Wireless Networks
https://doi.org/10.1007/s11276-020-02486-x

Lightweight Feistel structure based hybrid-crypto model for multimedia data security over uncertain cloud environment

Denis Rayappan[1] · Madhubala Pandiyan[2]

Accepted: 23 October 2020

Abstract

The exponential rise in software computing and internet technologies have broadened the horizon of cloud computing applications serving numerous purposes like business processes, healthcare, finance, socialization, etc. In the last few years the increase is security breaches and unauthorized data access has forced industry to achieve computationally efficient and robust security system. The increase in multimedia data communication over different cloud applications too demands an efficient security model, which is expected to have low computational complexity, negligible quality-compromise and higher security robustness. Major conventional security-systems like cryptography and steganography undergo high computational overhead, thus limiting their potential towards cloud-communication where each data input used to be of large size and a gigantic amount of multimedia data is shared across the network. To alleviate above stated problems and enable a potential solution, in this paper a highly robust Lightweight Feistel Structure based Substitution Permutation Crypto Model is developed for multimedia data security over uncertain cloud environment. Our proposed model applies substitution permutation crypto concept with Feistel structure which performs substitution-permutation over five rounds to achieve higher confusion and diffusion. To retain higher security with low computation, we applied merely 64-bit block cipher and equal key-size. MATLAB based simulation revealed that the proposed lightweight security model achieves better attack-resilience even maintaining low entropy, high-correlation, and satisfactory computation time for multimedia data encryption. Such robustness enables our proposed security model to be applied for real-world cloud data security.

Keywords Multimedia data security · Cloud computing · Hybrid cryptosystem · Feistel structure · Substitution and permutation network

1 Introduction

The exponential rise in software technologies and sophisticated hardware platforms has broadened the horizon for highly integrated services and solutions to serve varied socio-industrial demands. In the last few decades, multimedia communication and allied information exchange has gained wide-spread attention. Similarly, the fast-increasing internet technologies too have broadened the horizon for new computing environment like cloud computing, internet-of-things (IoTs), etc. Undeniably, the large numbers of internet enabled applications or the communication systems are generating huge data everyday to provide corresponding solutions such as social networking sites, healthcare purposes, e-commerce, scientific communities, financial sectors and other industrial demands like surveillance and security systems. Social media and entertainment, surveillance footages [1–3], consumer multimedia data, IoT assisted communication environment [2, 4–7] demand potential security solution and policies to protect their data from unauthorized access. Similarly, enterprise software has also witnessed significant growth across the industries, government agencies, banks and other organizations, which generates and communicates data

✉ Denis Rayappan
denisatshc@gmail.com

Madhubala Pandiyan
madhubalasivaji@gmail.com

[1] Department of Computer Science, Periyar University, Salem, Tamil Nadu, India

[2] Department of Computer Science, Don Bosco College (Affiliated to Periyar University), Dharmapuri, Tamil Nadu, India

Published online: 11 November 2020

(including multimedia data) in large volume. On the contrary, in the last few years, the adversarial efforts have increased significantly forcing industries to achieve secure data communication over the different ecosystems including IoT and cloud-infrastructures [1–5, 8–10]. Functionally, the amalgamation of the different data sources and allied voluminous data aggregation has given rise to the technology named cloud computing. Cloud computing enables different stakeholders to access data, making real-time computation and decision using cloud infrastructure irrespective of location or geographical boundaries. The prominent concern in cloud computing is the data security [2, 8]. More importantly, ensuring data security with low computational complexity, high time-efficiency with uncompromised multimedia data quality has been the key driving force for research communities [1, 2, 5, 6]. To avoid security breaches a number of efforts have been made; however, the major at-hand approaches function either by introducing data-access security models or infrastructure security or by implementing certain on-data security features [8]. Researchers have proposed security models in which the user requires getting authenticated before accessing the data (access-control), or the data itself is processed in such manner that it is communicated as a hidden content without revealing to the unauthorized users (Ex. Steganography).

Towards major multimedia data security approaches, steganography and cryptosystems are the most used methods [9, 10]; however, their robustness as standalone solution has remained questionable. Majority of the classical cryptosystems like RSA, AES, ECC, homomorphic models etc., consume significantly high computation due to higher key size. Though, higher key size hypothesizes to have higher attack-resiliency; however, at the cost of increased computational overhead. On the other hand, the recent events of the attacks like brute-force attack, impersonation attack etc., have put question on their robustness. Though, a few researches have suggested applying high bit-size to confuse the attacker, the computational cost of such approaches can't be denied. These facts alarms requirement of a more robust and computationally-efficient (say, lightweight) security system. With this motive, in this paper a highly robust and lightweight cryptosystem is developed which amalgamates the robustness of substitution-permutation (SP) concept and Feistel structure. The use of Feistel structure enables better confusion and diffusion while maintaining equivalent encryption and decryption which eventually helps retaining lower computational cost with higher attack-resiliency. The proposed Lightweight Hybrid SP-Feistel Crypto-Model embodies symmetric key-block cipher constituting 64-bit key size, which makes it computationally more efficient even without compromising with the level of security. Additionally, we introduced a novel Key-Expansion Block Function (KEBF) which helped in retrieving five distinct keys over five rounds to introduce higher level of confusion and diffusion towards higher attack-resilience. To process confusion and diffusion (CDF) our proposed model executed KEBF for five rounds where for each round 4-bit of data was processed at a time. It enabled computational efficiency to handle multimedia data even of the large size and volume. The overall proposed model was developed using MATLAB 2019b, where its efficiency was assessed over the multimedia data of the different sizes. The performance assessment was made in terms of histogram analysis, correlation assessment, entropy, computation-time, Number of Changing Pixel Rates (NPCR) and the Unified Average Channel Intensity (UACI). Additionally, we examined robustness of the proposed security model qualitatively, where it was found suitable to avoid attacks like weak-key combination attack, square attack, regular and singular attacks (say, steganalysis), etc.

The remaining sections of the presented manuscript are given as follows. Section II discusses the related work, which is followed by the discussion of problem formulation in Section III. Section IV presents the overall proposed system and its implementation, while the simulation results are discussed in Section V. Conclusion of the overall research is given in Section VI.

