A COMPREHENSIVE SURVEY ON SECURITY APPROACHES FOR HEALTHCARE DATA IN IOT

Afreen Fatima Mohammed, Research Scholar, Department of CSE, UCE, Osmania University, Hyderabad, India, afreenfatima05@gmail.com

Dr.Ahmed Abdul Moiz Qyser, Professor & Head of CSE, Muffakham Jah College of Engineering & Technology, Hyderabad, India, aamoiz@gmail.com

Abstract IoT in healthcare industry make smart medical devices and wearable interconnected. IoT consists of battery operated resource constrained devices like RFID, sensors. A security mechanism must be chosen that operates in such a resource constrained devices. Lightweight cryptography offer both security as well as performance. In terms of hardware implementations, chip size and energy consumption by lightweight cryptography are less compared to the general cryptography. In software implementations, the smaller code and RAM size are preferable for lightweight applications. The medical data collected consist of text and images, which make text encryption methods in most cases not applicable to images. The differences include the size of an image. The image data is typically much larger than that of text data. The other difference relates to data loss when a compression technique is used. Unlike image data, text data when compressed rarely permit loss. Hence, researchers investigated several lossy/lossless image encryption methods. The paper proposes to use a Signature mechanism to promote confidentiality, integrity and non-repudiation in a single step. It has discussed to use optimization algorithm in order to augment the security by selecting the optimal key and promoting an optimal key exchange.

***Keywords* —authentication, encryption, key exchange, Lightweight cryptography, medical images, Optimization, Signcryption**

I. INTRODUCTION

Healthcare is one of the application areas in IoT, where the traditional healthcare is augmented by IoT devices such as smart bio-sensors, wearable devices and on-body sensors that collect patient's data and transfer it to the centralized cloud for storage. This centralized cloud database is managed by the hospital management system and can be accessed by authorized patient, doctors, nurses and other hospital staff.

Medical data of a patient includes, bio sensors data, patient's diagnostic information as well as scanned medical images such as X-Ray, Ultrasound, MRI, CT and etc. Before the data is sent to the cloud, a security mechanism must be employed to send the secured data. Numerous mechanisms have been employed for secure data transmission. By means of employing a cryptographic technique, data confidentiality can be maintained. A Digital signature mechanism can also be employed to ensure the integrity of a signed medical data and verify the identity of the signer i.e., patient, doctor, hospital staff .Digital Signature is a good solution for detecting the intentional or accidental modification of digital contents [2]. Authentication and verification of the key can be done using message Authentication Protocol (MAC) [11]. The primitives of the lightweight cryptography are encryption, hash functions, and digital signature. The sensor data is encrypted by using hash functions and digital-signatures [34]. For enhancing the security level of encryption and decryption, optimization algorithms must also be employed [33]. The process of optimization can be described to find the best solution of the function from the system within constraints [35]. These algorithms can be used for selecting best optimal key in cryptography as well as involve in optimal key exchanges. Image encryption schemes are classified into two broad categories: spatial domain methods and frequency domain methods. The term spatial domain refers to the image plane itself, and approaches in this category are based on direct manipulation of the pixels in an image. In these algorithms, the general encryption usually destroys the correlation amongst pixels and thus makes the encrypted images incompressible. Frequency domain methods are based on modifying the frequencies of an image. The image pixels can be reconstructed (recovered) completely via an inverse process with no loss of information. This allows working in the frequency domain and then returning to the spatial domain without any loss in information [12].

 DOI : 10.35291/2454-9150.2022.0034

Medical data usually contains medical images. Various measures have been taken to provide security to medical data such as the information hiding technique which include digital watermarking of an image, the encryption which includes conventional encryption techniques and others such as chaotic encryption [8]. Watermarking techniques enhances security of medical images [2]. Digital watermarking is a technique to embed encoded information into digital data so that the information is imperceptible but easily decoded by authorized parties. Chaos theory plays an important role in cryptography because of their corresponding counterparts in cryptosystems, such as the sensitivity on initial conditions and system parameters, ergodicity and topological transitivity. They rely on chaotic maps to encrypt images[10]. Chaos theory, which essentially emerged from mathematics and physics, deals with the behavior of certain nonlinear dynamic systems that exhibit a phenomenon under certain conditions known as chaos which adopt the Shannon requirement on diffusion and confusion [3][4][6]. Also, unlike the conventional cryptographic algorithms, which are mainly based on discrete mathematics, chaos-based cryptosystems rely on the complex dynamics of nonlinear systems which are deterministic[8].

Many chaos-based cryptographic algorithms have been extensively studied. These algorithms consist of two major phases: permutation and substitution[15]. Optical encryption methods have attracted much attention for their high speed, parallel processing and large storage memories[14]. Cellular automatons (CA) are another kind of dynamical systems that has been successfully and widely used to build robust images cryptosystems by exploiting their dynamical and randomness properties, with the capacity to exhibit complex and unpredictable behavior [13]. Research has also been done on medical image encryption scheme based on the cosine number transform (CNT). Since the CNT is defined over algebraic structures with a finite number of elements (a finite field), only modular arithmetic is needed for computing the transform. Consequently, the computation of a CNT is considerably sensitive to changes in the vector being transformed. In other words, two slightly different vectors may have significantly distinct CNTs, which is desirable for cryptographic applications[16]. Various studies have been done for image authentication based on Digital Signature and Watermarking mechanisms. A digital signature includes a set of extracted features, which captures the essence of image content in compact representation. It is stored as an extra file and later used for authentication. Signature based methods work on both integrity protection of an image and repudiation prevention of the sender. Watermarking is used for protecting the integrity of the image [36].

Much research is also been done in the area of steganography which is the science of concealing data in a transmission medium in such a way that it would not draw the attention of eavesdroppers. Various algorithms have been proposed to implement steganography in digital images [4]. Encryption and watermarking are considered together to trace data during its distribution [5]. Existing digital color image encryption schemes are less preferable for encryption of digital gray images due to the following two reasons. The first is that color encryption algorithms have low encryption rate and secondly, they are lossy by nature. Therefore, it is desirable to develop a secure and efficient encryption algorithm for digital gray images [7]. However there are some implementations of color image encryption which improve the quality of decrypted image by applying super-resolution techniques [9]. Researchers have also studied the application of ECC, AES algorithm for image encryption [17] [18].

