04     | -0.0022          | -3.1e-04         |
|         | G           | 0.9540       | 0.9910           | 0.9480      | -5.3e-04     | -0.0011          | 0.0012           |
|         | B           | 0.9545       | 0.9918           | 0.9490      | 0.0015       | -0.0038          | 5.01e-04         |
|         | R           | 0.9578       | 0.9939           | 0.9525      | 3.12e-04     | -0.0016          | 0.0011           |
|         | G           | 0.9500       | 0.9906           | 0.9510      | 0.0015       | 0.0024           | -0.0022          |
|         | B           | 0.9565       | 0.9925           | 0.9520      | -0.0013      | 0.0011           | 0.0023           |
|         | R           | 0.9494       | 0.9889           | 0.9386      | 3.23e-04     | 8.45e-05         | 0.0012           |
|         | G           | 0.9480       | 0.9875           | 0.9360      | 0.0016       | 0.0013           | -0.0014          |
|         | B           | 0.9485       | 0.9870           | 0.9375      | 4.50e-05     | 0.0017           | -0.0014          |

Figure 7: Distributed very close adjacent pixel (horizontal, vertical, and diagonal plane) at keyframe as well as encrypted keyframe (red channel of a baboon).
In this article, Table 11 demonstrates the random assortment of ten thousand combinations of two corresponding pixels at every three directions and correlation coefficient (CCxy) values for test image pepper, lake, and extracted keyframe images with the size of \((512 \times 512)\). The discoveries of Table 11 and Figures 7–9 state significantly that the CCxy of two adjoining pixels of extracted keyframe images in each direction, such as diagonal, vertical, and horizontal is just about to 1. However, the encrypted-cipher keyframe is almost zero. Produced result expressions of Table 11 including visual histogram representation at Figures 7–9, effectively validate the uppermost superiority of breaching the correlation link amongst the adjoining pixel at the test images including extracted keyframe images through planned STC-IES methods and fairly comparison on Table 12 through former referenced encryption approaches such as [39, 50, 66, 75, 84, 85, 87]. The results and comparison prove that the proposed STC-IES methodology is exceedingly unaffected to any sorts of statistical attacks into smart healthcare IIoT-enabled system.

5.6. Analysis of Produced Key. Configuration among the chaotic seed maps is susceptible towards preliminary surroundings. A cryptographic scheme is classified of superior quality or appropriate key size if it has sufficiently computational complexity with such a heightened sensitivity to modify the key. The proposed STC-IES has \(2^{256}\) key size means 256-bit long proportion. That encounters the key performance requirements and is exceedingly operative in sidestepping dissimilar sort of security attacks [40, 56, 88]. Additionally, the proposed methodology, including key structure, behaves extremely sensitive to design architecture in five blocks. The STC-IES methodology articulated key size in Table 13 and equitably comparison with the past referenced encryption algorithms such as [37, 65, 71, 89–93]. It endorses that the proposed keys size delivers a reasonably healthier variety of the key space to engender more complex chaotic actions. Consequently, STC-IES has the satisfactory key size to evade all the possibility of brute force attacks.

5.7. Comparative Analysis among the Monitoring and Surveillance System. This subdivision is comparatively based on the proposed methodology with the heretofore referenced surveillance as well as image encryption algorithms in Table 14. Table 14 expressively illustrates all the key characteristics in terms of security surveillance and encryption methodology that can prove secure and robustness constraint based on key analysis, encryption speeds, entropy analysis, correlation coefficients (CCxy), NPCR and UACI produced outcomes. The outcomes of the proposed

---

**Figure 8:** Distributed very close adjacent pixel (horizontal, vertical, and diagonal plane) at keyframe as well as encrypted keyframe (green channel of a baboon).
methodology are fairly reasonable as well as nearly ideal standards. We compared proposed methods with past referenced schemes such as [20, 39, 41, 42, 50, 71]. We noticed that the referenced surveillance and encryption scheme is produced relative results to attain confidentiality of the security. We compared our results with numerous images employing diverse platforms and upbringing functionality, each restrained factor. The proposed methodology has comparatively better speed with minimal complexity in the execution, analogous better-quality entropy, lowermost correlation coefficient (CCx,y), satisfactory NPCR, and UACI statistics. Significantly improved results are resolutely signposted. That the proposed methodology has exceedingly adequate in the arena of smart healthcare IIoT enabled setup with monitoring (surveillance) as well as cryptographically secure ecosystem.