2 Related work

Xue et al. [11] proposed content adaptive steganography, where the secret data was embedded into the noisiest pixels. Vipula et al. [12] combined AES crypto-algorithm with steganography to hide secret data within the cover multimedia images. Unlike [11], Lokesh [13] used alteration component method to hide AES encrypted message within the cover image. Saleh [14] applied modified AES algorithm for encrypting the secret message to be hidden in the cover image. M.E. Saleh et al. [15] proposed a new image steganography enhancement method for the pixel value difference (PVD) method and achieved maximum hiding capacity and image quality. Duluta et al. [16] found that the classical encryption algorithms have numerous limitations which can confine its suitability for cloud computing environment. Pancha [17] encrypted the input image to retrieve cipher image by applying encryption key in conjugation with Chirikov mapping. Subsequently, they applied steganography to hide cipher image within the cover image. To introduce higher level of confusion, Leung et al. [18] applied multiple encryption techniques to encrypt different parts of the media for the best security protection subject to the given computing resources. Mukhedkar [19] too applied different cryptosystems such as DES, 3DES, AES, Blowfish Algorithm to encrypt the secret data before embedding within cover image. Li et al. [20] applied region of interest identification and clustering concept for video fingerprinting-based multimedia security. Ahmed [21] applied elliptic curve cryptography (ECC) based (text) encryption, followed by LSB embedding to safeguard the data over uncertain channel. To further strengthen their approach, authors [21] transmitted data over the different channels to the same target. Undeniably, this approach could undergo significantly large computational overheads. To achieve non-perceptibility over steganography, Hajduk [22] performed secret message encryption using quick response code (QR). The embedding process was additionally protected by AES algorithm. Alam [23] applied McEliece cryptosystem for data encryption to improve the security and privacy. Kumar et al. [24] proposed a symmetric key cryptography algorithm for secure three-dimensional color image security. Sharma [25] performed speech-signal encryption followed by steganography to secure data over communication channels. Wang et al. [26] applied watermark concept for multimedia data transmission over unsecure channel transmission.

Zaher [27] enhanced classical chaotic shift keying (CSK) method where the secret data were hidden within the chaotic transmitter states that could change among four different chaotic attractors in such manner that the binary information could effectively diffused. Authors applied cryptography to change the transmitter parameters in such manner that they have a quadruple form and therefore breaking into the public communication channel using return map attacks will fail. Realizing time-exhaustion due to chaotic map-based encryption, Hossain et al. [28] proposed a non-linier 3D chaos based simple encryption technique by applying 3D chaos for position permutation and value transformation technique. Saxena et al. [29] combined encryption and digital watermarking to enhance the image security. Gupta [30] recommended using discrete wavelet transform (DWT) to split input image into four sub band, followed by data hiding within the splits. Hiding the text-data within the image, authors performed compression to achieve transmission efficiency. Authors [31–37] combined cryptography and steganography; however, it could not guarantee computational efficiency over cloud infrastructure. Torvi [38] proposed unique data security using text steganography (UDSTS) framework that can transmit and receive encrypted messages embedded in a rich text format. Saraireh [35] used filter bank cipher to encrypt the secret text message, followed by DWT based steganography to hide the encrypted message within the cover image. Towards imperceptibility, Laskar et al. [37] applied discrete cosine transform (DCT) method to perform data hiding (in cover image) in frequency domain. Pleshkova et al. [39] proposed a mathematical concept for public key infrastructure (PKI) to secure the audio-data transmission from unauthorized access. Pai [40] encrypted video data and generated video-ciphers in a time and space efficient approach. Authors found that region permutation followed by application of AES and DES can enhance security of video files. However, such systems were found computationally costly [13].

Cui et al. [41] developed encrypted data sharing environment for secure image service for mobile devices with privacy assurance over cloud environment. Usman et al. [42] developed a privacy preserving security model for internet of multimedia things (IoMT). Zheng et al. [43] developed an encrypted cloud model with secure de-duplication for secure video transmission. Authors exploited the concept of scalable video coding (SVC) and secure de-duplication to achieve multimedia security over Azure platform. However, it could not be assessed in terms of data reconstruction quality and computational overhead. Abdul et al. [44] developed biometric security model with visual encryption technique. Though the use of visual cryptography and Zero-watermarking helped protecting the ownership of multimedia content, it was found computationally exhaustive. X. Li et al. [45] assessed different security models for cloud computing, where he found that cloud computing requires maintaining a fair balance in between the computation as well as attack-resilience. It indicates towards the need of certain lightweight solution. Q. Li et al. [46] proposed privacy preserving access control concept for multimedia data security over cloud platform. Authors applied ciphertext-policy attribute-based encryption (CP-ABE) that enabled cloud-assisted mobile multimedia data sharing. Hamid et al. [47] developed privacy preserving model with pairing based cryptography for medical data security for cloud computing. To achieve computational efficiency authors applied a tri-party one-round authenticated key agreement model. Khedr et al. [48] developed SecureMed a GPU accelerated homomorphic encryption concept for medical data security.

Zhu et al. [49] developed image encryption technique using non-uniform sampling to introduce more attack-resilience. As standalone multimedia security, Zhang et al. [50] developed ECC based image encryption with Diffie-Hellman public key sharing concept. Tawalbeh et al. [51] applied two ECC-based encryption algorithms for secure multimedia communication. The first algorithm performed selective encryption on the transform coefficients during compression, whereas the second algorithm achieved perceptual encryption based on selective bit-plane encryption before compression. Guan et al. [52] developed frequency domain DNA coding based chaotic image encryption model for multimedia data security where both the amplitude and phase components in frequency-domain were diffused and scrambled. J.He et al. [53] developed a bit stream-based JPEG image encryption. Hamza et al. [54] focused on key-frame confidentiality and developed hash-based encryption for key-frame of diagnosis hysteroscopy. Authors [54] designed local sensitive hash (LSH) to strengthen data security. Xia et al. [55] suggested a content-based image retrieval (CBIR) privacy-preserving scheme that enables the data owner to outsource the image database and CBIR service to the cloud, without exposing the actual database content to the cloud server. Xu et al. [56] applied hamming embedding algorithm to generate binary signatures for image security. This method achieved the balance between security, accuracy and efficiency of safe large-scale image retrieval in public clouds. Fawaz et al. [57] have suggested a scheme for image encryption based on two rounds of substitution—diffusion. They applied it in a block by block manner to attain the avalanche effect in overall image level, and ensured a high level of security and randomness.

Noura et al. [58] developed an effective image encryption scheme based on a dynamic structure. The proposed cipher structure consists of two distinct lightweight rounds (forward and backward chaining blocks) and a block permutation mechanism. Furthermore, the development of a dynamic key based on a secret key and a nonce was proposed as a key derivation feature. This key can be modified for each validate period (session), or for each new input image, depending on its configuration. Then the cipher layers were generated on the basis of this key, which were an integer or a binary diffusion matrix and an S-box substitute table, together with a P-box permutation table. The image was divided into blocks by Visalakshi et al. [59], and then transformed by moving the columns from left to right and right to left. After that, Blowfish algorithm was applied. A new lightweight secure cryptographic scheme for secure image communication was proposed by Mondal et al. [60]. In this scheme the plain image was permuted first using a sequence of pseudo random number (PRN) and encrypted by deoxyribonucleic acid (DNA) computation. The scheme was proposed for gray label images but the scheme can be extended for color images and text data. However, in order to make it applicable to the internet of things, there is potential for more developments in encryption techniques. In order to secure medical images, Noura et al. [61] proposed a cipher scheme with three variants (selective, middle-full and full). For each input image the scheme was based on primitive dynamic diffusion and/or confusion, which ensured good cryptographic efficiency with reduced rounds.