A number of conventional encryption schemes have appeared in the literature such as DES, Triple DES, IDEA, AES, etc. However, these schemes require a large computational time, and are mainly used to protect textual data. They have been found poorly suitable for digital images characterized with some intrinsic features such as high pixel correlation and redundancy [20]. Thus, they are not suitable for encrypting digital medical images due the intrinsic characteristics of these images such as large data size, existence of bulk data capacity, high redundancy and strong correlation between adjacent pixels. In recent years, selective image encryption, which is a trend to minimize the processing time for encryption and decryption of images while maintaining a sufficient security level, has grasped the attention of researchers. Unlike conventional encryption schemes that act on the whole plain image, selective encryption schemes act on selected portions of the plain image. There exist a number of selection techniques such as edge maps, region of interest (ROI) and entropy-based techniques [19].

II. RELATED WORK

Rajagopalan et al. [21] have proposed a server – client model of authenticated medical image communication. In this paper, it is discussed how a medical record of any patient can be accessed from a centralized database, maintained by Hospitals. The medical records are generally consist of medical images such as radiography, sonography, ultrasound scanned images. Whenever an intended user, wants to access a particular medical image from the server, the server will trace a particular medical record, encrypt it using AES algorithm with 128-bit key. This AES encrypted medical image is further secured by embedding a 4-digit onetime password (OTP) in the random pixels of the AES encrypted image. The 4-digit OTP is generated using a Tent map, which is a pseudo random sequence generator. This

 DOI : 10.35291/2454-9150.2022.0034

OTP embedded image is then shared to the intended user via intranet. Upon receiving the OTP through GSM, the authorized user verifies the similarity of received OTP in mobile and extracted one from the encrypted medical image. After integrity checking, the decryption is performed to retrieve the original medical record.

Mohanty et al. [22] have proposed a hardware architecture for a Secure Digital Camera (SDC) integrated with the Secure Better Portable Graphics (SBPG) compression algorithm, suitable for applications in IoT. The paper focuses on patient data protection and authentication. SDC is a device that augments the standard features of a digital camera with additional built-in facilities for real-time performance, low-cost and low-power operation. In this paper, a novel encoder with built-in watermarking, encryption facility along with compression facility called SBPG is presented. The watermarked data is encrypted using AES and embedded in the center quarter of the image and then compressed using BPG Compression Encoder. The watermarking is done in frequency domain selecting mid-frequency range and by using Discrete Cosine Transform (DCT). The conjoint use of encryption and watermarking algorithms provide full protection in terms of confidentiality and data integrity. BPG Compression is done, based on High Efficiency Video Coding (HEVC), which is considered as a major advance in compression techniques.

Al-Shayea et al. [23] focuses on preserving the authenticity of the origin of medical images from distortion and various malicious attacks using Digital Watermarking of medical images. It proposed a hybrid measurement technique for digital image watermarking which utilizes medical images such as X-ray, MRA and CT. Hybridization is carried out on three levels decomposition of Discrete wavelet transformation. Each level uses various types of wavelet transformation to present the watermarked image, and then extracts the medical watermark from the original watermarked image. The results of diverse types of attacks have been compared and statistical parameters are evaluated, which measures the quality of an image.

Khan et al. [24] have focused to protect medical data by using image encryption techniques. The paper proposes an encryption mechanism that involves three rounds of high-speed scrambling and pixel adaptive diffusion operations, for shuffling random neighboring pixels. Pixel adaptive mechanism implements modulo arithmetic operation. Simulations and experiments demonstrate that the encryption mechanism employing modulo arithmetic operation have comparatively higher levels of security.

Wang et al. [25] have proposed a Logistic Mapping-based Encryption in Wireless Body Area of network(WBAN). WBAN is a network in IoT domain, which provides interconnection between numerous wearable biomedical sensors and centralized databases. The purpose of WBAN is to provide continuous monitoring, remote diagnosis, emergency and remote medical services, there by utilizing less power consumption. The paper focuses on to balance the trade-off between hardware resource utilization and protection level. The paper discusses that how in a certain chaotic system, Lyapunov factor is utilized to evaluate chaotic characteristic. Its expression is a simple nonlinear iterative equation, which is defined as follows:

$$x_{n+1} = \mu x_n(1 - x_n), \; x_n \in [0, 1], \; n = 0, 1... \quad (1)$$

Each pixel value of an image can be encrypted. The pixel value of an image and binary sequence are XOR bit by bit to get the transmission cipher text. The study has shown the evaluation results illustrate that the proposed encryption scheme yields high performance and high efficiency-hardware resources utilization.

Sangavi et al. [26] proposed an encryption scheme based on Rossler Chaotic System and Sine map. The row-wise and column-wise permutations incorporate the outcomes of Rossler chaotic sequences. The diffusion process is carried out using the yielded sequence of both Rossler system and Sine map.. The proposed encryption scheme exhibited good degree of efficiency and robustness to withstand all kinds of statistical attacks against other schemes.

Abd EL-Latif et al. [27] have proposed a framework for secure privacy-preserving for IoT-based healthcare utilizing the benefits of quantum walks, in which the patients in one location encrypt confidential images using the suggested encryption mechanism, uploading the cipher images to the cloud-IoT. The proposed Encryption Algorithm is based on running CAQWs on a circle. It is composed of substitution and permutation phases based on CAQWs. Simulation results and numerical analysis proved that the proposed encryption mechanism has high efficiency as well as high security based on quantum mechanics.

Khan et al. [28] have proposed a Secure Surveillance Mechanism with Probabilistic Image Encryption on Smart Healthcare IoT System. In the proposed scheme, meaningful images are extracted from a summarized video in keyframe extraction module. Then an efficient probabilistic and lightweight encryption algorithm is implemented at extracted frames to keep it secure from any adversary.

Sruthi et al. [29] proposed a Hybrid Lightweight Signcryption scheme for IoT. The data collected by IoT device employs this proposed scheme by encrypting a data using ultra-lightweight symmetric block cipher PRESENT. In this study, 80 bit session key is used to encrypt 64 bit plain text. This session key must be securely transmitted to the receiver, which is done by encrypting the session key by receiver's public key, using ECC algorithm. The cipher

 DOI : 10.35291/2454-9150.2022.0034

text and cipher key are being sent to the receiver along with the signature. Signature generation and encryption processes are done in parallel to minimize the time taken for processing. In the receiving end, cipher key, cipher text and signature are verified. The proposed Signcrytion scheme is efficient in terms of providing security to the message, as well as message authorship and non-repudiation is guaranteed. The proposed system lowers the overhead in the existing system by using a lightweight technique in hybrid methodology.

