ECTI Transactions on Computer and Information Technology
Journal homepage: https://ph01.tci-thaijo.org/index.php/ecticit/
Published by the ECTI Association, Thailand, ISSN: 2286-9131

Hybrid Visual and Optimal Elliptic Curve Cryptography for Medical Image Security in Iot

L. Ashok Kumar[1*], Sumit Srivastava[2], Balaji S. R.[3] , Francis H Shajin[4] and P. Rajesh[5]

ABSTRACT

In this manuscript, a hybridizing visual cryptography with Optimal Elliptic Curve Cryptography is proposed for medical image security in Internet of Things (IoT). The visual cryptography is generally used to send the secure and confidential medical image to the receiver. Here, the medical image is transmitted as shares and all shares of the medical image are collectively loaded to retrieve the original medical image. Moreover, the multiple shares are created interms of pixel values of medical image and this share is extracted and partioned in blocks. The blocks of every share are encrypted with elliptic curve cryptography (ECC) mechanisms and encrypted image is decrypted using ECC decrypts. In hybridizing visual crypto with optimal elliptic curve crypto, the optimal key will be generated using an imperialist competitive algorithm. Finally, the decrypted output image compares to the original image. The proposed system is executed on MATLAB platform and performance is evaluated with existing method like Score-based Key Enumeration Algorithm (SKEA). The proposed ESEA approach reduces the file size as 45.76%, 24.97%, 15.86%, 33% and 33.86%.And higher PSNR as 29.08%, 25.86%, 23.98%, 25.86% and 42.75%. The proposed ESEA approach achieves 6.89% higher security than existing SKEA method. Furthermore, the simulation outcome demonstrates that the proposed technique can be able to find the optimal global solutions efficiently and accurately than the existing techniques.

Article information:

Keywords: Encryption, Elliptical Curve Cryptography, Visual Cryptography, Imperialist Competitive Algorithm, Decryption

Article history:
Received: February 16, 2021
Revised: June 14, 2021
Accepted: December 6, 2021
Published: August 20, 2022
(Online)

DOI: 10.37936/ecti-cit.2022163.246991

1. INTRODUCTION

Nowadays, the Internet is used in everywhere [1-3]. So, the Internet of things makes to build the communication circumstances in interconnected devices and stages to concentrate practical and substantial world [4,5]. The IoT deals several intelligent devices such as sensors, and associated actuators to manage physical conditions and human frame work [6,7]. An IoT plays an important role in innovative and creative arrangements for using the internet. IoT provides telemedicine in the information technology with the help of sensors and systems, also used to assign the knowledge of the patient with the collaboration with remote professionals [8-10]. IoT security and data integrity is used to examine the real importance of IoT [11]. Patient satisfaction and home treatment provide the medical service provider plays an important role in the medical field. IoT is the central part of the various therapeutic devices, sensors, analytical and imaging devices. In this method, the security and reliability of symptomatic data of patients are not achieved clearly. The path messages are encoded in the Encryption Cryptography [12,13].

In this process, the programmers cannot read the data and can be approved to available faculty [14].

[1*]The author is with Department of Electronics and Communication Engineering, Panimalar Institute of Technology, Poonamallee, Chennai - 600 123, Tamilnadu, India., E-mail: : ashok2002ttd@gmail.com
[2]The author is with Department of Electronics and Communication Engineering, FET, MJP Rohilkhand University Bareilly, India., E-mail: arsvns1@gmail.com
[3]The author is with Department of Electronics and Communication Engineering, Panimalar Engineering College, Poonamallee, Chennai - 600 123, Tamilnadu, India., E-mail: balasrb2000@gmail.com
[4]The author is with Department of Electronics and Communication Engineering, Anna University, Chennai, Tamilnadu, India., E-mail: shajin.mt@gmail.com
[5]The author is with Department of Electrical and Electronics Engineering, Anna University, Chennai, Tamilnadu, India., E-mail: rajeshkannan.mt@gmail.com

To decrease this problem, the two major algorithms are used to encrypt the data link in the task, the algorithm is advanced Encryption standard algorithm (AES) [15] or Rivest-Shamir-Adleman (RSA) [16]. Remote health observation provides promotion of several restorative applications in IoT. For instance, to evaluate the conditions of the patient to recognize the treatment as an optimal intercession in earlier stage [17]. The safety indicates the treatment of patients using the traditional system and to bind the devices in IoT. This method is detailed by using the coding and decoding process and to avoid the breaking of long keys while taking photos. Business and individual is used in the communication process and calculated by using the RSA method in open key [18]. This method aims to perform the safety measures of patient with wireless sensor network and encrypting the data. IoT security provides strengthened to the investigators and to provide the keys to optimal imperialist to develop a competitive, several techniques are enhanced[19].

In this manuscript, the hybridization of visual cryptography with optimal elliptic curve cryptography is proposed for the security of medical images on Internet of Things (IoT). Elliptic Curve Cryptography (ECC) is more complex and also maximizes the possibility of execution errors, thus dropping image security. The ECC also maximizes the size of encrypted message concurrently. To overcome the drawback of ECC a hybrid technique is introduced. The proposed technique is the joint execution of Visual cryptography and Elliptical curve cryptography (ECC) [20]. It also has some drawbacks that is visual cryptography sends an original image with multiple shares at that time the shares are encrypted in the transmitter side and decrypted in the receiver side. When encrypting processes take place a key generated known as the public key prime numbers in random and in decrypting the key generation generate private key will not able to generate the key randomness [21,22]. So, there is a hybrid technique is needed to avoid this problem, for that joint execution of Visual cryptography and Elliptical curve cryptography (ECC) is proposed.

The main contribution of this manuscript is summarizes as follows:

- In this manuscript, a hybridization of Elliptical curve cryptography (ECC) and visual cryptography is proposed [23] for medical image security in Internet of Things (IoT).
- The visual cryptography is utilized for sending a secure and confidential medical image to the receiver. Here, the medical image is transmitted as shares and all shares of the medical image are collectively loaded to retrieve the original medical image.
- Also the multiple shares are created in terms of pixel values of medical image and this share is extracted and portioned in blocks.
- The blocks of every share are encrypted with ECC mechanisms and encrypted image is decrypted using ECC decrypts.
- In hybridizing visual crypto with optimal elliptic curve c+-rypto, the optimal key will be generated using an imperialist competitive algorithm [24].
- Finally, the decrypted output image compares to the original image.
- Finally, implementation is carried out in MATLAB platform for evaluating their performance.
- The performance is evaluated with existing method like Score-based Key Enumeration Algorithm (SKEA).