![Figure 9: Distributed very close adjacent pixel (horizontal, vertical, and diagonal planes) at keyframe as well as encrypted keyframe (blue channel of a baboon).](image)

| Methods            | Images     | Plain images | Encrypted images |
|--------------------|------------|--------------|------------------|
|                    |            | H            | D                |                     |
| Proposed P002 (keyframe 2) | R          | 0.9578       | 0.9911           | 2.3e-05, -4.3e-04, 0.0032 |
| RGB frame          | G          | 0.9560       | 0.9905           | 0.0028, -9.1e-04, 0.0033 |
| [39]              | B          | 0.9570       | 0.9901           | 5.2e-07, -3.3e-04, 0.0011 |
| [50]              |            | 0.99370      | 0.9910           | 0.00120, -0.00270, 0.00020 |
| [84]              |            | 0.99090      | 0.98340          | -0.00070, 0.00210, -0.00100 |
| [66]              |            | 0.99310      | 0.98240          | 0.00150, -0.00100, 0.00070 |
| [73]              |            | 0.99439      | 0.9880           | 0.0051, -0.0033, 0.0015 |
| [75]              |            | 0.99225      | 0.7860           | 0.0087, -0.0051, -0.0089 |
| [85]              |            | 0.967841     | 0.976007         | -0.001557, 0.002225, 0.000582 |
| [86]              |            | 0.9824       | 0.9632           | 0.0016, 0.0015, -0.0017 |
| [73]              |            | 0.9518       | 0.9751           | -0.0049, 0.0019, 0.0010 |
| [75]              |            |              |                  | 0.0022, 0.0022, -0.0019 |
Table 13: Comparative key space analysis.

| Algorithm       | Image size | Key space | Speed | Entropies | CC_{xy} | NPCR | UACI  |
|-----------------|------------|-----------|-------|-----------|---------|------|-------|
| STC-IES         | 512 × 512  | 2^{56}    | 0.2205–0.2541 | 7.9998 | 0.0011 | 99.6536 | 33.4086 |
| [20]            | 512 × 512  | 10^{90}   | 0.6708 | 7.9998    | 0.0035 | 99.6125 | 33.4451 |
| [39]            | 640 × 480  | 2^{372}   | 0.95/0.96 | 7.9994  | 0.0021 | 99.609  | 33.465  |
| [41]            | Keyframe 0065 | 2^{711} | 2.58   | 7.9998    | 0.0019 | 99.609  | 33.450  |
| [42]            | 1024 × 1024 | 2^{300}   | NA     | 7.91      | 0.03    | 99.5826 | 33.4213 |
| [50]            | 512 × 512  | 2^{128}   | 0.2811–0.3119 | 7.9991 | 0.0015 | 99.6212 | 33.4406 |
| [71]            | Keyframe 640 × 480 | 2^{192} | 0.790  | NA        | 0.0035 | 99.615  | 33.4658 |

Table 14: Fair comparative discussion amongst the monitoring and surveillance architecture.

| Algorithms | Image size | Key length | Speed | Entropies | CC_{xy} | NPCR | UACI  |
|------------|------------|------------|-------|-----------|---------|------|-------|
| STC-IES    | 512 × 512  | 2^{56}     | 0.2205–0.2541 | 7.9998 | 0.0011 | 99.6536 | 33.4086 |
| [20]       | 512 × 512  | 10^{90}    | 0.6708 | 7.9998    | 0.0035 | 99.6125 | 33.4451 |
| [39]       | 640 × 480  | 2^{372}    | 0.95/0.96 | 7.9994  | 0.0021 | 99.609  | 33.465  |
| [41]       | Keyframe 0065 | 2^{711}  | 2.58   | 7.9998    | 0.0019 | 99.609  | 33.450  |
| [42]       | 1024 × 1024 | 2^{300}   | NA     | 7.91      | 0.03    | 99.5826 | 33.4213 |
| [50]       | 512 × 512  | 2^{128}    | 0.2811–0.3119 | 7.9991 | 0.0015 | 99.6212 | 33.4406 |
| [71]       | Keyframe 640 × 480 | 2^{192} | 0.790  | NA        | 0.0035 | 99.615  | 33.4658 |