Ren et al. [30] proposed a practical homomorphic encryption scheme that enables data users in IoT systems to securely operate data over encrypted data, thereby protecting the privacy of key data in the system. Homomorphic Encryption (HE) enables computation to be performed over encrypted data without retrieving the plain text. HE-enabled IoT Systems securely bring together data owners (Dos), data users(DUs) who need the data. DUs securely operate data over third-party cloud server without leakage of any information. An enhanced protocol is proposed to improve the security and privacy of cloud-based IoT systems.

Sun et al. [31] have provided a new attribute-based encryption scheme (ABE) called the Sub-String Searchable ABE (SSS-ABE) scheme for sharing and querying of encrypted data. In SSS-ABE scheme, the data owner encrypts the data under an access structure and uploads the encrypted data to the cloud server. And only the data user who satisfies the access structure can query it. In addition, the outsourcing method is also introduced to reduce the local computation of the decryption process, so that the outsourcing SSS-ABE can be applied to IoT devices.

S.Sheeba Rani et al. [32] have analyzed the difficulties with data collection in IoT-based healthcare applications and, proposed a healthcare data secure scheme to provide security and ensuring the privacy of the patient's data. A SIMON block cipher algorithm is applied on the sensed data for encryption. The share generation model is developed based on Chinese Remainder Theorem(CRT) for improving the privacy of healthcare data among individuals. Using CRT, copy of every ciphertext is generated based on the selected number of users. The optimal selection of users is done based on the metaheuristic algorithm called Hybrid Teaching and Learning Based Optimization(HTLBO). The performance of the proposed work is evaluated in terms of energy cost, computation time and the outcomes ensure the security chances in IoT-based healthcare systems.

III. OBSERVATIONS

Based on the experimental results conducted in the papers studied, observations were made by studying the performance evaluation parameters. Table I gives the comparison of evaluated PSNR and BER. From the observations studied in the papers, it has been noticed that cipher images are dispersed uniformly for Histogram Analysis in [24], [27], [28], which proves that encrypted keyframe image histograms have uniform pattern of pixel values and are completely different from the original keyframe image histograms. To assess the Key Sensitivity in [27], decryption is performed with several keys for permutation process by keeping the initial values for substitution keys as it is. For every round of data sizes in [32], the throughput computed is found to be minimal. Based on the values of PSNR computed in [21], [22], [33], BER is calculated as:

$$BER=1/PSNR \qquad (2)$$

Table I. Comparison of evaluated PSNR and BER

References	PSNR	BER
[21]	43.8654	0.0228
[22]	55.4	0.01805
[33]	59.45	0.01682

The graphical Comparison of evaluated BER and PSNR is shown in Fig 1.

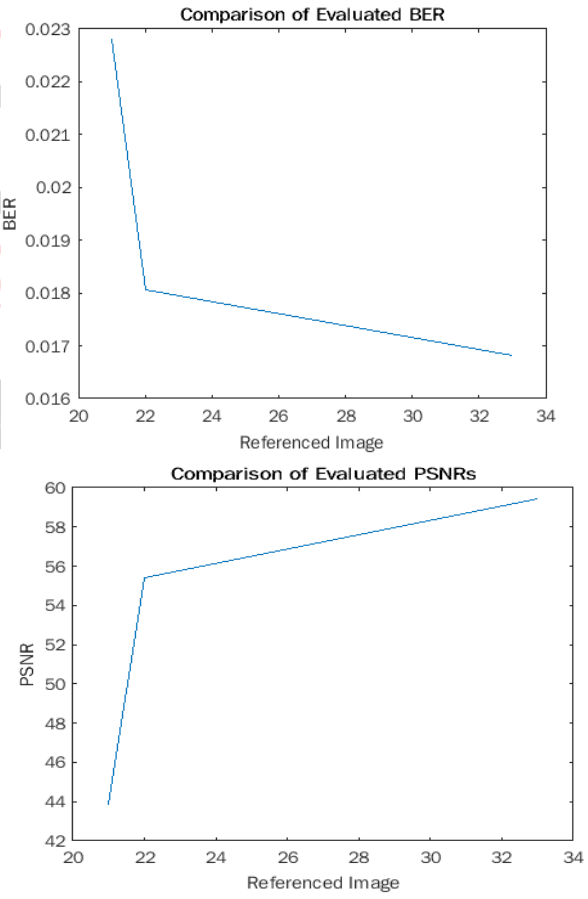


Fig 1. Graphical Comparison of evaluated BER and PSNR

 DOI : 10.35291/2454-9150.2022.0034

TABLE I : DEFINITIONS OF PERFORMANCE EVALUATION PARAMETERS

Performance Evaluation Parameters		Definitions	Equations/Observations
Performance Measures	**Performance Metrics**		
Statistical Analysis	Entropy Analysis	-Entropy is an important analysis to evaluate the uniform distribution of grayscale values. -To yield better security, entropy of encrypted image must be close to 8 in case of 8-bit medical image.	$H = -\sum_{i=1}^{N} P(x_i)\log_2 P(x_i)$
	Histogram Analysis	-Histogram analysis is used as a tool in image analysis to evaluate frequency distribution of pixel values. -A robust image encryption algorithm ought to have a uniform distribution of pixel values from cipher images to guarantee to withstand statistical attacks.	Concerning histogram analysis, if each cipher images are dispersed uniformly, it means that each cipher image is very different from plain image. So, it will be very difficult to guess actual information for any attacker or adversary-.
	Correlation Analysis	-Correlation is another measure to judge the randomness. -It has three coefficients namely horizontal, vertical and diagonal which are calculated using the mathematical equations. -To justify that the encryption is good, correlation coefficient values must be close to zero.	$E(x) = \frac{1}{N}\sum_{i=1}^{N} x_i$ $D(x) = \frac{1}{N}\sum_{i=1}^{N} (x_i - E(x))^2$ $Cov(x,y) = \frac{1}{N}\sum_{i=1}^{N} (x_i - E(x))(y_i - E(y))$ $\gamma_{xy} = \frac{Cov(x,y)}{\sqrt{D(x)}\sqrt{D(y)}}$
	SSI Analysis	-SSI is used for measuring the similarity between two images. -It is also defined as a method for predicting the perceived quality of an image based on an initial uncompressed or distortion-free image as reference. -It is also referred as a perceptual metric that quantifies the image quality degradation such as data compression or by losses in data transmission.	$SSI = \frac{(2\,\text{mean}(A*B)+c1)(2\,con(A*B)+c2)}{(\text{mean}(A^2)+\text{mean}(B^2)+c1)(con(A^2)+con(B^2)+c2)}$
Differential Attack Analysis	NPCR, UACI	-The differential attack examines how well the ciphertexts will influence the difference between plaintexts. -Differential attack can be effectively measure in the encryption mechanism with the help of NPCR (number of pixels change rate) and UACI (uniform average change intensity) quantitiated values of the image. -NPCR and UACI are also called as differential analyses. These are used to evaluate the encrypted images with keys to find the average pixel changes.	$UACI = \frac{\sum_{k=1}^{H*W} \lvert C1(i,j) - C2(i,j)\rvert}{H \times W \times 255} \times 100\%$ $NPCR = \frac{\sum_{i,j} D(i,j)}{M \times N} \times 100$ $D(i,j) = \begin{cases} 0 & \text{if } C_1(i,j) = C_2(i,j) \\ 1 & \text{if } C_1(i,j) \neq C_2(i,j) \end{cases}$