The rest of this manuscript is designed as below. Section 2 delineates that Preliminaries of Elliptical curve cryptography (ECC) and visual cryptography. Section 3 explains that Literature survey. Section 4 illustrates that Proposed Hybrid Elliptic Curve (ECC) and Visual Cryptography (VC) with ICA Optimization. Section 5 demonstrates that result and discussion. Finally, Section 6 concludes the manuscript.

2. PRELIMINARIES

2.1 Elliptic Curve Cryptography

Elliptic curve cryptography (ECC) is a public cryptography introduced independently. Information technology is growing rapidly at current with advanced technologies, but there are some restrictions while using the internet.

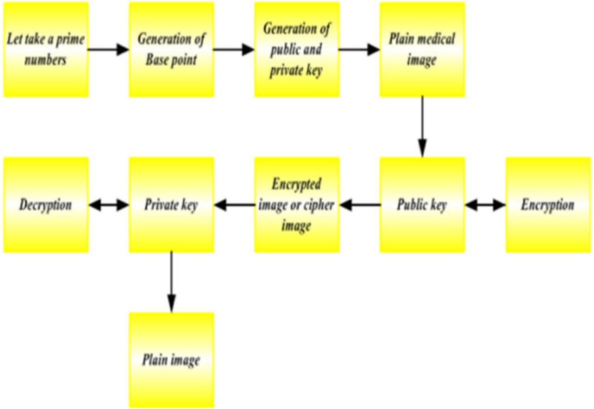


Fig.1: *Basic structure of Elliptic Curve Cryptography.*

Memory is limited, high computing power and cannot have the possibility of usage as high bandwidth for communication purpose. An ECC cryptography system is required to solve these issues with smaller keys and small signature size. So that high security level can obtain with lesser keys. Fig. 1 depicts the basic framework of ECC method.

2.2 Visual Cryptography

Visual cryptography (VC) is proposed for sharing the visual data with high security. The encryption method of real image in shared images reveals that secret message or original image, undoubtedly, after assembling an appropriate number of actions. The basics of VC and the process of transformation of VC are as follows.

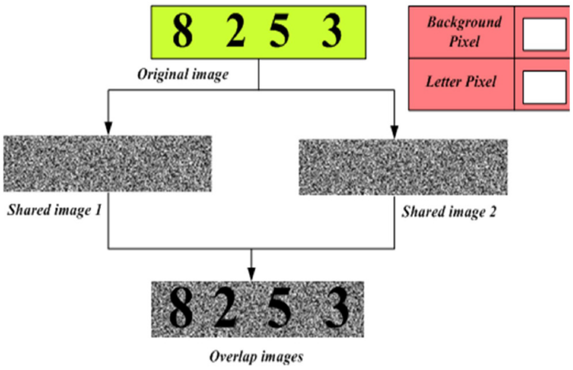


Fig.2: *Procedure for generating shared images as real image and view secret message.*

The first process is to prepare the original image with secret messages and some patterns to transform a real image. This pattern has pixels that are arranged in 2×2 arrays. The half of four pixels makes with black and remaining sub pixels are transparent. Six patterns generated based on this rule. From that two are horizontal in shape, two are vertical in shape and 2 are diagonal in shape like 2$^{\text{nd}}$ row of fig. 2.

According to VC the shared image is generated only shapes. This cryptography converts a pixel of real image to approximately any shape, such as horizontal, vertical and diagonal. Then the sub-pixels as noise with random pattern combinations have a black and white reorganization, so that image looks as a gray image for human eyes. The background pixel matrix must be followed for the conversion of background pixel on real image to one of the patterns for constructing the image as shared.

Fig. 3 shows the generation of message part of shared image with a matrix message pixel. The message pixel on real image is converted into a randomly determined diagonal pattern; the sub-pixel of first shared image must set the left diagonal pattern on same position. Another shared image must be set as an opposite shape in same position. The entire message part of the shared image is packed in this manner. The pixels in the secret message part turn black since the transparent pixels are replaced by a black pattern in another shared image and appear black.

Finally, the shared image 1 on Fig. 2 looks gray and from Fig. 2 the shared images 2 also emerge the same with initial shared image. Every shared image not at all reveals an “8253” secret message and no rules for constructing the shared image. In particular, while shared images are assembled, the human’s view may confirm the message as bottom image on Fig 2. Shared images do not match as start point to end point or message cannot be displayed if one of the shared images is distorted. Thus, VC contains minimal calculation for encryption and no computation is required for decryption.

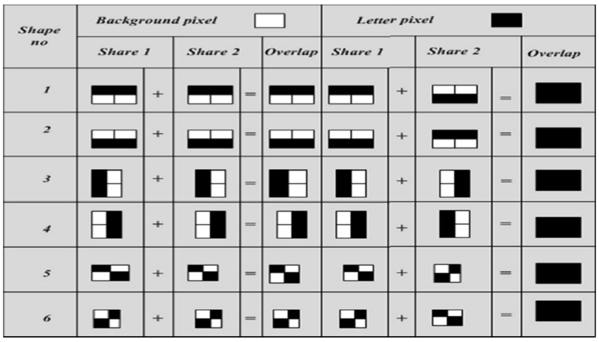


Fig.3: *Framework for pixel pattern generation in shared image.*

3. LITERATURE SURVEY

Table 1 shows the comparison table for literature review.

4. PROPOSED HYBRID ELLIPTIC CURVE (ECC) AND VISUAL CRYPTOGRAPHY (VC) WITH ICA OPTIMIZATION

In this manuscript, Hybrid elliptical curve cryptography and visual cryptography approach is proposed in the medical image security in IoT. The imperialist competitive algorithm is utilized for generating optimal key. Hybrid encryption process enhances the security of medical images and reduces the data loss at any time. Fig.4 portrays the block diagram of Proposed Hybrid Elliptic Curve (ECC) and Visual Cryptography (VC) with ICA Optimization.

Initially, the proposed Hybrid elliptical curve cryptography and visual cryptography approach generates shares from the pixel value of the secret medical image as black (B) and white (W) pixels. These pixel values are extorted from the secret medical image (BW image) and it is represented as a matrix in the form of B_M and W_M. The extorted pixel values are accustomed to generating numerous shares and that shares are alienated into blocks. Then the elliptical curve cryptography is used to encrypt the blocks of the shares and the encrypted image is decrypted by ECC decryption mechanism. Finally, the output decrypted image is compared with the original medical image.