Belguith et al. [62] proposed a lightweight encryption algorithm consisting of a combination of symmetric algorithms to encrypt data and asymmetric ones to distribute keys. This work can be improved by proposing a new key distribution system that aims to offer the encryption key to any approved user without the involvement of the cloud provider. Daniel et al. [63] combined hashing and symmetric encryption with improved distributed hash table data structure to reduce overhead communication and computation for integrity verification and also to allow efficient operations of the data. The storage cost was drastically decreased by deduplication using the combined techniques of convergent encryption and filters. Rad et al. [64] introduced the concept of extending the capabilities of cloud file storage from just storing images to also performing encryption and analytics by moving and executing user-defined programs close to the data within an object cloud. The proposed PFCC algorithm provides a new parallel scheme for image encryption for cloud file sharing environment. One of the main differences between the existing transform-based encryption schemes and the proposed algorithm was the dual encryption method, which introduces a large amount of encryption complexity. Jinbo Xiong et al. [65] proposed a role symmetric encryption (RSE) algorithm and an RSE-based Proof of Ownership (RSE-PoW) scheme for secure deduplication in hierarchical heterogeneous environments, based on the role of symmetric encryption, proof of ownership and bloom filter. Aljawarneh et al. [66] proposed a resource-efficient encryption method for encrypting multimedia big data in IoT. The proposed framework took advantage of Feistel Encryption Scheme, advanced encryption standard (AES) and genetic algorithms. Alassaf et al. [67] analyzed the efficiency of the SIMON cryptographic algorithm and suggested a SIMON-based lightweight cryptography algorithm to minimize encryption time and preserve the realistic trade-off between security and performance in an IoT-driven setup for its potential use. The modified SIMON with 32, 48, 64, 96-bit block sizes showed interesting speed-up compared to the original SIMON, where some of them were found to be slower than AES. A lightweight selective encryption scheme was introduced by Amna Shifa et al. [68] in which encoder syntax elements were encrypted with the revolutionary EXPer (extended permutation with exclusive OR). A hybrid encryption algorithm for lightweight data stored in a cloud has been proposed by Liang et al. [69]. By increasing the key size to produce large prime numbers, this hybrid algorithm strengthens the RSA algorithm and then combined it with the AES algorithm. The authors of [70] proposed a one-round cipher (implemented on static images) for IoMT (Internet of Multimedia Things) in which the substitution and permutation principles were selected for the encryption.

3 Problem formulation

Majority of the at-hand image security models apply classical cryptosystems or steganography concepts, whose limited attack-resiliency and increased computational overhead can't be denied [45]. As standalone solution, most of the cryptosystems propose encryption with higher key-size (Ex. AES-256, RSA-256, homomorphic computation, etc.). Though, increasing key-size can increase the level of security and complexity towards unauthorized decryption, it significantly increased large computational overheads and processing-time. Such limitations confine their efficacy to meet real-world cloud computing demands. Steganography as an alternate too is found computationally exhaustive due to overheads imposed by wavelet transform, cipher embedding, compression etc. Additionally, the major steganography concepts don't address imperceptibility objective, which is must in the contemporary cloud communication environment. This is because majority of the statistical assessment-based attackers like steganalysis with sophisticated decryption tools can sense the hidden data and can eventually retrieve the same.

Addressing above stated problems and to achieve a novel and robust multimedia data security model, in this paper a lightweight cryptosystem has been developed. Unlike classical cryptosystem, our proposed model intends to maintain lower bit size or key-size (here, only 64-bit key) and lower computational while maintaining higher level of confusion to avoid any attack over cloud network. Our proposed security system can be considered as a hybrid model which exploits robustness of block cipher technique like substitution and permutation network (SPN) and Feistel architecture (a type of symmetric block cipher technique) to inculcate higher level of attack-resiliency even with lower computational overheads. Functionally, our proposed model consists of three consecutive steps, key generation, encryption and decryption. Here, at first, we apply SPN block cipher with iterative and alternating rounds of substitution and permutation (say, transposition) while ensuring that it fulfills the demands of Shannon's Confusion and Diffusion characteristics. To achieve it, we have developed a novel key-expansion block function (KEBF) which intends to assure that the cipher has been manipulated in pseudo random manner. To introduce more level of confusion and security-structure KEBF has been applied over five rounds, where in each round it intends to fulfill above stated Shannon's confusion and diffusion conditions. In this manner the proposed model ensures maintaining higher confusion with lower computation (Note, unlike classical AES cryptosystem which applies 15 rounds of encryption with 256-bit key size, our proposed model applies merely 5-round of computation with merely 64-bit key size. It can reduce overall computation to a great extent). The proposed model enables manipulating cipher text in such manner that it can avoid easy exposure of the original data to the intruder. To further strengthen the efficiency, we applied Feistel architecture with SPN to perform encryption and decryption of the input image data. Noticeably, the application of Feistel architecture enables decryption in the same way as encryption and hence reduces additional computational-exhaustion. Unlike other ciphers such as DES, Camelia, Blowfish etc., our proposed Feistel architecture can enable swift and more efficient encryption-decryption over large data size.

4 System model

As indicated in the previous section, the proposed security model can be stated as a hybrid cryptosystem functional on the basis of a symmetric key block cipher constituting 64-bit key and plain-text. In any symmetric key model, our proposed encryption method applies 5-rounds iterative mechanism which is also called encryption-rounds. In this process each round operates over certain predefined mathematical functions (here, KEBF) to generate confusion and diffusion matrix. Though, higher rounds assure better level-of-security; however, at the cost of increased computational overheads. The typical cryptographic methods apply an average of 10–20 rounds to encrypt the target data, which can cause significantly huge computational overhead and time-exhaustion. To avoid such complexity and time-exhaustion we performed KEBF merely for five rounds (Fig. 1) so as to enhance computational time, resource, redundancy etc.without compromising with the level-of-security. In other words, we performed only five-round of encryption where each encryption round processes over a 4-bit of input data. When encrypting the input data, the encryption function is executed in such manner that it creates sufficient confusion and diffusion to avoid any possible attack. To achieve it, we applied Feistel architecture to perform substitution and diffusion. The detailed discussion of the key-generation and expansion unit is given as follows. Some notations used in the explanation are shown in Table 1.