TABLE I (Continued)

Performance Evaluation Parameters		Definitions	Equations/Observations
Performance Measures	**Performance Metrics**		

 DOI : 10.35291/2454-9150.2022.0034

Error Metric Analysis	MSE	-Mean Square Error (MSE) and Peak Signal to Noise Ratio (PSNR) are error metrics to compare image compression quality. -MSE refers to the cumulative squared error between compressed and original image, where as PSNR measures the peak error. -The lower the MSE, the lower the error. -Root Mean Square Error (RMSE) merit is used to measure the robustness and strength of the compressed images. -BER represents the percentage of bits that have errors relative to the total number of bits received in transmission.	$RMSE = \frac{1}{\sqrt{MN}} \sum_{i=0}^{M-1} \sum_{j=0}^{N=1} \|\|(O(i,j) - O'(i,j)\|\|^2$ $PSNR = 20 \log \left(\frac{Emax}{MSE} \right)$
	PSNR		
	BER		BER=1/PSNR
Key Analysis	Key Space Analysis	-The key space is the set of all valid, possible, distinct keys of a given cryptosystem.	-The larger key space will provide protection against Brute-force attack.
	Key Sensitivity Analysis	-An ideal image encrypt ion procedure should be sensitive to the secret key.	It means that a little bit change in a secret key should produce completely different image.
Computational Analysis	Encryption /Signcryption Time	-Computational Analysis determines the Encryption, Signcryption, Decryption, Response and Delay time. It also deals with the measure of Throughput and Energy/Power consumption.	An efficient algorithm will provide less computation overhead.
	Decryption Time		
	Throughput		
	Response Time		
	Delay Time		
Data loss & Noise Analysis	Visual Quality Analysis	-Data that is transferred over noisy channels gets easily corrupted by noise or data loss. Consequently, it is essential for a well-designed image encryption scheme to be robust enough in order to resist noise and data loss attacks. -To evaluate the capability of image encryption mechanism, to resist the attacks of noise and data loss, perform a data cutting block with a size of 30 × 30 (60 × 60) or add 1% (10%) Salt & Pepper noise to the cipher images, and then decrypt it. -By adding noise, the decrypted images have good visual quality with no loss for the visual information within the position of the cutting part.	A visual quality of a data need to be maintained

TABLE II: Summary of Evaluated Parameters

Ref	Parameters evaluated	Results	Research Gaps/Future Work
[21]	Entropy, correlation, NPCR,UACI,MSE,PSNR	-To yield better security, the entropy of encrypted image must be close to 8 in case of 8-bit medical image. - The encryption was a mere AES which has yielded approximate entropy of 7.33 only but can be improved by few rounds of diffusion operations.	-Encryption is performed by the server, only when the request for data arrives at the server. –To provide security to the data, the data should be stored in an encrypted format in the server. -Future work includes developing a crypto stego model for medical images with chaos based encryption on reconfigurable hardware platform.
[22]	RMSE, PSNR	- Results have shown that PSNR value above 47.9 dB is maintained and thereby verify that the proposed SBPG architecture provides high quality watermarking along with better compression compared to JPEG. -Improvement after decompression in the visual quality of the watermarked and compressed images with larger PSNR values confirms the strength of the proposed SBPG encoder in maintaining the quality of the watermarked images and making it impossible for the human eye to detect the signatures of the Watermarks in the images. -Higher values of PSNR demonstrate the quality of the images compressed with SBPG as well as the attack resilience and consequent robustness of the	- It focused only on the authenticity of watermarked image, there by an unencrypted image is send without security -Future work includes modifications to other types of medical data as well as development of highly energy-efficient architectures for SBPG and novel IoT based smart applications of SBPG for disaster relief, emergency management, crime detection and prevention, etc.
[24]	Information Entropy, NPCR, UACI, Histogram Analysis, Correlation	-Simulation results and security analysis acknowledge that proposed mechanism has high security standard to secure any adversary or attacker in the smart healthcare IoT system. -Entropy calculated is 7.99955 which is closer to 8.	-. -For future work security aspect need to be implemented to protect digital medical data in smart healthcare system..

 DOI : 10.35291/2454-9150.2022.0034

	Analysis, Key Analysis	-NPCR is evaluated to 99.9976 and UACI is evaluated to 33.3281. This indicates that our proposed mechanism has strong ability to resist various types of differential attacks. - Proposed approach has approximately very near to 8 value of entropy which indicated that proposed approach has provided uncertainty and randomness in the cipher images. -Concerning histogram analysis each cipher images are dispersed uniformly. It means each cipher image is very different from plain image. So, it will be very difficult to guess actual information for attacker or any adversary. -Correlation analysis shows that there is no relation among the adjacent pixels which is nearly zero whether positively or negatively in the values. This demonstrated that the proposed method has nearly zero correlation coefficient which showed dispersed actual relationship that have plain image. -256 key length to defend any adversary or attack. This 256-bit length key is extremely sensitive as well secure to protect smart healthcare system.	-Other Cryptographic algorithms need to be explored and comparative analysis is required.
[27]	Correlation analysis, Pixel change rate, Histogram analysis, Information Entropy, Data loss and noise analysis, key space and key sensitivity analysis.	- Results show that no significant beneficial knowledge can be gained about the plain image by correlations analysis for cipher images. - Histograms of different plain gray-scale images are of various shapes while the distributions of their analogous cipher ones are uniform with each other. Consequently, the proposed image encryption scheme could withstand attacks based on histogram analysis. - The evaluated entropy values of the encrypted Images are very near to 8-bit.Therefore, the designed encryption mechanism is secure against entropy attacks. - By adding noise, the decrypted images have good visual quality with no loss for the visual information within the position of the cutting part. - The key space for the presented image encryption mechanism is 10^{160}, which is large enough for any encryption algorithm to resist brute-force attacks.	-When compared theoretically be used to break all existing implementations of asymmetric cryptography, such as- RSA, Diffie-Hellman and Elliptic Curve cryptography. -Moreover, quantum computing would affect symmetric cryptography by requiring a slightly larger secret key.