6. Conclusion

The technological progression of the hybrid IoT ecosystem is referred to as the IIoT system. It is extensively organized with the industrial, medical healthcare system to deliver the finest services counting security and privacy about patients. The produced report formally focuses on security, privacy, and its challenges in smart setup healthcare IIoT architecture. We implemented secure monitoring (surveillance) with intelligently keyframe extraction and lightweight cosine function hybrid chaotic map encryption. It also assists, including security and privacy from the outside world or any adversary. At first, a well-disciplined model of keyframe extraction is employed with a lightweight YOLOv3 algorithms. This model is successfully operated and tested with a vast collection of image dataset Face Database to retrieve meaningful detected frames (normal/abnormal events) through the visual sensor. The average accuracy is received optimally around 90% with an acceptable frame per second rate. Second, a lightweight cosine function encryption is employed over approved extracted keyframe to remain exceptionally secure and safe from further attacks. The generated cosine function chaotic sequences are a non-linear transform to engender as well as exhibit expressively very complex chaos behavior. Our encryption methodology implies a better diffusion-confusion process of bitwise XOR operation and highly efficient scrambling algorithms, which are achieved to encrypt each color image channel separately and scatter neighboring pixels into different positions quickly. This proposed methodology ensured satisfactorily encrypted matrix as a cipher keyframe without identifying real keyframes into smart setup healthcare from adversarial threads.

Numerous security discussions and analysis results интеграта the effectiveness of the proposed methodology. This has relatively higher security characteristics, and minimal computational processing agreed and contending with the earliest image encryption approaches. It also validates its accomplishment in the IIoT ecosystem with minimizing bandwidth, storage space, communication cost, transmission expenses, and correspondingly waning time spending of specialists handling due to huge amount of monitoring data to take verdict over any such suspicious incidents detection or any suspicious action detection as an emergency need from the patients at smart setup healthcare architecture. The produced concept can also be utilized in many relatively analogous urgent responded real-time projects: traffic-control, fire-detection, crime-control, and smart transportation at smart cities.

For future concern, this approach can be supported to assimilate information from further systems, aimed at numerous applications and additional advanced security facet and privacy dealings in any exact areas within the healthcare sector. The innovative way can probably integrate dynamic key as an alternative applied process for additional ornamental security and privacy.

Data Availability

Previously reported are used to support this study and are available at [Wider-Face Data Set, Face Database (FDB), USC-SIPI Image Data Set Repository]. These prior studies (and datasets) are cited at relevant places within the text as references [51, 52, 54].

Conflicts of Interest

The authors declare that they have no conflicts of interest.

Acknowledgments

This work was supported by the National Natural Science Foundation of China (Grant No. 61370073), the National High Technology Research and Development Program of China (Grant No. 2007AA01Z423), and the project of Science and Technology Department of Sichuan Province. The authors are also acknowledging the generous support from the Research supporting Project number (RSP-2021/122), King Saud University, Riyadh, Saudi Arabia.

References

[1] R. A. Memon, J. P. Li, J. Ahmed, M. I. Nazeer, M. Ismail, and K. Ali, "Cloud-based vs. blockchain-based IoT: a comparative survey and way forward," Frontiers of Information Technology & Electronic Engineering, vol. 21, no. 4, pp. 563–586, 2020.
[2] X. Huang, “Intelligent remote monitoring and manufacturing system of production line based on industrial Internet of Things,” *Computer Communications*, vol. 150, pp. 421–428, 2020.

[3] K. N. Qureshi, S. S. Rana, A. Ahmed, and G. Jeon, “A novel and secure attacks detection framework for smart cities industrial internet of things,” *Sustainable Cities and Society*, vol. 61, p. 102343, 2020.