The original (unique) pixel values of the image I is given in the following equation (1)

$$unique\ pixel = \sum (B_z + W_z) \tag{1}$$

Table 1: *comparison table for literature review.*

S.No	Author	Methodology	Advantages	Disadvantages
1	Avudaiappan et al., [25].	The dual encryption method has been utilized for the encryption of medical images. Blowfish Encryption and signcryption algorithm were used for the confirmation of the encryption structure. Opposition-based flower pollination (OFP) is also employed for upgrading the public and private keys.	The computational time was less and the power required to register was low.	The requirement of memory was high.
2	Banik et al., [26].	An Elgamal elliptic curve analog cryptosystem and Mersenne Twister pseudo-random number generator have been introduced for encrypting multiple medical images.	It solved the data expansion issue and reduced the number of calculations in elliptic curve math.	The execution time was high due to the expansion of calculation.
3	Hamza et al., [27].	A privacy-preserving chaos-based encryption cryptosystem has been introduced to protect the privacy of patients. This cryptosystem secured patient images as compromised runner. A fast probabilistic cryptosystem also utilized of medical key frames security was removed as wireless capsule endoscopy process. Also, it processes medical data with no leaking any information, therefore protecting patient privacy through permitting only authorized users to decrypt	Randomness behavior was less, which proved less computational efficiency and high security level for the key frames against various attacks. It decreased the energy, bandwidth for communication.	

S.No	Author	Methodology	Advantages	Disadvantages
4	Khari et al., [28].	Elliptic Galois cryptography protocols have been presented to encrypt the important data forms various medical sources. The Matrix XOR encoding steganography system was used for embedding the cipher data into less complex image. Adaptive Firefly was used for optimizing the assortment of coverage blocks in the image	High confidentiality, efficiency and less robustness were the advantages.	The drawbacks were high computation time and the memory required was high.
5	Koppu and Viswanatham, [29].	Self-Adaptive Gray wolf optimization (GWO) has been suggested to optimize 2-dimensional logistic chaotic mapping (2DCM). Chaos-based security has been highly reliable and effective way of image security.	The advantages were large key space, high security and high efficiency for better encryption.	It was highly sensitive for initial rules as well as parameter of system, the pseudo-random property and non-periodicity,
6	Shankar et al., [30].	Image safety model signcryption with adaptive elephant herding optimization technique was utilized for medical image security. The signcryption supports encryption and digital signature functionality at one logical step.	Confidentiality was high and the recovered image quality has been better.	The hardware complexity and robustness were high. So the computation time for encryption also high.
7	Shankar et al., [31].	The wave-based secret image exchange system has been presented by encrypted shadow images utilizing optimal HE (homomorphic encryption) method for secured image	Data loss has been less and quality of image was high after decrypted the image using this method.	Similar key was utilized in encryption and decryption process, so the attackers can easily access the data.

S.No	Author	Methodology	Advantages	Disadvantages
		transmission.		
8	Sivasankari and Krishnaveni [32].	Opposition-Based Harmony Search (OHS) Algorithm has been utilized for the generation of optimal keys. through Secret Share Cryptography (SSC) to raise the level of security. Medical images were taken to stego imaging process. Optimal Discrete Wave Transform (DWT) has been utilized for securing encryption. Daubechies coefficients (db2) were utilized for area transform in addition enhanced PSNR's continuous harmony search (CHS) was employed for improving those coefficients.	A unique secret image has recovered at receiver side shows better visual quality is an advantages of this technique.	It diminishes the nature of the decoded shading image.
9	Villanueva [33].	This paper study about the key enumeration problem, which is connected to the key recovery problem posed in the cold boot attack setting. In this setting, an attacker with physical access to a computer may obtain noisy data of a cryptographic secret key of a cryptographic scheme from main memory via this data remanence attack. Therefore, the attacker would need a key-recovery algorithm to reconstruct the secret key from it's	Trade-off between the required number of side-channel observations and the computational power of the adversary.	A new energy efficient management approach for wireless sensor networks in target tracking.

S.No	Author	Methodology	Advantages	Disadvantages
		noisy version. This attack setting is described first and then poses the problem of key recovery in a general way and establishes a connection between the key recovery problem and the key enumeration problem.		

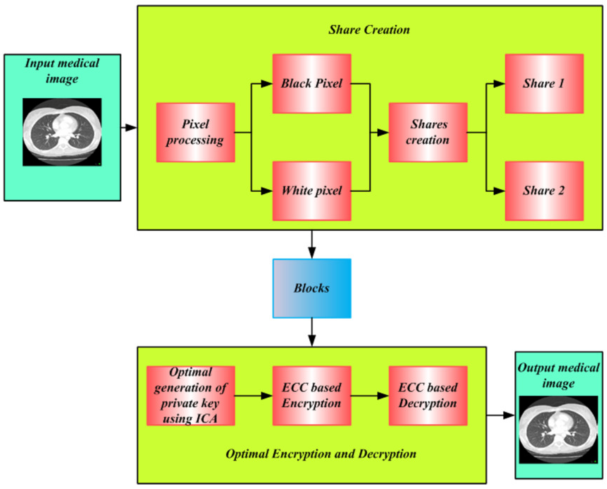


Fig.4: *Block diagram for a proposed method.*

4.1 Share creation

Shares are generally termed as all the pixel value (Black and white pixel) of the secret medical image. Shares (B_S and W_S) are also called compilation of sub-pixels of original medical image. Here, the removal of the pixel value from the original medical image of each band (B_z and W_z) can be determined by the following equation (2-3),

$$B_z = \int_1^A B_{mn} \tag{2}$$

$$W_z = \int_1^A W_{mn} \tag{3}$$

where m and n are the position of matrix. The surreptitious sharing method is encrypted a secret medical image into futile share images. And it should not reveal information about the original medical image until each and every one of the shares is obtained. Then, numerous shares are created with the help of the basic matrix k and it is given in the following equation (4)

$$Number\ of\ multiple\ shares = 2^k \tag{4}$$

The basic matrix can be created by the following equation (5)

$$W = \frac{B}{k} \tag{5}$$

Therefore, base matrix M_{CD} of the 3×3 matrix can be determined by

$$\begin{gathered} M_{C11} = W \\ M_{C22} = W \\ M_{C33} = B_z - 2W \end{gathered}$$

Generally, basic matrices $B_M = B_{C1} + B_{C2} + B_{C3}$

$$\begin{gathered} M_{C1} = 128 - M_{c11} \\ M_{C2} = 128 - M_{c22} \\ M_{C3} = 128 - M_{c33} \end{gathered}$$

The black band shares (SHARES 1) are created using XOR operation and given in the following equation (6-9)

$$B_1 = M_{C1}\ XOR\ key \tag{6}$$

$$B_2 = M_{C1}\ XOR\ M_{C2} \tag{7}$$

$$B_3 = M_{C2}\ XOR\ B_1 \tag{8}$$

$$B_4 = B_1\ XOR\ B_z \tag{9}$$

Similarly, the above process is applied for white band share (SHARES 2).