[28]	Computational complexity, Information Entropy Analysis, Differential Attack Analysis-NPCR,UACI, Statistical Attack Analysis-Histogram Analysis, Correlation Analysis, Key space analysis, Comparative Analysis with existing	- Resulted in a minimum computation with faster run time. - The entropy results of each color channel (R, G, B) of key frame encrypted images are very similar to 8. This demonstrates that the proposed CTC-IES has delivered the appropriate degree of security and randomness against the entropy attack. - The diffusion feature demonstrates that the cipher image could disperse a slight change throughout the plain image over the whole information or data. The proposed mechanism shows the resistance to differential attack analysis. - The histogram analysis demonstrates that the proposed CTC-IES algorithm avoids the numerical or statistical attacks and thereby confirmations consistency, integrity in the communication. - Results show that the neighboring pixels in the original keyframe images are strongly (highly) correlated in vertical, horizontal, and diagonal directions, whereas the neighboring pixels are correlated weakly in the all three directions in the encrypted keyframe images. This demonstrates that the proposed CTC-IES is highly resistant to a statistical attack in the smart healthcare IoT ecosystem. - The CTC-IES key space is 2^{256}, which meets the key performance necessities and it is highly effective in avoiding different types of security attacks. -When compared with other existing approaches , the proposed approach has fast speed in execution, comparable better entropy, lowest correlation coefficient, acceptable NPCR and UACI values, which is firmly indicated that proposed work has highly acceptable in the field of cryptographically secure surveillance on smart healthcare IoT ecosystem.	- For future work, it can be carried out to integrate information from other systems, for many applications, as well as further advance security aspect such as access control, privacy measures. -New direction can also be possible to implement dynamic secure key instead of implemented method for further enhancing security and privacy

 DOI : 10.35291/2454-9150.2022.0034

[29]	Signcryption time	The proposed system takes 8.75 ms to signcrypt the message which is less time when compared to the Identity based Signcryption system.	-The proposed hybrid Signcryption system is implemented to provide security to the data as well as key. It is strong against SUF-CMA, EUF-CMA attacks, in specific EUF CMA, but the UUF-CMA attacks are possible to the proposed hybrid lightweight Signcryption system
[32]	Energy consumption, throughput, Response time, Delay time, Encryption time, Decryption time, Execution time	-If the data sizes are increased, key size and number of rounds are increased. - For every round in data sizes the throughput value reduced. - Encrypted and decrypted time minimizes in the proposed model (SIMON Optimal share creation) compared to KATAN and SIMON. - In the proposed security model the execution time is reduced for every data sizes. - Optimal CRT depicts maximum security level as 65–95% for several blocks compared to other techniques. - In our proposed hybrid model (HTLBO) energy is minimized for every iteration.	-For further investigations, the detailed implementation of the algorithms can be studied with different measures by using innovative data encryption methods with the hybrid optimization approach. This will be pertinent to various applications in cloud data security under threats/attacks condition.
[33]	PSNR,SSI,MSE,BER	The highest PSNR of the test images is 59.45 dB and comparatively higher than MSE and BER which are 0.09 and 0.01 with the most extreme SSI being 1. - The proposed RSA and ECC with GO + PSO strategy decreases the encryption and decryption time when compared with an existing technologies.	-Procedure used is not secure enough as it never furnished great impalpability -Future work should focus on tamper localization as opposed to strict integrity executed in the current algorithms

Table III. Study of Performance Evaluation Parameters

Performance Evaluation Parameters		**References**							
Performance Measures	**Performance Metrics**	**[21]**	**[22]**	**[24]**	**[27]**	**[28]**	**[29]**	**[32]**	**[33]**
Statistical Analysis	Correlation Analysis	√		√	√	√			
	Histogram Analysis			√	√	√			
	Entropy Analysis	√		√	√	√			
	SSI Analysis								√
Differential Attack Analysis	NPCR	√		√	√	√			
	UACI	√		√		√			
Error Metric Analysis	MSE	√	√						√
	PSNR	√	√						√
	BER								√
Key Analysis	Key Space Analysis			√	√	√			

TABLE IV: Observations

Performance Evaluation Parameters		**References**							
Performance Measures	**Performance Metrics**	**[21]**	**[22]**	**[24]**	**[27]**	**[28]**	**[29]**	**[32]**	**[33]**
Statistical Analysis	Correlation Analysis	not calculated		not calculated	0.0002	0.0015			
	Histogram			done	done	done			

 DOI : 10.35291/2454-9150.2022.0034

	Analysis								
	Entropy Analysis	7.33		7.9955	7.9981	7.9991			
	SSI Analysis								1
Differential Attack Analysis	NPCR	99.9771		99.9976	99.6197	99.6212			
	UACI	59.4473		33.3281		33.4406			
Error Metric Analysis	MSE/RMSE	809.1511	0.92						0.09
	PSNR	43.8654 dB	55.4 dB						59.45dB
	BER								0.01
Key Analysis	Key Space Analysis			2^{256}	10^{160}	2^{256}			
	Key Sensitivity Analysis				done				
Computational Analysis	Encryption /Signcryption Time					0.2811-0.3119	8.75ms	not specified	
	Decryption Time							not specified	
	Throughput							√	
	Response Time							2.52s	
	Delay Time							2.88s	
	Energy Consumption							3.22 PJ/bit	