4.1 Key-generation and expansion

Considering the fact that in cloud computing environment each node behaves like a key generator as well as decoder, it is vital to maintain minimum possible computations. To achieve it, we designed a mathematical model by using XOR and XNOR logical function and data concatenation. The key task during encryption and decryption is the key

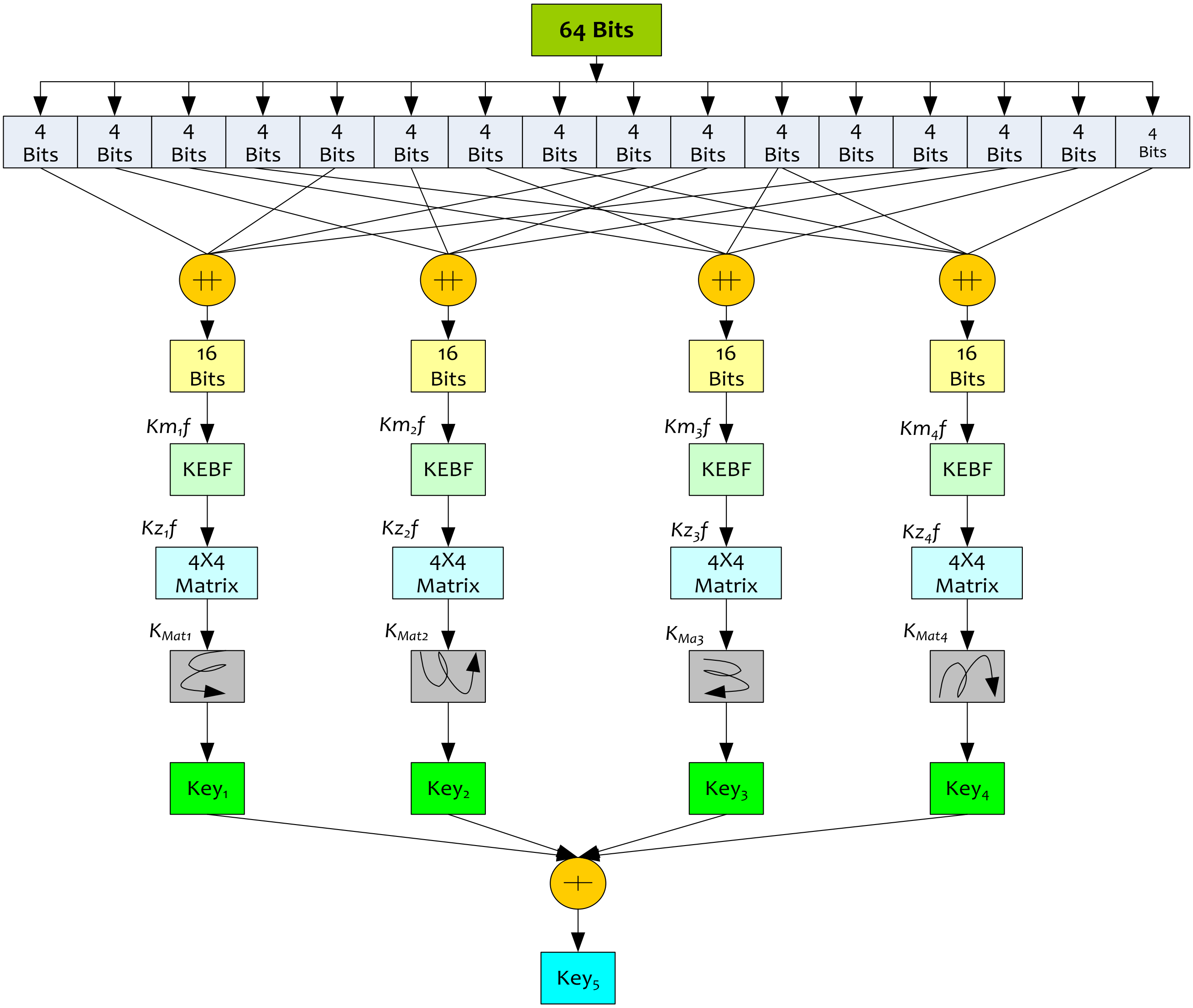


Fig. 1 KEBF assisted key expansion mechanism

Table 1 Notations

Notation	Function
⊕	XOR
⊙	XNOR
⧺ , ||	Concatenation

generation and therefore key-generation is the most essential component of the key-generation and expansion step. To accommodate it, we applied Feistel architecture-based encryption, which has been performed in multiple rounds (here, five), where each round requires distinct key (i.e., five distinct keys). To achieve it, we developed a function called "key-expansion block function (KEBF)". Noticeably, KEBF intended to strengthen attack-resilience towards any search-based attack which is common in online environment, by maintaining sufficiently large key size k_t that made it impossible for the intruder to perform 2^{k_t-1} encryption/decryption to gain key information for data retrieval. We designed our security model as a 64-bit block cipher that means, it demands 64-bit key to perform encryption of the 64-bit input data. In our proposed model, we applied 64-bit's cipher key k_c which has been further used as the input of the KEBF block that executes mathematical function to generate confusion and diffusion and eventually retrieves five distinct keys. Thus, it obtained five distinct keys for each round of encryption, which are subsequently applied for encryption and decryption process. Thus, unlike classical cryptosystems where single key is used for encryption, our proposed model presents more robustness and attack-resilience due to five-distinct key-based encryption.

A snippet of the KEBF model and allied key-expansion mechanism is illustrated in Fig. 1. As depicted in Fig. 1, KEBF block applies a function “F” (say, KEBF Function) which has been developed as per the suggestions made for block-cipher generation in [71]. Factually, Khazad cipher as discussed in [71] doesn’t represent the Feistel cipher and hence employs broad-trial-mechanism (BTM), where it (i.e., BTM) executes multiple linear and non-linear transformations. Though, this process assures the definite relationship and inter-dependency amongst the output cipher bits and the input bits in a predefined complex approach [72]. As depicted in Fig. 1, the 64-bit input data is at first split into 16 distinct chunks of 4-bits each. The subsequent four distinct chunks of 4-bits are concatenated, thus constituting 16-bit of data for which Feistel network obtains the keys (Fig. 1). As illustrated in Fig. 1, once executing KEBF over the 16 bits of the concatenated input, it generates a matrix of 4-bits each. The overall process of KEBF encompasses the following steps:

4.2 Step-1

Take the 64-bit input cipher k_c from the user and split it into four distinct segments of 4-bits.

4.3 Step-2

As depicted in Fig. 1, initiate the KEBF Function over each split component (i.e., 16-bit data). Noticeably, with 4-bits distinct segments, we obtained 16-bits data for each block on which KEBF was applied. Obtaining the 16-bits data after processing KEBF, execute the initial substitution of the blocks or segments of k_c using (1), similarly we obtained 16-bits for each KEBF Function.

$$Km_{i\in 1,2,3,4}f = ||_{(j=1)}^{4} Kn_{4\,(j-1)+i} \tag{1}$$

In (1), the variable i =1to 4 for first 4 round keys.