4.2 Block

The multiple shares are alienated into blocks to acquire the original medical image can be determined with the help of the following equation (10-11)

$$\mathrm{B} = \mathrm{B}_1\ XOR\ B_2\ XOR\ B_3\ XOR\ B_4\ XOR\ key \tag{10}$$

$$\mathrm{W} = \mathrm{W}_1\ XOR\ W_2\ XOR\ W_3\ XOR\ W_4\ XOR\ key \quad (11)$$

here shares reconstruction takes place and the process of encryption and decryption interms of ECC system applied to the shares which are reconstructed. Every shared image is divided into blocks previous to the encryption and decryption process and size of each partitioned block is denoted as 4 * 4.

4.3 Encryption and Decryption

ECC algorithm is applied for implementation of public key cryptography and similar to the asymmetric key cryptography. An equation of ECC is derived based on the maximum limit of prime number function and base point. An encryption function is evaluated after this operation. The equation of ECC is,

$$E = [PRIME(K)]^3 + I \times PRIME(K) + J \quad (12)$$

here I and J are constant and the value of $I = J = 2$.

4.3.1 Generation of key

Generation of key plays a significant role in encryption process based on cryptographic function. The first step in the encryption process is creating the public key for encrypting the message and this key is obtained as receiver side. The next step is generating the private or secret key on the receiver side for decryption process.

$$P = H_{opt} \times B_{en} \quad (13)$$

where P is the public key, H_{opt} is denoted as optimal private key, the base point of curve is represented as B_{en} and H_{opt} be the selected random number to $n-1$ in the range of 1.

4.3.2 Encryption Process

Each block is encrypted using encryption process and number of blocks denoted $N(j, j)$ here, i and j indicates row and column of image blocks. The pixels $R_g(i, j)$ and $R_h(i+1, j)$ also it's corresponding point is expressed in the given equation,

$$E_1 = H_{opt} \times B_{en} \quad (14)$$

$$E_2 = (R_g, R_h) + E_1 \quad (15)$$

4.3.3 Decryption Process

The private key H_{opt} is utilized for decryption process is decrypting the message in receiver side. Pixel point is decrypted by point E_3 and the final result of the decryption process E_{ij} are given below in the following equation (16-17)

$$E_3 = H_{opt} \times E_1 \quad (16)$$

$$E_{i,j} = E_2 - E_3 \quad (17)$$

Finally, the output decrypted image is hoarded simultaneously for getting original medical image and determined using the following equation (18)

$$\mathrm{B}_Z = B_1\ XOR\ B_2\ XOR\ B_3\ XOR\ B_4\ XOR\ key \quad (18)$$

4.3.4 Optimization of key generation using Imperialist CompetitiveAlgorithm (ICA)

Imperialist CompetitiveAlgorithm is stimulated using socio-political procedure of imperialism and this algorithm has excellent convergence and universal accomplishments.Generally,this ECC algorithm is used to generate the key generation associated with Imperialist CompetitiveAlgorithm. The general steps for finding best key with the help of Imperialist CompetitiveAlgorithm. To get the key solution, country for key selection process is given below,

$$country = \{P_1, P_2, \ldots\ldots\ldots, P_Y\} \quad (19)$$

The optimal key selection can be determined by the following equation (20)

$$cost = Fitness(P_1, P_2, \ldots\ldots\ldots, P_Y) \quad (20)$$

The countries (population) with preeminent fitness values are usually choosen as imperialists and non-preeminent fitness values are usually choosen as colonies of these imperialists. To find the optimal fitness values can be determined with the help of the normalized cost of the imperialist and given below in the equation (21)

$$Normalized\ cost = imperialist\ cost_n - maximum\ cost_m \quad (21)$$

Using normalized cost of entire imperialist, the normalized power of all imperialist can be determined in the given equation (22)

$$Normalized\ power\ of\ all\ imperialist = \left| \frac{Normalized\ cost}{\sum_{m=1}^{No\ of\ imperialist} maximum\ cost_m} \right| \quad (22)$$

Every imperialist with its pertinent colonies are called empire. Afterwards, the colonies in each empire progress towards the pertinent imperialist using assimilation operator and if there is an empire that consists of minimum cost to imperialist, swap the position of that colony and imperialist. Calculate the total cost of entire empires is given below in the equation (23).

$$Total\ cost = cost(no\ of\ imperialist) + ßmean\ \{cost(no\ of\ empire)\} \quad (23)$$

where ß represents the random number and the value should be less than 1. Pick the weakest colony from the weakest empire and provide it to the best empire. The empires with no colonies will be deleted. The terminating criteria are repeated with the existence of one empire and deletion of others.

4.4 Output medical image

Finally, decrypted output medical image is obtained from optimal Encryption and Decryption block and it is compared with the original image.

5. EXPERIMENTAL RESULTS AND DISCUSSION

The performance of proposed method is evaluated and experimental results are estimated using the parameter metrics such as PSNR, CC (Correlation Coefficient) and MSE (Mean Square Error). In this manuscript, entire calculations are executed in MATLAB platform on Windows 7 system by Intel (R) Core (TM) i7-4790 3.6 GHz CPU with 8 GB of RAM. The performance of the proposed hybridizing visual cryptography with Elliptical Score-based Key Enumeration Algorithm (ESKEA) is compared with the existing method like Score-based Key Enumeration Algorithm (SKEA) [29].

5.1 Evaluation Metrics

5.1.1 Peak signal-to-noise ratio (PSNR):

It is utilized for estimating the features of reconstruct image from process image. It is provided in equation (24) as:

$$PSNR = 20\log_{10}\frac{2^n - 1}{MSE} \quad (24)$$

A minimum value of root mean square error and maximum value of peak signal-to-noise ratio denotes better signal-to-noise ratio.