[4] B. Jiang, J. Li, G. Yue, and H. Song, “Differential privacy for industrial internet of things: opportunities, applications and challenges,” *IEEE Internet of Things Journal*, vol. 8, p. 1, 2021.

[5] L. Nie, X. Wang, S. Wang et al., “Network traffic prediction in industrial internet of things backbone networks: a multi-task learning mechanism,” *IEEE Transactions on Industrial Informatics*, vol. 17, pp. 7123–7132, 2021.

[6] M. Serro, S. Hack, M. Henze, M. Schuba, and K. Wehrle, “Challenges and opportunities in securing the industrial internet of things,” *IEEE Transactions on Industrial Informatics*, vol. 17, no. 5, p. 1, 2020.

[7] T. Wang, H. Luo, W. Jia, A. Liu, and M. Xie, “MTES: an intelligent trust evaluation scheme in sensor-cloud-enabled industrial internet of things,” *IEEE Transactions on Industrial Informatics*, vol. 16, no. 3, pp. 2054–2062, 2020.

[8] S. Khan and M. Altayar, “Industrial Internet of things: investigation of the applications, issues, and challenges,” *International Journal of Advances in Applied Sciences*, vol. 8, no. 1, pp. 104–113, 2021.

[9] R. A. Memen, J. P. Li, M. I. Nazeer, A. N. Khan, and J. Ahmed, “DualFog-IoT: additional fog layer for solving blockchain integration problem in internet of things,” *IEEE Access*, vol. 7, pp. 169073–169093, 2019.

[10] J. Chi, Y. Li, J. Huang et al., “A secure and efficient data sharing scheme based on blockchain in industrial Internet of Things,” *Journal of Network and Computer Applications*, vol. 167, p. 102710, 2020.

[11] J. Khan, J. P. Li, I. Ali et al., “An authentication technique based on oauth 2.0 protocol for internet of things (IoT) network,” in *Proceedings of the 2018 15th International Computer Conference on Wavelet Active Media Technology and Information Processing (ICCWAMTIP)*, pp. 160–165, Chengdu, China, 14–16 Dec. 2018.

[12] J. Khan, H. Abbas, and J. Al-Muhtadi, “Survey on mobile user’s data privacy threats and defense mechanisms,” in *Procedia Computer Science*, 2015.

[13] S. Khan, “Modern Internet of Things as a challenge for higher education,” *International Journal of Computer Science and Network Security*, vol. 18, no. 12, pp. 34–41, 2018.

[14] K.-K. R. Choo, S. Gritzalis, and J. H. Park, “Cryptographic solutions for industrial internet-of-things: research challenges and opportunities,” *IEEE Transactions on Industrial Informatics*, vol. 14, no. 8, pp. 3567–3569, 2018.

[15] A. AlAbdulatif, I. Khalil, X. Yi, and M. Guizani, “Secure edge of things for smart healthcare surveillance framework,” *IEEE Access*, vol. 7, pp. 31010–31021, 2019.

[16] P. Sundaravadi, K. Kesavan, L. Kesavan, S. P. Mohanty, and E. Kogianos, “Smart-log: a deep-learning based automated nutrition monitoring system in the IoT,” *IEEE Transactions on Consumer Electronics*, vol. 64, no. 3, pp. 390–398, 2018.

[17] S. H. Alsamhi, O. Ma, M. S. Ansari, and F. A. Almalki, “Survey on collaborative smart drones and internet of things for improving smartness of smart cities,” *IEEE Access*, vol. 7, pp. 128125–128152, 2019.

[18] P. Chanak and I. Banerjee, “Congestion free routing mechanism for IoT-enabled wireless sensor networks for smart healthcare applications,” *IEEE Transactions on Consumer Electronics*, vol. 66, no. 3, pp. 223–232, 2020.

[19] M. Shuai, L. Xiong, C. Wang, and N. Yu, “A secure authentication scheme with forward secrecy for industrial internet of things using Rabin cryptosystem,” *Computer and Communications*, vol. 160, pp. 215–227, 2020.

[20] 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 Transactions on Industrial Informatics*, vol. 14, no. 8, pp. 3679–3689, 2018.