Table V. Summary of Related Work

Ref	Title	Year	Scheme	Methodology	Observation	Implementation
[21]	IoT Framework For Secure Medical Image Transmission	2018	Server– Client	AES	Provide authentication to access a medical image. DICOM image encryption using AES and OTP authenticated medical image verification performed by a server-client model.	Python 2.7
[22]	SBPG: Secure Better Portable Graphics For Trustworthy Media Communications in the IoT	2018	SDC with integrated SBPG compression algorithm	AES, watermarking using block wise DCT	Provides the authenticity of origin of data, providing patient data protection and authentication by employing the techniques of encryption, watermarking using block-wise DCT of size 8 x 8 pixels and SBPG Compression. The proposed architecture reduces computational complexity while provide strong protection.	Simulink prototype for the proposed architecture is built and tested.
[24]	Medical Image Encryption into Smart Healthcare IOT System	2020	Encryption by means of scrambling and diffusion	High Speed Scrambling and Pixel Adaptive diffusion using Arithmetic Modulo Operation	Provides security to medical images by means of a proposed Encryption Algorithm which uses high speed scrambling and diffusion.	MATLAB
[27]	Controlled Alternate Quantum Walks based Privacy Preserving Healthcare images in Internet of Things	2019	Quantum Computing	Controlled Alternate Quantum Walks(CAQWS)	The encryption algorithm proposed is to preserve the privacy of health care images in IoT environments, by applying the substitution and permutation based on CAQWs	MATLAB, gray scale and color images
[28]	SMSH: Secure Surveillance Mechanism On Smart Healthcare Iot System With Probabilistic Image Encryption	2017	Wireless Multimedia Surveillance Networks(WMSN)	Probabilistic Image Encryption, Cosine Transform –based chaotic sequence	Patient's privacy is preserved by proposing a secure Surveillance Mechanism with Probabilistic Image Encryption in Smart Healthcare IoT System	Tensor Flow, python, lightweight YOLOv3 Algorithm and MATLAB

 DOI : 10.35291/2454-9150.2022.0034

[29]	Hybrid Lightweight Signcryption Scheme for IoT	2021	Hybrid Signcryption scheme	PRESENT, ECC	A hybrid Signcryption is proposed that employs PRESENT, a lightweight block cipher algorithm to encrypt the data, and the session key is encrypted by ECC	Raspberry Pi3 B model, Python
[32]	Optimal Users Based Secure Data Transmission On The Internet Of Healthcare Things(Ioth) With Lightweight Block Ciphers	2019	Encryption and Optimization	SIMON,CRT ,HTLBO	Provide security to Healthcare data by encrypting using SIMON block Cipher and for ensuring the privacy of healthcare data among individuals, share generation model is implemented using Chinese Remainder Theorem(CRT). The selection of users is made by metaheuristic algorithm called Hybrid Teaching and Learning Based Optimization(HTLBO). This scheme provides full scope of medical services to people enrolled in IoTH.	Net beans with JAVA Programming Language JDK 1.7.0
[33]	Hybrid optimization with cryptography encryption for medical image security in Internet of Things	2018	Hybrid Encryption Algorithm	ECC with PSO and GO	Proposed a Hybrid Encryption model that combines Cryptographic model with optimization strategies.	MATLAB

RESEARCH METHODOLOGY

A. Problem Gap

The data protection and privacy issues related to the patient are two essential features. With data security, data privacy is available only to those who have the right to view and use the data, ensuring that their data is stored and transmitted in a secure, comprehensive, valid and reliable manner. The most reasonable security strategies can be designed to meet different needs and requirements. While most healthcare companies do not spend enough resources to protect safety and privacy, there is no doubt that security and privacy play an important role in the Internet of Things.

B. Research Objectives

To overcome the above mentioned problems, we concentrate to propose novel crypto scheme. The main objectives of proposed scheme are listed as follows:

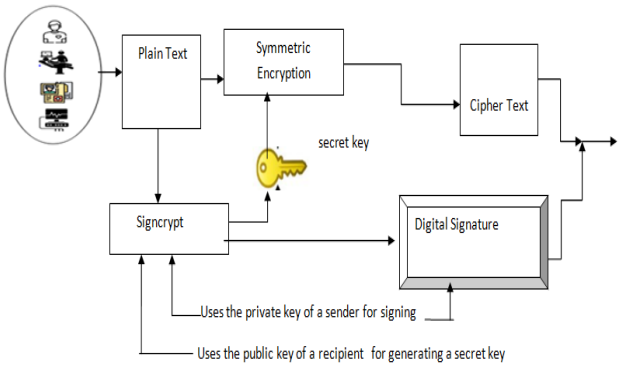
1. To investigate and implement an efficient key exchange and authentication algorithm for healthcare data security in IoT.
2. To implement an optimization algorithm to select optimal best key for data encryption and decryption among multiple keys.
3. To build an optimal hybrid lightweight signcryption model that provide perfect forward secrecy with high efficiency.
4. To perform a comparative analysis, to show the effectiveness of the proposed scheme.

C. Proposed Research Design

Motivated by the contributions made by authors in [29], [32], [33], a research design is proposed.

1) Signcryption Mechanism

In Signcryption, digital signature and encryption function are performed in parallel, thereby providing confidentiality, integrity and non-repudiation. Traditionally, in public-key schemes, a message to be send is signed first and then encrypted. This process found to have low efficiency, high cost of summation and not guaranteeing strong security. Signcryption is proposed as a new cryptographic technique which performs the functions of digital signature and encryption in a single logical step and can effectively decrease the computational costs and communication overheads in comparison with the traditional signature-then-encryption schemes. Fig 11 shows Signcryption done at sender and recipient side.



a. At Sender Side

 DOI : 10.35291/2454-9150.2022.0034

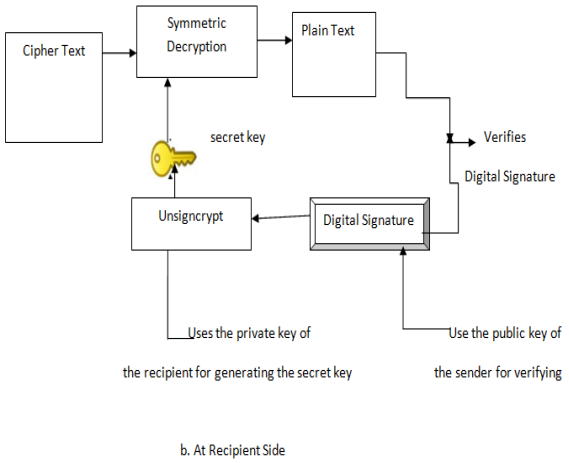


Fig 2. .Signcryption at Sender and Recipient side

2) Lightweight Cryptography

Lightweight Cryptography is implemented in IoT, which encompasses resource-constrained devices, with tailored Substitution and Permutation boxes and the number of gate equivalents are very low when compared with traditional cryptographic techniques. Lightweight Cryptography is lightweight in terms of both software with small S and box and P box, and hardware with less amount of gate equivalence required. Low power security protocols are an effective security solution for resource constrained environment like IoT, which are provided by lightweight cryptographic algorithms [29].