5.1.2 Mean Square Error (MSE):

It is used to calculate the signal fidelity. It given by equation (25) as

$$MSE = \frac{1}{R \times S}\sum\sum\left(f(i,j) - f^P(i,j)\right)^2 \quad (25)$$

Fig. 5 portrays that encryption and decryption process of the proposed method and it shows the PSNR and MSE value. In brain, during encryption and decryption the PSNR value is 58.57 and MSE value is 0.97. In Eyes, during encryption and decryption the PSNR value is 56.48 and MSE value is 0.106. In Lungs, during encryption and decryption the PSNR value is 57.69 and MSE value is 0.113. In Kidney, during encryption and decryption the PSNR value is 58.3 and MSE value is 0.126. In Pancreas, during encryption and decryption the PSNR value is 56.21 and MSE value is 0.129.

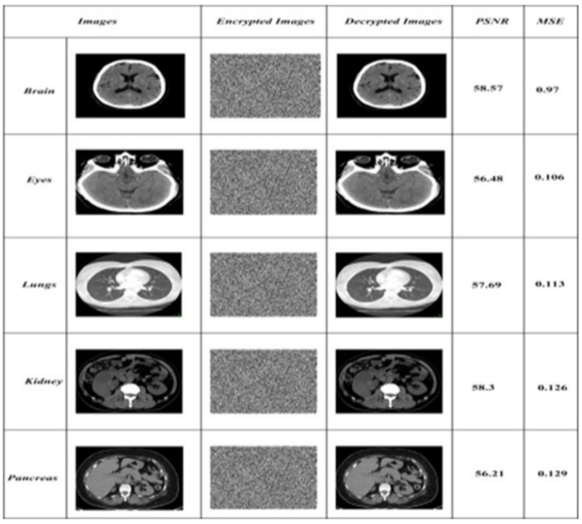


Fig.5: Encryption and Decryption process of the proposed method.

Fig. 6 shows the performance analyses of the images are analyzed. The encryption time of the head is 1341ms, security level is 96, PSNR is 61, MSE is 0.08, BER is 0 and CC is 0.99. The encryption time of the brain slice is 1068ms, security level is 96, PSNR is 59, MSE is 0.09, BER is 0 and CC is 0.98. The encryption time of the brain is 956ms, security level is 96, PSNR is 61, MSE is 0.11, BER is 0.01 and CC is 0.99. The encryption time of the eye is 3241ms, security level is 96, PSNR is 61, MSE is 0.07, BER is 0.01 and CC is 0.97. The encryption time of the abdomen is 6254ms, security level is 96, PSNR is 61, MSE is 0.08, BER is 0 and CC is 0.99.

Fig.7 shows the file uploading time using proposed ESKEA and existing SKEA method. Here, the proposed ESKEA of file size 2000 is 16.66 %, file size 4000 is 23.52%, file size 6000 is 33.33%, file size 8000 is 20% and file size 10000 is 14.10% lower than the existing SKEA method. The comparison analysis shows the proposed method achieves lower uploading time compared to the existing method.

Fig.8 shows the file downloading time using proposed ESKEA and existing SKEA method. Here, the proposed ESKEA of file size 2000 is 11.11%, file size 4000 is 25.33%, file size 6000 is 23.07%, file size 8000 is 16.66% and file size 10000 is 6.02% lower than

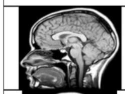
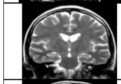
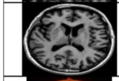
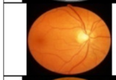
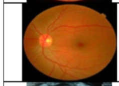
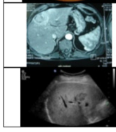
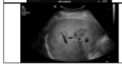
Image	Encryption Time in ms	Security Level	PSNR	MSE	BER	CC
	1341	96	61	0.08	0	0.99
	1068	96	59	0.09	0	0.98
	956	96	61	0.11	0.01	0.99
	3241	96	61	0.07	0.01	0.97
	4253	96	62	0.12	0	0.99
	6254	96	61	0.08	0	0.99
	3247	96	61	0.11	0	0.98

Fig.6: *Performance analysis of images.*

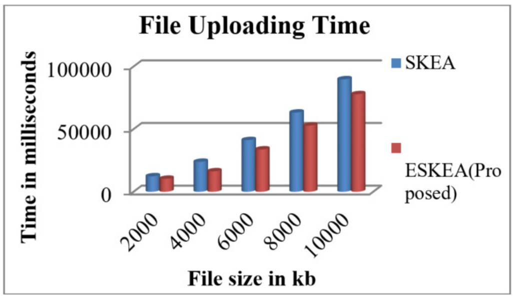


Fig.7: *File uploading time.*

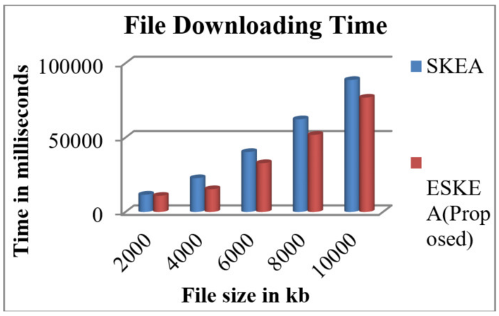


Fig.8: *File downloading time.*

the existing SKEA method. The comparison analysis shows the proposed method achieves lower downloading time compared to existing method.

Fig. 9 shows the Memory usage on encryption using proposed ESKEA and existing SKEA method. Here, the proposed ESKEA at file size 2000 is 9.42%, at file size 4000 is 5.66%, at file size 6000 is 8.24%, at file size 8000 is 7.30% and file size 10000 is 6.38% lower than existing SKEA method. The comparison analysis shows the proposed method achieves lower memory usage on encryption compared to existing method.