[21] M. Sajjad, I. Mehmoond, and S. W. 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, 2014.

[22] Z. Yang, B. Liang, and W. Ji, “An intelligent end-edge-cloud architecture for visual IoT assisted healthcare systems,” *IEEE Internet Things J.*, 2021.

[23] I. Mehmoood, M. Sajjad, W. Ejaaz, and S. W. Baik, “Saliency-directed prioritization of visual data in wireless surveillance networks,” *Information Fusion*, vol. 24, pp. 16–30, 2015.

[24] S. Nazir, S. Khan, H. U. Khan et al., “A comprehensive analysis of healthcare big data management, analytics and scientific programming,” *IEEE Access*, vol. 8, pp. 95714–95733, 2020.

[25] J. Ding, L. Jiang, and C. He, “User-centric energy-efficient resource management for time switching wireless powered communications,” *IEEE Communications Letters*, vol. 22, no. 1, pp. 165–168, 2018.

[26] H. Yang, Y. Ye, X. Chu, and M. Dong, “Resource and power allocation in SWIPT-enabled device-to-device communications based on a nonlinear energy harvesting model,” *IEEE Internet of Things Journal*, vol. 7, no. 11, pp. 10813–10825, 2020.

[27] K. Muhammad, T. Hussain, and S. W. Baik, “Efficient CNN based summarization of surveillance videos for resource-constrained devices,” *Pattern Recognition Letters*, vol. 130, pp. 370–375, 2020.

[28] T. Hussain, K. Muhammad, A. Ullah, Z. Cao, S. W. Baik, and V. H. C. De Albuquerque, “Cloud-assisted multiview video summarization using CNN and bidirectional LSTM,” *IEEE Transactions on Industrial Informatics*, vol. 16, no. 1, pp. 77–86, 2020.

[29] C. Huang and H. Wang, “A novel key-frames selection framework for comprehensive video summarization,” *IEEE Transactions on Circuits and Systems for Video Technology*, vol. 30, no. 2, pp. 577–589, 2020.

[30] J. Lei, Q. Luan, X. Song, X. Liu, D. Tao, and M. Song, “Action parsing driven video summarization based on reinforcement learning,” *IEEE Transactions on Circuits and Systems for Video Technology*, vol. 29, pp. 2126–2137, 2018.

[31] Y. Yuan, T. Mei, P. Cui, and W. Zhu, “Video summarization by learning deep side semantic embedding,” *IEEE Transactions on Circuits and Systems for Video Technology*, vol. 29, no. 1, pp. 226–237, 2019.

[32] J. Wang, K. Han, S. Fan et al., “A logistic mapping-based encryption scheme for Wireless Body Area Networks,” *Future Generation Computer Systems*, vol. 110, pp. 57–67, 2020.

[33] A. Al-Khedhairi, A. Elsonbaty, A. A. Elsadany, and E. A. A. Hagras, “Hybrid cryptosystem based on pseudo chaos of novel fractional order map and elliptic curves,” *IEEE Access*, vol. 8, pp. 57733–57748, 2020.

[34] Y.-Q. Zhang, J.-L. Hao, and X.-Y. Wang, “An efficient image encryption scheme based on S-boxes and fractional-order differential logistic map,” *IEEE Access*, vol. 8, pp. 54175–54188, 2020.
[35] L. Huang, S. Cai, X. Xiong, and M. Xiao, “On symmetric color image encryption system with permutation-diffusion simultaneous operation,” Optics and Lasers in Engineering, vol. 115, no. July 2018, pp. 7–20, 2019.

[36] I. T. Almalkawi, R. Halloush, A. Alsaaran, A. Al-Dubai, and J. N. Al-karaki, “A lightweight and efficient digital image encryption using hybrid chaotic systems for wireless network applications,” J. Inf. Secur. Appl. vol. 49, p. 102384, 2019.

[37] X. Chai, X. Fu, Z. Gan, Y. Lu, and Y. Chen, “A color image cryptosystem based on dynamic DNA encryption and chaos,” Signal Processing, vol. 155, pp. 44–62, 2019.