4.4 Step-3

Once obtaining the values for $Km_{i\in 1,2,3,4}f$, it has been further processed to give rise to $Ka_i f$ for each 16-bit blocks. Mathematically, $Kz_i f$ is obtained using (2).

$$Kz_i f = f(Km_i f) \tag{2}$$

4.5 Step-4

We designed KEBF Function as a strategic combination of dual functions PF and QF, as illustrated in Fig. 2. The functional schematic as illustrated in Fig. 2 states a linear (i.e., PF) and non-linear (i.e., QF) functions, respectively. The transformational mechanisms for both PF and QF are

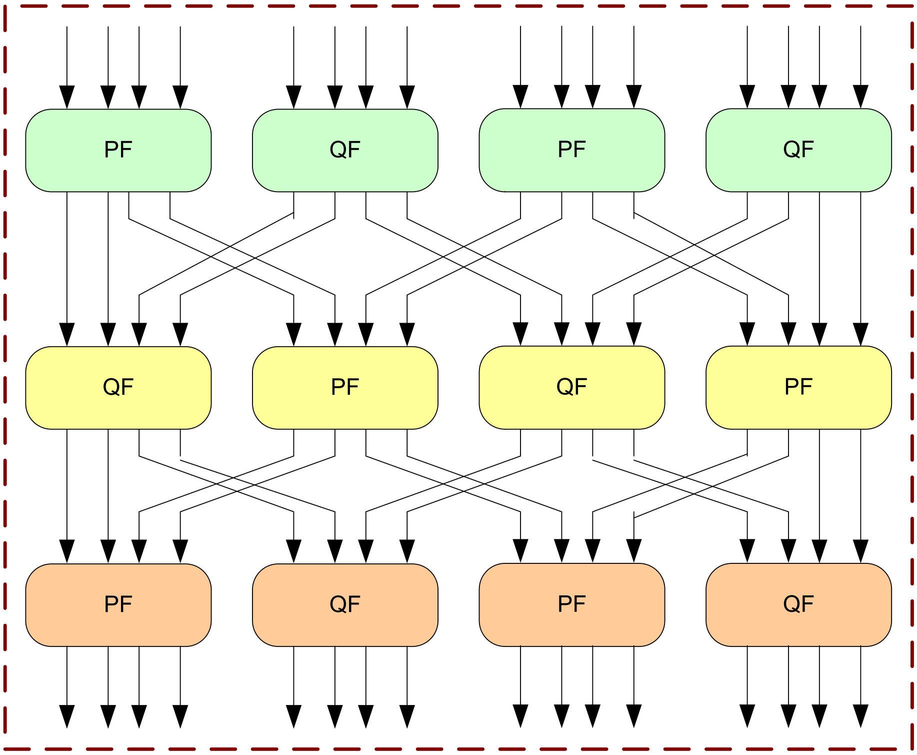


Fig. 2 KEBF function

Table 2 PF function

$k_{n,i\in 1,2,3,4}$	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
$p(k_{n,i\in 1,2,3,4})$	3	F	E	0	5	4	B	C	D	A	9	6	7	8	2	1

Table 3 QF function

$k_{n,i\in 1,2,3,4}$	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
$p(k_{n,i\in 1,2,3,4})$	9	E	5	6	A	2	3	C	F	0	4	D	7	B	1	8

given in Tables 2 and 3, respectively. Thus, obtaining values of PF and QF functional blocks as illustrated in Fig. 2, KEBF has been applied the same way as shown in Fig. 1 to perform encryption.

Once obtaining the KEBF Function for each 16-bit block, the output (of KEBF Function) was re-sampled in 4 × 4 matrix. Mathematically,

$$K_{Mat1}=\begin{bmatrix} Kz_1f_1 & Kz_1f_2 & Kz_1f_3 & Kz_1f_4 \\ Kz_1f_5 & Kz_1f_6 & Kz_1f_7 & Kz_1f_8 \\ Kz_1f_8 & Kz_1f_{10} & Kz_1f_{11} & Kz_1f_{12} \\ Kz_1f_{13} & Kz_1f_{14} & Kz_1f_{15} & Kz_1f_{16} \end{bmatrix} \tag{3}$$

$$K_{Mat2}=\begin{bmatrix} Kz_2f_1 & Kz_2f_2 & Kz_2f_3 & Kz_2f_4 \\ Kz_2f_5 & Kz_2f_6 & Kz_2f_7 & Kz_2f_8 \\ Kz_2f_8 & Kz_2f_{10} & Kz_2f_{11} & Kz_2f_{12} \\ Kz_2f_{13} & Kz_2f_{14} & Kz_2f_{15} & Kz_2f_{16} \end{bmatrix} \tag{4}$$

$$K_{Mat3}=\begin{bmatrix} Kz_3f_1 & Kz_3f_2 & Kz_3f_3 & Kz_3f_4 \\ Kz_3f_5 & Kz_3f_6 & Kz_3f_7 & Kz_3f_8 \\ Kz_3f_8 & Kz_3f_{10} & Kz_3f_{11} & Kz_3f_{12} \\ Kz_3f_{13} & Kz_3f_{14} & Kz_3f_{15} & Kz_3f_{16} \end{bmatrix} \tag{5}$$

$$K_{Mat4}=\begin{bmatrix} Kz_4f_1 & Kz_4f_2 & Kz_4f_3 & Kz_4f_4 \\ Kz_4f_5 & Kz_4f_6 & Kz_4f_7 & Kz_4f_8 \\ Kz_4f_8 & Kz_4f_{10} & Kz_4f_{11} & Kz_4f_{12} \\ Kz_4f_{13} & Kz_4f_{14} & Kz_4f_{15} & Kz_4f_{16} \end{bmatrix} \tag{6}$$

4.6 Step-5

Once obtaining the key matrix, to further retrieve the keys for each 16-bit block (i.e., $K_{Mat1}, K_{Mat2}, K_{Mat3}$ and K_{Mat4}), it has been converted into four distinct arrays of 16 bits. Here we call these arrays as "per-round-key (PRK)". The four distinct keys and allied attribute arrangement is depicted in Eq. (7) to Eq. (10). Noticeably, in below equations the operator # signifies the concatenation.