3) Optimization Approach

The strength of any cryptographic algorithm depends on a stronger key. The key space should be large enough so that it can resist any brute-force attack. The generation and selection of a key is one of the major step in cryptography and this problem of selecting a best key from a given keyspace is referred as optimization problem and the best key which is selected is called as optimal key. Recently study advances have been made to use Metaheuristic algorithms to generate optimal keys for encryption. Metaheuristics are strategies that guide the search process. The goal is to explore the search space in order to find the optimal solution[35]. Therefore, Metaheuristic algorithms considered to provide a good or optimal solution to an optimization problem.

4) Hybrid Approach

Hybrid Approach involves the combination of various security mechanisms listed below:

a) Hybrid Signcryption

Signcryption ensures confidentiality, integrity and non-repudiation in single step, by combining both Symmetric and Asymmetric cryptographic techniques, a hybrid signcryption is a good approach towards a stronger encryption. Symmetric approach is less time-consuming but the security of secret/symmetric key is taken into consideration. The Asymmetric approach is much stronger but time consuming than symmetric approach. Hybrid Encryption combines the advantage of both symmetric and asymmetric approaches.

b) Hybridization of Metheuristic Algorithms with Lightweight Signcryption

With this approach, metaheuristic or optimization algorithms can be utilized for key generation/selction and exchange process in the signcryption scheme, thereby providing solution with minimum computation time.

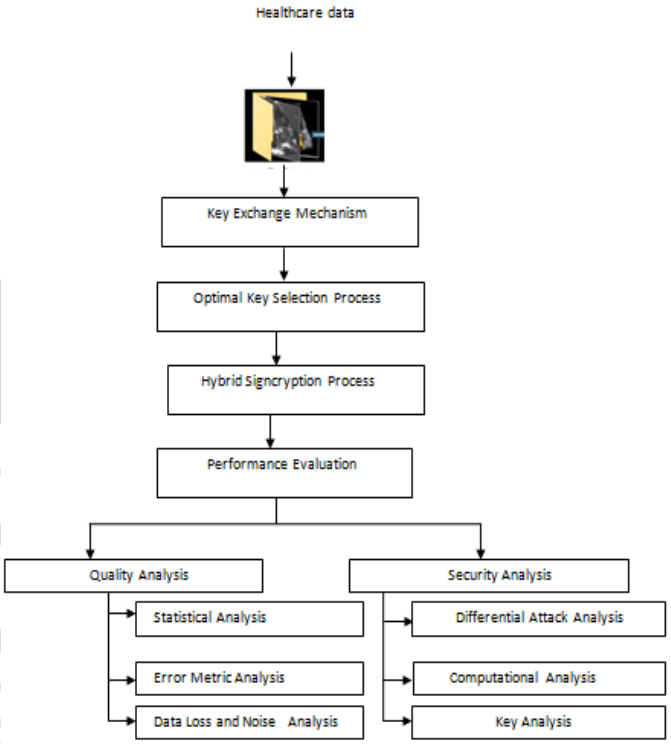


Fig 3.Proposed Research Design

CONCLUSION

Based on the study made by different authors, it is observed that how different security mechanisms are employed to provide security to medical data. It has been observed that Lightweight encryption algorithm utilizes very less hardware resources and is suitable for encrypting the data collected from resource constrained devices. Authentication and data integrity also play an important role in solving the security and privacy issues, that can be achieve by using an appropriate Digital Signature scheme. Together encryption and Signature mechanism refers to Signcryption which ensures confidentiality, integrity and non-repudiation in a single step. Optimization algorithm must be implemented to augment the security by selecting the optimal key and promoting an optimal key exchange. Future work will be carried on proposing a Hybrid Optimal Signcrytion scheme and performing a comparative analysis with the existing approaches.

 DOI : 10.35291/2454-9150.2022.0034

REFERENCES

[1]Alvarez, G., Li, S. and Hernandez, L., 2007. Analysis of security problems in a medical image encryption system. *Computers in Biology and Medicine*, *37*(3), pp.424-427.

[2]Lim, E.Y., 2008. Data security and protection for medical images. In *Biomedical information technology* (pp. 249-257). Academic Press.

[3]Li, S., Li, C., Chen, G. and Lo, K.T., 2008. Cryptanalysis of the RCES/RSES image encryption scheme. *Journal of Systems and Software*, *81*(7), pp.1130-1143.

[4]Cheddad, A., Condell, J., Curran, K. and McKevitt, P., 2010. A hash-based image encryption algorithm. *Optics communications*, *283*(6), pp.879-893.

[5]Bouslimi, D., Coatrieux, G. and Roux, C., 2012. A joint encryption/watermarking algorithm for verifying the reliability of medical images: application to echographic images. *Computer methods and programs in biomedicine*, *106*(1), pp.47-54.

[6]Som, S. and Sen, S., 2013. A non-adaptive partial encryption of grayscale images based on chaos. *Procedia Technology*, *10*, pp.663-671.

[7]Pareek, N.K., Patidar, V. and Sud, K.K., 2013. Diffusion–substitution based gray image encryption scheme. *Digital signal processing*, *23*(3), pp.894-901.

[8]Volos, C.K., Kyprianidis, I.M. and Stouboulos, I.N., 2013. Image encryption process based on chaotic synchronization phenomena. *Signal Processing*, *93*(5), pp.1328-1340.

[9]Li, X.W., Cho, S.J. and Kim, S.T., 2014. High security and robust optical image encryption approach based on computer-generated integral imaging pickup and iterative back-projection techniques. *Optics and Lasers in Engineering*, *55*, pp.162-182.

[10] Naeem, E.A., Abd Elnaby, M.M., Soliman, N.F., Abbas, A.M., Faragallah, O.S., Semary, N., Hadhoud, M.M., Alshebeili, S.A. and Abd El-Samie, F.E., 2014. Efficient implementation of chaotic image encryption in transform domains. *Journal of Systems and Software*, *97*, pp.118-127.