[38] X. Y. Wang and Z. M. Li, “A color image encryption algorithm based on Hopfield chaotic neural network,” Optics and Lasers in Engineering, vol. 115, pp. 107–118, 2019.

[39] R. Hamza, Z. Yan, K. Muhammad, P. Bellavista, and F. Titouna, “A privacy-preserving cryptosystem for IoT E-healthcare,” Information Science, vol. 527, pp. 493–510, 2019.

[40] Z. Hua, Y. Zhou, and H. Huang, “Cosine-transform-based chaotic system for image encryption,” Information Science, vol. 480, pp. 403–419, 2019.

[41] R. Hamza, K. Muhammad, Z. Lv, and F. Titouna, “Secure video summarization framework for personalized wireless capsule endoscopy,” Pervasive and Mobile Computing, vol. 41, pp. 436–450, 2017.

[42] 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, 2019.

[43] M. Kaur, D. Singh, K. Sun, and U. Rawat, “Color image encryption using non-dominated sorting genetic algorithm with local chaotic map,” Future Generation Computer Systems, vol. 107, pp. 333–350, 2020.

[44] A. Broumandnia, “The 3D modular chaotic map to digital color image encryption,” Future Generation Computer Systems, vol. 99, pp. 489–499, 2019.

[45] B. Mondal, S. Singh, and P. Kumar, “A secure image encryption scheme based on cellular automata and chaotic sawt tent map,” J. Inf. Secur. Appl. vol. 45, pp. 117–130, 2019.

[46] J. Khan, J. Li, A. Khan, G. A. Khan, and S. Ahmad, “Efficient secure surveillance on smart healthcare IoT system through cosine-transform encryption,” Journal of Intelligent and Fuzzy Systems, vol. 40, no. 1, pp. 1417–1422, 2021.

[47] A. U. Haq, J. P. Li, J. Khan et al., “Intelligent machine learning approach for effective recognition of diabetes in E-healthcare using clinical data,” Sensors, vol. 20, no. 9, pp. 2649, 2020.

[48] L. Gong, K. Qiu, C. Deng, and N. Zhou, “An image compression and encryption algorithm based on chaotic system and compressive sensing,” Optics & Laser Technology, vol. 115, pp. 257–267, 2019.

[49] J. Wu, B. Cheng, M. Wang, and J. Chen, “Energy-aware concurrent multipath transfer for real-time video streaming over heterogeneous wireless networks,” IEEE Transactions on Circuits and Systems for Video Technology, vol. 28, no. 8, pp. 2007–2023, 2018.

[50] J. Khan, J. P. Li, B. Ahamad et al., “SMSH: secure surveillance mechanism on smart healthcare IoT system with probabilistic image encryption,” IEEE Access, vol. 8, pp. 15747–15767, 2020.

[51] J. Redmon and A. Farhadi, “YOLOv3: an incremental improvement,” Computer Vision and Pattern Recognition, 2018.

[52] J. Redmon, Darknet Open Source Neural Network Framework, [Online]. Available: https://github.com/pjreddie/darknet Accessed, 2016.

[53] J. Li, J. Gu, Z. Huang, and J. Wen, “Application research of improved YOLO V3 algorithm in PCB electronic component detection,” Applied Sciences, vol. 9, no. 18, 2019.

[54] T. C. U. of H. K. Multimedia Laboratory, Department of Information Engineering, WIDER FACE: A Face Detection Benchmark, [Online]. Available: http://shuoyang1213.me/WIDERFACE/ Accessed.

[55] K. D. Mislov Grgic, FACE RECOGNITION HOME-PAGE,[Online]. Available: http://www.face-rec.org/databases/ Accessed.

[56] G. Alvarez and S. Li, “Some basic cryptographic requirements for chaos-based cryptosystems,” Int. J. Bifurc. Chaos, vol. 16, no. 08, pp. 2129–2151, 2006.

[57] Digital Test Image, Uci-sipi Image Database for Research in Image Processing, Image Analysis, and Machine Vision, [Online]. Available: http://sipi.usc.edu/database/ Accessed, 2021.

[58] K. A. Kumar 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, 2019.