$$Key_1 = a_4\#a_3\#a_2\#a_1\#a_5\#a_6\#a_7\#a_8\#a_{12}\#a_{11}\#a_{10}\#a_9\#a_{13}\#a_{14}\#a_{15}\#a_{16} \tag{7}$$

$$Key_2 = b_1\#b_5\#b_9\#b_{13}\#b_{14}\#b_{10}\#b_6\#b_2\#b_3\#b_7\#b_{11}\#b_{15}\#b_{16}\#b_{12}\#b_8\#b_4 \tag{8}$$

$$Key_3 = c_1\#c_2\#c_{32}\#c_4\#c_8\#c_7\#c_6\#c_5\#c_9\#c_{10}\#c_{11}\#c_{12}\#c_{16}\#c_{15}\#c_{14}\#c_{13} \tag{9}$$

$$Key_4 = d_{13}\#d_9\#d_{52}\#d_1\#d_2\#d_6\#d_{10}\#d_{14}\#d_{15}\#d_{11}\#d_7\#d_3\#d_4\#d_8\#d_{12}\#d_{16} \tag{10}$$

Now, estimating the key values, we have performed XOR logical operation amongst the four distinct keys (each for one round) as obtained above (7–10) to get a Fused-Key (11).

$$Key_5 = \oplus_{i=1}^{4} Ki \tag{11}$$

4.7 Data encryption

Once retrieving the keys per round, data encryption was performed. For confusion and diffusion over encryption process, we applied different logical functions such as shifting (left–right), entity-swapping and substitution. The overall encryption process is illustrated in Fig. 3. As illustrated in Fig. 3, for the first round of operation the 64 bit plain text (Pt) is split into four chunks containing 16 bits distinctly, (i.e., Px_{0-15}, Px_{16-31}, Px_{32-47} and Px_{48-63}). Progressing over bits operation in each round, the proposed model performs swapping to reduce the data originality by means of bit's order-alteration. It increased confusion in cipher text. Meanwhile, it performs bitwise XNOR logical operation in between the corresponding round key Key_i and Px_{0-15}. This process is repeated between K_i and Px_{48-63} to generate Ro_{11} and Ro_{14}, respectively. Once obtaining the output from XNOR logical operator it is fed to the KEBF block (Fig. 3), and generates two distinct outputs Ef_{l1} and Ef_{r1}. Noticeably, KEBF applied for encryption is same as used for KEBF (say, key expansion function), with

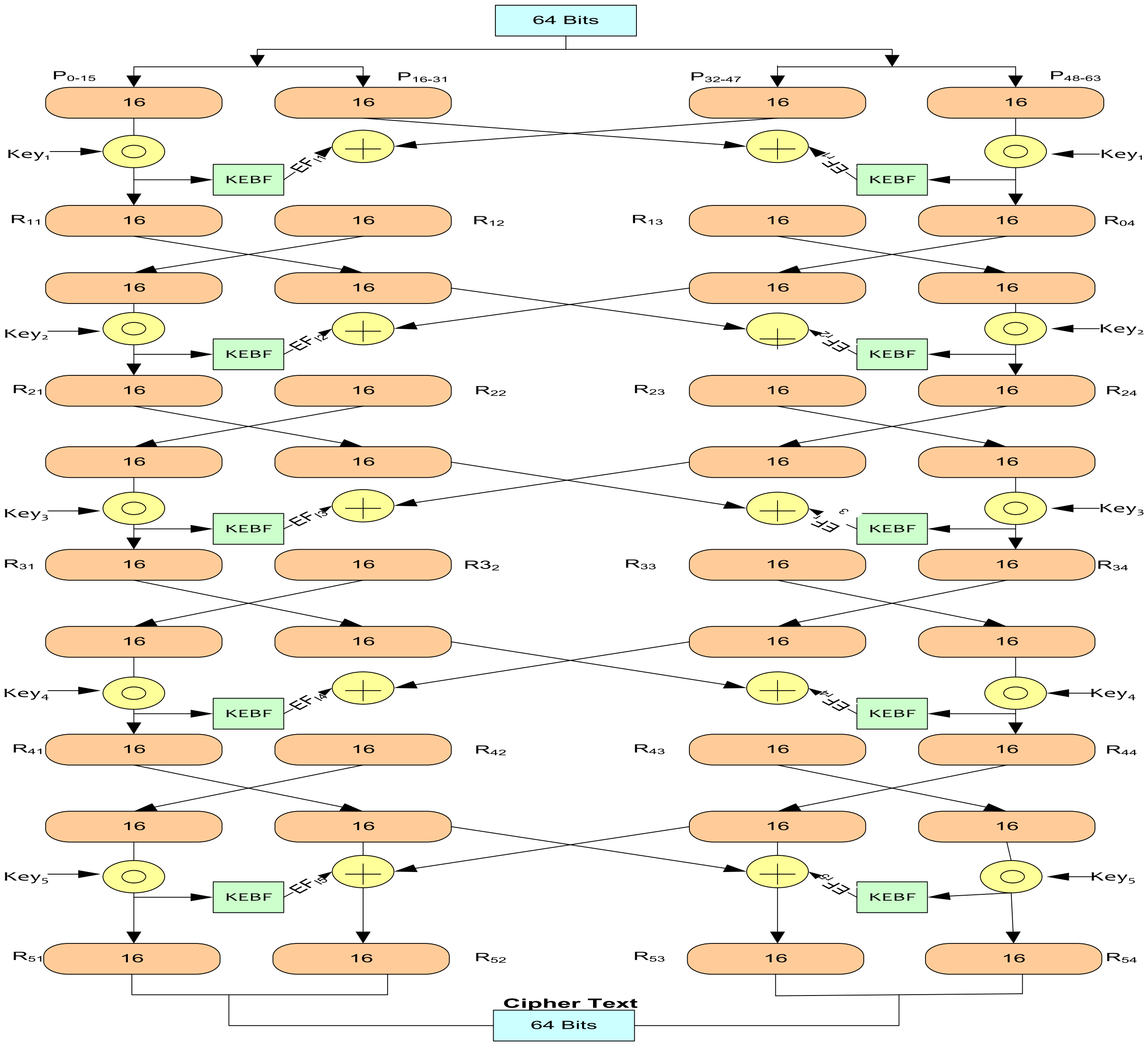


Fig. 3 Feistel network assisted data encryption

processes like swapping and substitution. Now, with the obtained Ef_{11}& Px_{32-47}, we performed bitwise XOR to obtain Ro_{12}, while the same in between Ef_{r1} and Px_{16-31} provided Ro_{13} (Fig. 3).

$$Ro_{i,j} = \begin{cases} Px_{i,j} \odot K_i; & j = 1 \text{ and } 4 \\ Px_{i,j+1} \oplus Ef_{li}; & j = 2 \\ Px_{i,j-1} \oplus Ef_{ri}; & j = 3 \end{cases} \tag{12}$$

Thus, after processing above methods, a transformation process was executed in such manner that for each subsequent round Ro_{11} turns out to be Px_{16-31}, while Ro_{12} becomes Px_{0-15}, Ro_{13} as Px_{48-63}, and Ro_{13} as Px_{32-47}. This process is continued for all remaining rounds as per (12), and thus the eventual result of final round are concatenated to form the final cipher text (CT) to be used for further communication (13).

$$CT = R_{51} \# R_{52} \# R_{53} \# R_{54} \tag{13}$$

The detailed discussion of the simulation results and its inferences is given in the sub-sequent section.