[11] Isa, M.A.M., Ahmad, M.M., Sani, N.F.M., Hashim, H. and Mahmod, R., 2014. Cryptographic key exchange protocol with message authentication codes (mac) using finite state machine. *Procedia Computer Science*, *42*, pp.263-270.

[12] Tedmori, S. and Al-Najdawi, N., 2014. Image cryptographic algorithm based on the Haar wavelet transforms. *Information Sciences*, *269*, pp.21-34.

[13] Mohamed, F.K., 2014. A parallel block-based encryption schema for digital images using reversible cellular automata. *Engineering Science and Technology, an International Journal*, *17*(2), pp.85-94

[14] Liu, H. and Liu, Y., 2014. Security assessment on block-Cat-map based permutation applied to image encryption scheme. *Optics & Laser Technology*, *56*, pp.313-316.

[15] Jolfaei, A., Wu, X.W. and Muthukkumarasamy, V., 2014. Comments on the security of "Diffusion–substitution based gray image encryption" scheme. *Digital signal processing*, *32*, pp.34-36

[16] Lima, J.B., Madeiro, F. and Sales, F.J., 2015. Encryption of medical images based on the cosine number transform. *Signal Processing: Image Communication*, *35*, pp.1-8.

[17] Nagaraj, S., Raju, G.S.V.P. and Rao, K.K., 2015. Image encryption using elliptic curve cryptograhy and matrix. *Procedia Computer Science*, *48*, pp.276-281.

[18] Shankar, K. and Eswaran, P., 2015. Sharing a secret image with encapsulated shares in visual cryptography. *Procedia Computer Science*, *70*, pp.462-468.

[19] Kanso, A. and Ghebleh, M., 2015. An efficient and robust image encryption scheme for medical applications. *Communications in Nonlinear Science and Numerical Simulation*, *24*(1-3), pp.98-116.

[20] Chen, J.X., Zhu, Z.L., Fu, C., Zhang, L.B. and Zhang, Y., 2015. An image encryption scheme using nonlinear inter-pixel computing and swapping based permutation approach. *Communications in Nonlinear Science and Numerical Simulation*, *23*(1-3), pp.294-310.

[21] Rajagopalan, S., Janakiraman, S., Rengarajan, A., Rethinam, S., Arumugham, S. and Saravanan, G., 2018, January. IoT framework for secure medical image transmission. In *2018 international conference on computer communication and informatics (ICCCI)* (pp. 1-5). IEEE.

[22] Mohanty, S.P., Kougianos, E. and Guturu, P., 2018. SBPG: secure better portable graphics for trustworthy media communications in the IoT. *IEEE Access*, *6*, pp.5939-5953.

[23] Al-Shayea, T.K., Mavromoustakis, C.X., Batalla, J.M. and Mastorakis, G., 2019. A hybridized methodology of different wavelet transformations targeting medical images in IoT infrastructure. *Measurement*, *148*, p.106813.

[24] Khan, J., Li, J., Haq, A.U., Parveen, S., Khan, G.A., Shahid, M., Monday, H.N., Ullah, S. and Ruinan, S., 2019, December. Medical Image Encryption into Smart Healthcare IOT System. In *2019 16th International Computer Conference on Wavelet Active Media Technology and Information Processing* (pp. 378-382). IEEE.

[25] Wang, J., Han, K., Fan, S., Zhang, Y., Tan, H., Jeon, G., Pang, Y. and Lin, J., 2020. A logistic mapping-based encryption scheme for Wireless Body Area Networks. *Future Generation Computer Systems*, *110*, pp.57-67.

[26] Sangavi, V. and Thangavel, P., 2020. An exotic multi-dimensional conceptualization for medical image encryption exerting Rossler system and Sine map. *Journal of Information Security and Applications*, *55*, p.102626.

[27] Abd EL-Latif, A.A., Abd-El-Atty, B., Abou-Nassar, E.M. and Venegas-Andraca, S.E., 2020. Controlled alternate quantum walks based privacy preserving healthcare images in internet of things. *Optics & Laser Technology*, *124*, p.105942.

[28] Khan, J., Li, J.P., Ahamad, B., Parveen, S., Haq, A.U., Khan, G.A. and Sangaiah, A.K., 2020. SMSH: secure surveillance mechanism on smart healthcare IoT system with probabilistic image encryption. *IEEE Access*, *8*, pp.15747-15767.

[29] M.Sruthi and Rajkumar Rajasekaran, Hybrid Lightweight Signcryption Scheme for IoT, Open Computer Science, 2021; 11:391-398

[30] Ren, W., Tong, X., Du, J., Wang, N., Li, S.C., Min, G., Zhao, Z. and Bashir, A.K., 2021. Privacy-preserving using homomorphic encryption in Mobile IoT systems. *Computer Communications*, *165*, pp.105-111.

[31] Sun, X., Wang, H., Fu, X., Qin, H., Jiang, M., Xue, L. and Wei, X., 2021. Substring-searchable attribute-based encryption and its application for IoT devices. *Digital Communications and Networks*, *7*(2), pp.277-283.

[32] S.Sheeba Rani, Jafar A.Alzubi, S.K. Lakshmanaprabu, Deepak Gupta, Ramachandran Manikandan, Optimal users based secure data transmission on the internet of healthcare things(IoTH) with lightweight block ciphers, Multimedia Tools and Applications, Springer 2019

[33] Elhoseny, M., Shankar, K., Lakshmanaprabu, S.K., Maseleno, A. and Arunkumar, N., 2020. Hybrid optimization with cryptography encryption for medical image security in Internet of Things. Neural computing and applications, 32(15), pp.10979-10993

[34] K. Sambasiva Rao, M. Kameswara Rao A Lightweight Digital Signature Generation Mechanism for Authentication of IoT Devices International Journal of Recent Technology and Engineering (IJRTE) ISSN: 2277-3878, Volume-7, Issue-6, March 2019

[35] M.Gita, K.Akila, Survey : Cryptography Optimization Algorithms, IJISCS, 2018

[36] K.Doke, Kanchan & Patil, Shankar. (2012). Digital Signature Scheme for Image. International Journal of Computer Applications. 49. 1-6. 10.5120/7708-1012.

 DOI : 10.35291/2454-9150.2022.0034