[59] M. Alawida, A. Samsudin, J. Sen Teh, and R. S. Alkhawaldeh, “A new hybrid digital chaotic system with applications in image encryption,” Signal Processing, vol. 160, pp. 45–58, 2019.

[60] P. Ping, F. Xu, Y. Mao, and Z. Wang, “Designing permutation–substitution image encryption networks with Henon map,” Neurocomputing, vol. 283, pp. 53–63, 2018.

[61] A.-V. Diaconu, “Circular inter–intra pixels bit-level permutation and chaos-based image encryption,” Information Science, vol. 355–356, pp. 314–327, 2016.

[62] D. Kumar, A. B. Joshi, and V. N. Mishra, “Optical and digital double color-image encryption algorithm using 3D chaotic map and 2D-multiparameter fractional discrete cosine transform,” Results Opt, vol. 1, p. 100031, 2020.

[63] M. A. Khan, J. Khan, A. A. Alghamdi, and S. M. A. B. Saidan, “Image encryption enabling chaotic ergodicity with logistic and sine map,” International Journal of Advanced Computer Science and Applications, vol. 12, no. 7, pp. 437–442, 2021.

[64] X. Chai, Y. Chen, and L. Broyley, “A novel chaos-based image encryption algorithm using DNA sequence operations,” Optics and Lasers in Engineering, vol. 88, pp. 197–213, 2017.

[65] X. Chai, J. Bi, Z. Gan, X. Liu, Y. Zhang, and Y. Chen, “Color image compression and encryption scheme based on compressive sensing and double random encryption strategy,” Signal Processing, vol. 176, p. 107684, 2020.

[66] Z. Liu, C. Wu, J. Wang, and Y. Hu, “A color image encryption using dynamic DNA and 4-D memristive hyper-chaos,” IEEE Access, vol. 7, pp. 78367–78378, 2019.

[67] X. Kang, X. Luo, X. Zhang, and J. Jiang, “Homogenized Chebyshev-Arnold map and its application to color image encryption,” IEEE Access, vol. 7, pp. 114459–114471, 2019.

[68] D. Ravichandran, P. Praveen Kumar, J. B. B. Rayappan, and R. Amirtharajan, “DNA chaos bend to secure medical privacy,” IEEE Transactions on NanoBioscience, vol. 16, no. 8, pp. 850–858, 2017.

[69] A. A. Abd El-Atty, B. Abd-El-Atty, E. M. Abou-Nassar, and S. E. Venegas-Andraca, “Controlled alternate quantum walks based privacy preserving healthcare images in Internet of Things,” Optics & Laser Technology, vol. 124, p. 105942, 2020.

[70] A. Shakiba, “A randomized CPA-secure asymmetric-key chaotic color image encryption scheme based on the Chebyshev mappings and one-time pad,” J. King Saud Univ. - Comput. Inf. Sci, vol. 33, no. 5, pp. 562–571, 2021.

[71] R. Hamza, K. Muhammad, A. Kumar, and G. Ramirez-Gonzalez, “Hash based encryption for keyframes of diagnostic hysteroscopy,” IEEE Access, vol. 6, pp. 60160–60170, 2018.

[72] X. Kang, A. Ming, and R. Tao, “Reality-preserving multiple parameter discrete fractional angular transform and its application to color image encryption,” IEEE Transactions on
Circuits and Systems for Video Technology, vol. 29, no. 6, pp. 1595–1607, 2019.

[73] X. Ouyang, Y. Luo, J. Liu, L. Cao, and Y. Liu, “A color image encryption method based on memristive hyperchaotic system and DNA encryption,” International Journal of Modern Physics B, vol. 34, no. 04, p. 2050014, 2020.

[74] Y. Wu, J. P. Noonan, and S. Agaian, “NPCR and UACI randomness tests for image encryption,” Cyberjournals.Com, 2011.

[75] D. Herbadji, A. Belmeguenai, N. Derouiche, and H. Liu, “Colour image encryption scheme based on enhanced quadratic chaotic map,” IET Image Processing, vol. 14, no. 1, pp. 40–52, 2020.