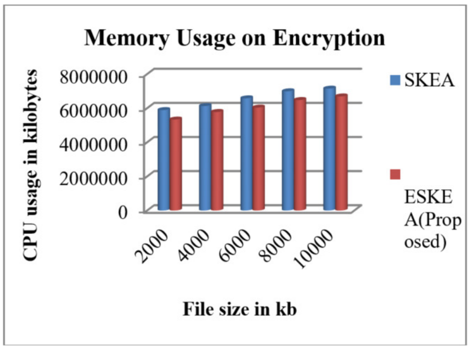


Fig.9: *Memory usage on encryption.*

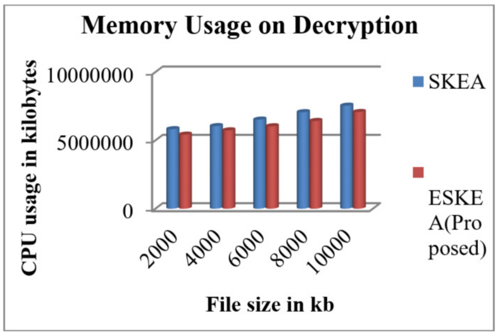


Fig.10: *Memory usage on decryption.*

Fig. 10 shows the Memory usage on decryption using proposed ESKEA and existing SKEA method. Here, the proposed ESKEA at file size 2000 is 6.88%, at file size 4000 is 5.16%, at file size 6000 is 7.46%, at file size 8000 is 9.09% and file size 10000 is 6.13% lower than existing SKEA method. The comparison analysis shows the proposed method achieves lower memory usage on decryption compared to existing method.

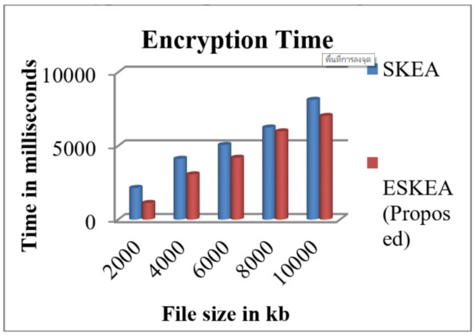


Fig.11: *Encryption time.*

Fig. 11 shows the encryption time using proposed ESKEA and existing SKEA method.Here, the proposed ESKEA of file size 2000 is 56.65%, file size 4000 is 33.07%, file size 6000 is 18.02%, file size 8000 is 17.28% and file size 10000 is 12.5% lower than existing SKEA method. The comparison analysis shows the proposed method achieves lower encryption time compared to the existing method.

Fig.12 shows the decryption time using proposed ESKEA and existing SKEA method. Here, the pro-

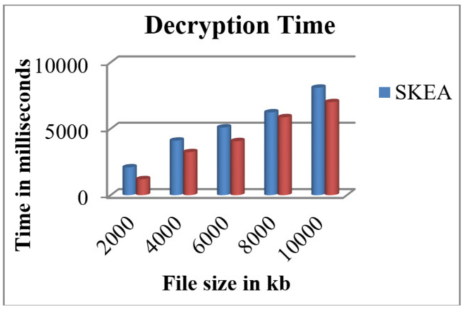


Fig.12: *Decryption time.*

posed ESKEA of file size 2000 is 60%, file size 4000 is 11.11%, file size 6000 is 7.98%, file size 8000 is 13.3% and file size 10000 is 12.5% lower than existing SKEA method. The comparison analysis shows the proposed method achieves lower decryption time compared to the existing method.

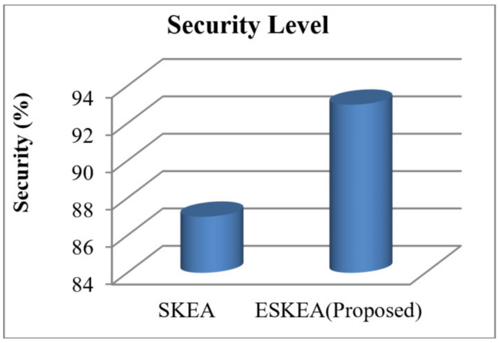


Fig.13: *Security level.*

Fig.13 portrays that Security level of proposed ESKEA and existing SKEA method. Here, the proposed method achieves 6.89% higher security than existing SKEA method.

Fig.14 shows the PSNR using proposed ESKEA and existing SKEA method. Here, the proposed ESKEA of image size 2000 is 28.26%, image size 4000 is 25%, image size 6000 is 13.72%, image size 8000 is 28.57% and image size 10000 is 24% higher than existing SKEA method. The comparison analysis shows the proposed method achieves high PSNR compared to the existing method.

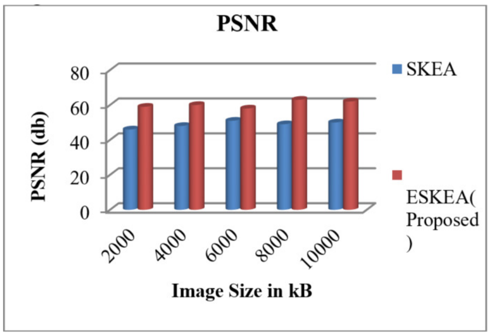


Fig.14: *Peak Signal to Noise Ratio.*

Fig. 15 shows the MSE using proposed ESKEA and existing SKEA method. Here, the proposed ESKEA of image size 2000 is 41.93%, image size 4000 is 34.48%, image size 6000 is 28.57%, image size 8000 is 43.33% and image size 10000 is 41.37% lower than existing SKEA method. The comparison analysis shows the proposed method achieves low MSE compared to the existing method.

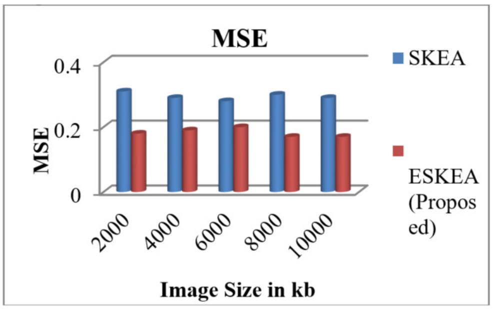


Fig.15: *Mean Square Error.*

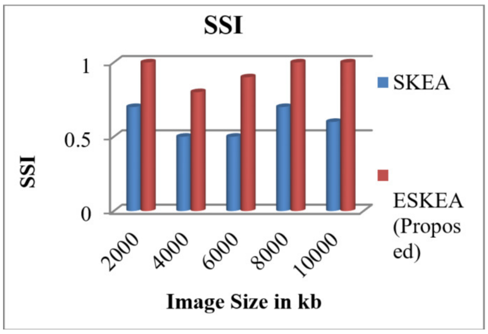


Fig.16: *Structured Similarity Index.*

Fig. 16 shows the SSI using proposed ESKEA and existing SKEA method. Here, the proposed ESKEA of image size 2000 is 42.85%, image size 4000 is 60%, image size 6000 is 80%, image size 8000 is 66.66% and image size 10000 is 55.23% higher than the existing SKEA method. The comparison analysis shows the proposed method achieves high SSI compared to the existing method.