Noticeably, with Feistel structure our proposed (block cipher) model exhibits decryption in the same way as encryption, though the structural sequence reverses the earlier (i.e., encryption). It reduces overall computation significantly making it lightweight and more cost-efficient.

5 Results and discussion

Considering the significance of a robust and lightweight security model for multimedia data security over cloud, in this research we focused on exploiting the efficacy of the advanced crypto-concepts such as Substitution and Permutation based diffusion to enable robust image encryption-decryption for attack-resiliency. To further strengthen the robustness under uncertain cloud environment we applied diffusion concept based on the well-known Feistel structure that performed Substitution Permutation based data encryption. To maintain lower computational overhead, our proposed model applied merely five rounds with 64-bit encryption. We applied Feistel structure to perform Substitution Permutation over multiple rounds so as to perform high level confusion and diffusion. As already stated, unlike classical RSA 256 bit or AES-256 models, we applied merely 64-bit block cipher and equally key-size which retained high computational efficiency with augmented security. The proposed crypto-model was developed using MATLAB 2019b tool, which was tested with both generic multimedia data as well as biomedical datasets such as diabetic retinopathy, glaucoma, MRI data etc. The performance of the proposed security model was examined qualitatively as well as quantitatively or empirically by simulating over benchmark datasets. The overall proposed model was simulated over Microsoft Operating System (OS) Windows 2010, with processor Intel – i3, with 8 GB RAM. Though, the computation time (Table 8) may be higher with better or more advanced processors like Intel i5 or i8. The detailed discussion of the performance assessment is given in the subsequent sections.

5.1 Quantitative assessment

To assess efficacy of the proposed multimedia data security model, we at first examined it for statistical performance parameters such as cipher generation, entropy, correlation and histogram results. To perform this assessment, we tested performance with different input images pertaining to normal life as well as biomedical significances such as fundus images, Magnetic Resonance Imaging (MRI) etc. As normal (daily) life images the standard images like Lena, Baboon, Panda, which are the well-known benchmark data for image analysis were tested. Noticeably, before executing our proposed crypto-model at first input images were converted into Gray from standard RGB data. Though, certain sophisticated pre-processing could have enabled better input environment; however since the focus of this research was to design security model, no pre-processing such as resizing, intensity equalization etc.was performed. As statistical performance assessment, we obtained key features like key sensitivity, image entropy, correlation, image histogram etc. Before discussing the simulation results, a snippet of the above stated statistical parameters is given as follows

To assess performance of the proposed multimedia data security model, we have considered images of the different types, encompassing general images as well as medical images as these two different types of inputs have distinct demands. In other words, the normal life data such as object data, person's images etc.can have certain (limited or definite) image quality trade off after communicating over the cloud platform. On contrary, image data demands seamless and quality-centric communication as even a minute difference in image spatio-temporal feature might decisively impact assessment and eventual decision. Such miss-location or min-information might force professionals to make wrong telemedicine decision. Considering these facts, in this paper we considered different types of inputs encompassing benchmark images like Lena, Baboon, Panda, Cameraman, three different fundus images retrieved from DRISTI-GS datasets and Medical Resonance Imaging (MRI) data available online. The input images were at first processed for pre-processing where those were converted from RGB to Gray form, and were resized to 256 × 256 dimension. Noticeably, the considered images were in *.PNG and *.JPG formation; though the proposed algorithm could process any form of input image data. Once exhibiting pre-processing, the images were processed for respective encryption and decryption hypothesizing communication to be made over uncertain cloud framework or platform. Thus, with the simulated results we obtained performance outcome in terms of entropy, correlation, NPCR and UACI along with the corresponding histogram outputs. Before discussing the simulation results, a snippet of the different statistical as well as visual assessment parameters used in this research is given as follow.

5.1.1 Entropy

As multimedia security process undergoes cipher generation which can significantly increase the disturbances across the image input. This as a result can cause increase in image entropy which not only degrades (image) quality but also broadens horizon for intruders to attack specific data. On the other hand, encryption imposes additional information to the multimedia data so as to make it complex for the intruder to distinguish the encrypted data and the original multimedia information. In such cases, maintaining the optimal entropy with the data under transmission is must. With this motive, in this paper we estimated entropy for each encrypted data to retain quality-centric multimedia data security (14).

$$ENT(I) = -\sum_{i=1}^{2^8} P(I_i)\log_b P(I_i) \quad (14)$$

In (14), $ENT(I)$ states the entropy of an image, where I signify the intensity, and $P(I_i)$ signifies the probability of the intensity value I_i.

5.1.2 Correlation

Correlation being a statistical parameter signifies the dependencies, inter-relationship or correlation between two distinct values. Typically, a data element or point possessing significant dependency signifies significant correlation. Towards multimedia security it is important to remove dependency of the cipher information from the original image. With such minimal dependency, no significant information can be extracted, which strengthens the data security feature. In this paper, we obtained the correlation coefficient γ in between the original multimedia data and encrypted data using (15). For an optimal condition γ must be maintained either equal or near zero. Correlation coefficient of one signifies the worst cipher condition.

$$\gamma_{x,y} = \frac{cov(x,y)}{\sqrt{D(x)\sqrt{D(y)}}} \quad (15)$$

In (15), $cov(x,y)$ states the covariance value, while $D(x)$ and $D(y)$ states the variances for the variable x and y, correspondingly. In general, the distribution of the variance of any single dimension arbitrary variable is obtained using (16).

$$D(x) = \frac{1}{N}\sum_{i=1}^{N}(x_i - E(x))^2 \quad (16)$$

In (16), $D(x)$ states the variance value for random variable x. To estimate covariance between two distinct arbitrary values x and y, we apply (17).

$$cov(x,y) = \frac{1}{N}\sum_{i=1}^{N}(x_i - E(x))(y_i - E(y)) \quad (17)$$

In (17), $E(x)$ and $E(y)$ states the expected values for x and y random values. Expectation values can be obtained as per (18).

$$E(x) = \frac{1}{N}\sum_{i=1}^{N}x_i \quad (18)$$

In (18), N signifies the total number of pixels in the image, which is usually estimated as $N = Row \times Column$, and x states the N-dimensional vector. x_i refers the i th intensity value of the original multimedia data or image.

5.1.3 Image histogram analysis

Histogram variation analysis enables examining visual effect of the cipher so as to encrypt an image and assess the randomness it causes in the original image after encryption. We applied image histogram analysis model to visualize the introduced randomness within the original image. Here, we intend to maintain minimum or negligible histogram difference after encryption to retain better security and visual perception based attack probability.