[76] A. El Halabi, A. Hachem, L. Al-Akhrass, H. Artail, and H. U. Khan, "Identifying the linkability between Web servers for enhanced Internet computing," in Proceedings of the MELECON 2014 - 2014 17th IEEE Mediterranean Electrotechnical Conference, pp. 1–5, Beirut, Lebanon, 13-16 April 2014.

[77] H. Khan and M. N. Faisal, "A Grey-based approach for ERP vendor selection in small and medium enterprises in Qatar," International Journal of Business Information Systems, vol. 19, no. 4, p. 465, 2015.

[78] O. A. Bankole, V. V. M. Lalitha, H. U. Khan, and A. Jinugu, "Information Technology in the maritime industry past, present and future: focus on LNG carriers," in Proceedings of the 2017 IEEE 7th International Advance Computing Conference (IACC), pp. 759–763, Hyderabad, India, 5-7 Jan. 2017.

[79] H. U. Khan, V. V. M. Lalitha, and J. F. Omonaiye, "Employees' perception as internal customers about online services: a case study of banking sector in Nigeria," International Journal of Business Innovation and Research, vol. 13, no. 2, p. 181, 2017.

[80] V. F. Brock and H. U. Khan, "Are enterprises ready for big data analytics? A survey-based approach," International Journal of Business Information Systems, vol. 25, no. 2, p. 256, 2017.

[81] Y. Zhang, X. Wang, L. Liu, and J. Liu, "Fractional order spatiotemporal chaos with delay in spatial nonlinear coupling," Int. J. Bifurc. Chaos, vol. 28, no. 02, p. 1850020, 2018.

[82] A. U. Rehman, H. Wang, M. M. A. Shahid, S. Iqbal, Z. Abbas, and A. Firdous, “A selective cross-substitution technique for encrypting color images using chaos, DNA rules and SHA-512,” IEEE Access, vol. 7, pp. 162786–162802, 2019.

[83] J. Zhang, D. Fang, and H. Ren, “Image encryption algorithm based on DNA encoding and chaotic maps,” Mathematical Problems in Engineering, vol. 2014, pp. 1–10, 2014.

[84] L. Li, G. Wen, Z. Wang, and Y.-X. Yang, “Efficient and secure image communication system based on compressed sensing for IoT monitoring applications,” IEEE Transactions on Multimedia, vol. 22, no. 1, pp. 82–95, Jan. 2020.

[85] A. Mansouri and X. Wang, “A novel one-dimensional chaotic map generator and its application in a new index representation-based image encryption scheme,” Information Science, vol. 563, pp. 91–110, 2021.

[86] F. Yang, J. Mou, K. Sun, Y. Cao, and J. Jin, “Color image compression-encryption algorithm based on fractional-order memristor chaotic circuit,” IEEE Access, vol. 7, pp. 58751–58763, 2019.

[87] L. Li, G. Wen, Z. Wang, and Y.-X. Yang, “Efficient and secure image communication system based on compressed sensing for IoT monitoring applications,” IEEE Transactions on Multimedia, p. 1, 2019.

[88] P. Nigel, Smart, "Algorithms, Key Size and Protocols Report (2018)," ECRYPT – CSA, [Online]. Available: http://www.ecrypt.eu.org/csa/documents/D5.4-FinalAlgKeySizeProt.pdf Accessed, 2018.

[89] 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 Processing: Image Communication, vol. 52, pp. 6–19, 2017.

[90] A. Yaghouti Niyat, M. H. Moattar, and M. Niazi Torshiz, “Color image encryption based on hybrid hyper-chaotic system and cellular automata,” Optics and Lasers in Engineering, vol. 90, pp. 225–237, 2017.

[91] J. Tamang, "Dynamical properties of ion-acoustic waves in space plasma and its application to image encryption," IEEE Access, vol. 9, pp. 18762–18782, 2021.

[92] X. Chai, X. Zhi, Z. Gan, Y. Zhang, Y. Chen, and J. Fu, “Combining improved genetic algorithm and matrix semi-tensor product (STP) in color image encryption,” Signal Processing, vol. 183, p. 108041, 2021.