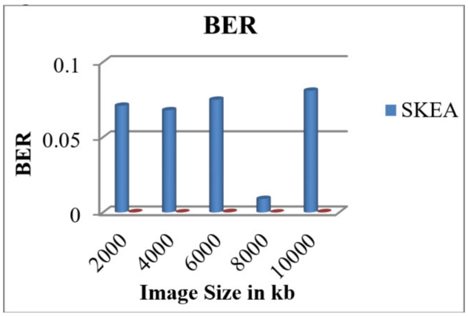


Fig.17: *Bit Error Rate.*

Fig. 17 shows the BER using proposed ESKEA and existing SKEA method. Here, the proposed ESKEA of image size 2000 is 99.71%, image size 4000 is 99.85%, image size 6000 is 99.6%, image size 8000 is 100% and image size 10000 is 99.75% lower than the existing SKEA method. The comparison analysis shows the proposed method achieves lower BER compared to the existing method.

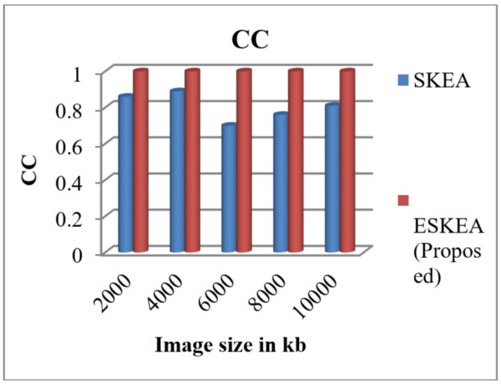


Fig.18: *Correlation Coefficient.*

Fig. 18 shows the CC using proposed ESKEA and existing SKEA method. Here, the proposed ESKEA of image size 2000 is 16.27%, image size 4000 is 12.35%, image size 6000 is 42.85%, image size 8000 is 31.57% and image size 10000 is 23.45% higher than the existing SKEA method. The comparison analysis shows the proposed method achieves high CC compared to the existing method.

6. CONCLUSION

In this manuscript, an optimal elliptic curve cryptography hybridization visual cryptography was proposed for Internet of Things (IoT) medical image security. In the proposed method, the optimal key was generated using imperialist competitive algorithm. Finally, the decrypted output image was compared to original image. The proposed ESEA approach reduces the file uploading time as 16.66%, 23.52%, 33.33%, 20% and 14.10%.And file downloading time as 11.11%, 25.33%, 23.07%, 16.66% and 6.02%.The proposed ESEA approach reduces the Memory usage on encryption as 56.65%, 33.07%, 18.02%, 17.28% and 12.5%.Memory usage on decryption as 60%, 11.11%, 7.98%, 13.3% and 12.5%.The proposed ESEA approach achieves 6.89% higher security than existing SKEA method. Furthermore, the simulation outcomes demonstrate that performance of proposed system may be able to get the optimal global solutions efficiently and accurately compared with existing techniques.

References

[1] J. Wu, X. Liao and B. Yang, “Color image encryption based on chaotic systems and elliptic curve ElGamal scheme,” *Signal Processing*, vol. 141, pp. 109-124, 2017.

[2] S. Li, L. Xu and S. Zhao, “5G Internet of Things: A survey,” *Journal of Industrial Information Integration*, vol. 10, pp. 1-9, 2018.

[3] S. Mythili, K. Thiyagarajah, P. Rajesh and F.H. Shajin , “Ideal position and size selection of unified power flow controllers (UPFCs) to upgrade the dynamic stability of systems: an antlion optimiser and invasive weed optimisation algorithm,” *HKIE Trans*, vol. 27, no.1, pp. 25-37, 2020.

[4] M. Conti, A. Dehghantanha, K. Franke and S. Watson, “Internet of Things security and forensics: Challenges and opportunities,” *Future Generation Computer Systems*, vol. 78, pp. 544-546, 2018.

[5] P. Rajesh and F. H. Shajin, “A Multi-Objective Hybrid Algorithm for Planning Electrical Distribution System,” *European Journal of Electrical Engineering*, vol.22, no.4-5, pp.377-387, 2020.

[6] M. Wollschlaeger, T. Sauter and J. Jasperneite, “The Future of Industrial Communication: Automation Networks in the Era of the Internet of Things and Industry 4.0,” *IEEE Industrial Electronics Magazine*, vol. 11, no. 1, pp. 17-27, 2017.

[7] FH. Shajin,P. Rajesh. “Trusted secure geographic routing protocol: outsider attack detection in mobile ad hoc networks by adopting trusted secure geographic routing protocol,” *International Journal of Pervasive Computing and Communications*, 2020.

[8] F. Alaba, M. Othman, I. Hashem and F. Alotaibi, “Internet of Things security: A survey,” *Journal of Network and Computer Applications*, vol. 88, pp. 10-28, 2017.

[9] M. Mahdavinejad, M. Rezvan, M. Barekatain, P. Adibi, P. Barnaghi and A. Sheth, “Machine learning for internet of things data analysis: a survey,” *Digital Communications and Networks*, vol. 4, no. 3, pp. 161-175, 2018.

[10] MK. Thota, FH. Shajin and P. Rajesh. “Survey on software defect prediction techniques,” *International Journal of Applied Science and Engineering*, vol.17, no.4, pp.331-44, 2020;

[11] G. Akpakwu, B. Silva, G. Hancke and A. Abu-Mahfouz, “A Survey on 5G Networks for the Internet of Things: Communication Technologies and Challenges,” *IEEE Access*, vol. 6, pp. 3619-3647, 2018.

[12] D. Boubiche, S. Athmani, S. Boubiche and H. Toral-Cruz, “Cybersecurity Issues in Wireless Sensor Networks: Current Challenges and Solutions,” *Wireless Personal Communications*, 2020.

[13] S. Bitam, S. Zeadally and A. Mellouk, “Bio-inspired cybersecurity for wireless sensor networks,” *IEEE Communications Magazine*, vol. 54, no. 6, pp. 68-74, 2016.

[14] U. Satija, B. Ramkumar and M. Sabarimalai

Manikandan, “Real-Time Signal Quality-Aware ECG Telemetry System for IoT-Based Health Care Monitoring,” *IEEE Internet of Things Journal*, vol. 4, no. 3, pp. 815-823, 2017.

[15] R. Riyaldhi, Rojali and A. Kurniawan, “Improvement of Advanced Encryption Standard Algorithm With Shift Row and S.Box Modification Mapping in Mix Column,” *Procedia Computer Science*, vol. 116, pp. 401-407, 2017.

[16] L. Handoko, C. Umam, D. Setiadi and E. Rachmawanto, “DIGITAL SIGNATURE PADA CITRA MENGGUNAKAN RSA DAN VIGENERE CIPHER BERBASIS MD5,” *Simetris: JurnalTeknikMesin, ElektrodanIlmuKomputer*, vol. 10, no. 1, pp. 357-366, 2019.

[17] M. Elhoseny, K. Shankar, S. Lakshmanaprabu, A. Maseleno and N. Arunkumar, “Hybrid optimization with cryptography encryption for medical image security in Internet of Things,” *Neural Computing and Applications*, vol. 32, no. 15, pp. 10979-10993, 2018.

[18] X. Cheng et al., “Secure Identity Authentication of Community Medical Internet of Things,” *IEEE Access*, vol. 7, pp. 115966-115977, 2019.

[19] R. Baashirah and A. Abuzneid, “SLEC: A Novel Serverless RFID Authentication Protocol Based on Elliptic Curve Cryptography,” *Electronics*, vol. 8, no. 10, p. 1166, 2019.

[20] A. Ostad-Sharif, D. Abbasinezhad-Mood and M. Nikooghadam, “Efficient utilization of elliptic curve cryptography in design of a three-factor authentication protocol for satellite communications,” *Computer Communications*, vol. 147, pp. 85-97, 2019.

[21] N. Singh, A. Hans and S. Kaur, “Layer and RFID Based Security Issues of Internet of Things,” *International Journal of Grid and Distributed Computing*, vol. 9, no. 10, pp. 301-310, 2016.

[22] S. Kalsi, H. Kaur and V. Chang, “DNA Cryptography and Deep Learning using Genetic Algorithm with NW algorithm for Key Generation,” *Journal of Medical Systems*, vol. 42, no. 1, 2017.

[23] M. Elhoseny, K. Shankar, S. Lakshmanaprabu, A. Maseleno and N. Arunkumar, “Hybrid optimization with cryptography encryption for medical image security in Internet of Things,” *Neural Computing and Applications*, vol. 32, no. 15, pp. 10979-10993, 2018.

[24] Y. Guan and X. Ge, “Distributed Secure Estimation Over Wireless Sensor Networks Against Random Multichannel Jamming Attacks,” *IEEE Access*, vol. 5, pp. 10858-10870, 2017.

[25] T. Avudaiappan, R. Balasubramanian, S.S., Pandiyan, M.Saravanan, S.K.. Lakshmanaprabu and K., Shankar, “Medical image security using dual encryption with oppositional based optimization algorithm,” *Journal of medical systems*, vol.42, no.11, pp.1-11, 2018.

[26] A. Banik, Z. Shamsi and D.S. Laiphrakpam, “An encryption scheme for securing multiple medical images,” *Journal of Information Security and Applications*, vol. 49, p.102398, 2019.

[27] R. Hamza, Z. Yan, K. Muhammad, P. Bellavista and F. Titouna, “A privacy-preserving cryptosystem for IoT E-healthcare,” *Information Sciences*, vol. 527, pp. 493-510, 2020.

[28] M. Khari, A. Garg, A. Gandomi, R. Gupta, R. Patan and B. Balusamy, “Securing Data in Internet of Things (IoT) Using Cryptography and Steganography Techniques,” *IEEE Transactions on Systems, Man, and Cybernetics: Systems*, vol. 50, no. 1, pp. 73-80, 2020.

[29] S. Koppu and V. Viswanatham, “Medical image security enhancement using two dimensional chaotic mapping optimized by self-adaptive grey wolf algorithm,” *Evolutionary Intelligence*, vol. 11, no. 1-2, pp. 53-71, 2018.

[30] K. Shankar, M. Elhoseny, E. Perumal, M. Ilayaraja and K.S. Kumar, “An efficient image encryption scheme based on signcryption technique with adaptive elephant herding optimization,” in *Cybersecurity and Secure Information Systems*, pp. 31-42, 2019 Springer, Cham.

[31] K. Shankar, M. Elhoseny, R.S. Kumar, S.K. Lakshmanaprabu and X. Yuan, “Secret image sharing scheme with encrypted shadow images using optimal homomorphic encryption technique,” *Journal of Ambient Intelligence and Humanized Computing*, vol.11, no.5, pp.1821-1833, 2020.

[32] A. Sivasankari and S. Krishnaveni, “Optimal Wavelet Coefficients Based Steganography for Image Security with Secret Sharing Cryptography Model,” in *Cybersecurity and Secure Information Systems*, Springer, Cham, pp. 67-85, 2019.

[33] R. Villanueva-Polanco, “A comprehensive study of the key enumeration problem,” Entropy, vol.21, no.10, p.972, 2019

L. Ashok Kumar received M. Tech degree from Sathyabama University. He is currently working as an Associate Professor in ECE department in Panimalar Institute of Technology, Chennai. He has totally 16 years of teaching experience. He is the lifetime member of ISTE and EMC Society for Engineers. His area of interest include Image processing and VLSI. He is the author for the books Electromagnetic Interference and Compatibility and Communication Networks.

Sumit Srivastava received the M.Tech. degree in Digital Communication from UKTU Dehradun . He has more than 14 years of teaching experience and working as an Assistant Professor in the Department of Electronics and Communication Engineering, FET, MJP Rohilkhand University Bareilly, INDIA. His research interests include RADAR systems,Microstrip Patch antennas, artificial Intelligence, machine learning and IOT based systems.

Balaji S. R. received B.E. degree in EIE from Annamalai University, Chidambaram, Tamilnadu in 2004. M. Tech degree in VLSI Design from Sathyabama University, Chennai, Tamilnadu in 2009. He is currently working as Associate Professor in the Department of Electronics and Instrumentation Engineering, Panimalar Engineering College, Poonamallee, Tamilnadu, Chennai, India. His research interests include image processing, VLSI Design, IoT, Machine Learning, Cryptography.

Francis H Shajin received his Bachelor of Engineering and Master of Engineering in Electronics and Communication Engineering from Anna University, Chennai, India. He has more than 7 years of IT experience. His current research interests include very-large-scale integration, soft computing, image processing, machine learning and networking.

Paulthurai Rajesh received his Bachelor of Engineering and Master of Engineering in Electrical and Electronics Engineering from Anna University, Chennai, India. He has more than seven years of IT experience. His current research interests include artificial intelligence, power system, smart grid technologies and soft computing.