5.1.4 Number of changing pixel rates (NPCR) and the unified average channel intensity (UACI)

NPCR and UACI are the randomness test measures often applied to assess differential attack resilience by an image encryption technique. Higher NPCR signifies more resilience towards differential attacks. The details of these randomness tests can be found in [73].

Table 4 presents the simulated results for the different input images and respective visual outcomes in the form of image histograms. Table 4 depicts the original inputs, histogram of the original inputs, encrypted image and its (encrypted) histogram results. As depicted (Table 4), we considered a total of nine images with different natures (normal, MRI and Fundus (for diabetic or Glaucomatic detection)). As depicted in the results (Table 4), after encryption the histogram of the cipher data is quite different making it imperceptible for an attacker to gain cipher access.

Table 5 presents the entropy level of the original images as well as corresponding encrypted image. As observed through the results (Table 5), the entropy level increases for encrypted images which helps introducing confusion to avoid easy detection of the original data. Noticeably, there are the different approaches advocating maintaining either low negligible entropy (such as steganography based approaches) or high entropy which is often considered in cryptography methods. The results affirm suitable entropy condition to avoid any detection by attacker over uncertain cloud conditions. In our proposed model, we considered 8 bits gray scale image which can have the highest entropy of 8 bits. Observing Table 5, it can be found that the highest entropy obtained over test cases is 7.99 (for encrypted images), which is fulfilling the above stated entropy condition for a quality-centric and secure multimedia data communication.

The correlation analysis of the proposed multimedia security model is given in Table 6. As already stated that for any encryption model achieving higher correlation difference can enable high-imperceptibility and hence high attack-resilience. As depicted through the results (Table 6), the proposed model shows significantly large correlation

Table 4 Histogram analysis

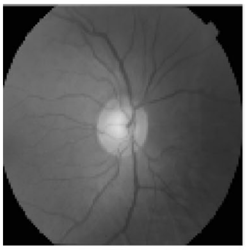
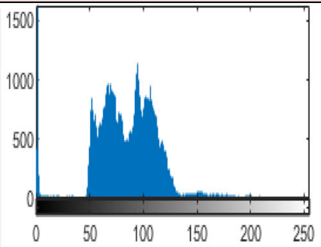
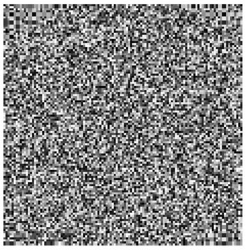
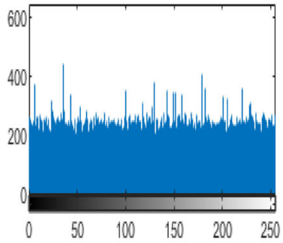
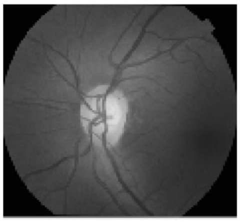
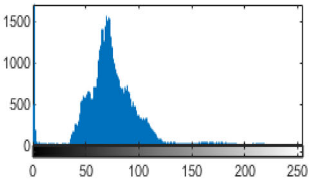
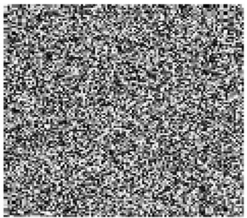
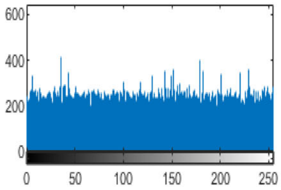
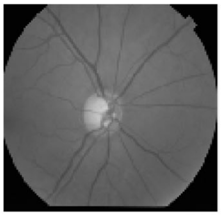
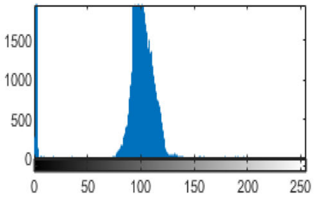
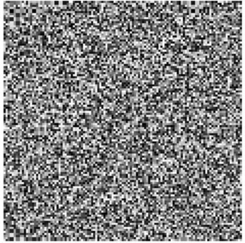
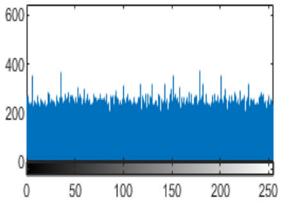
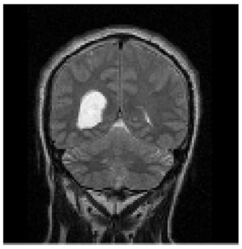
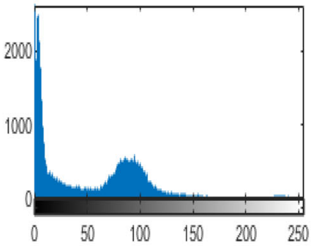
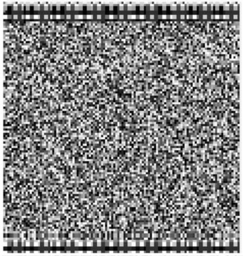
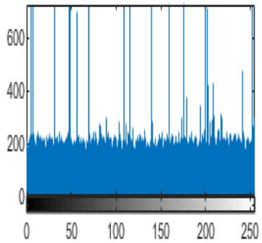
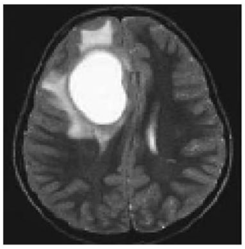
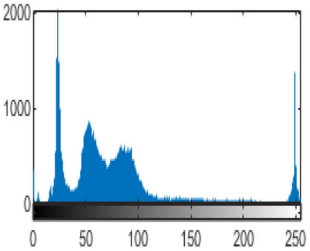
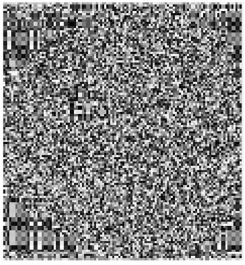
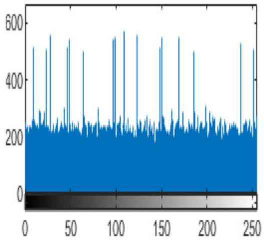
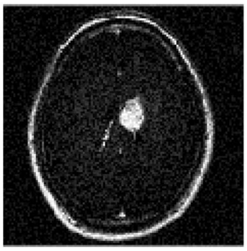
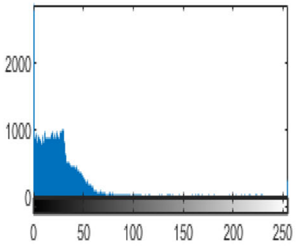
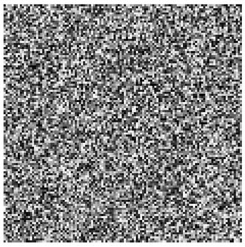
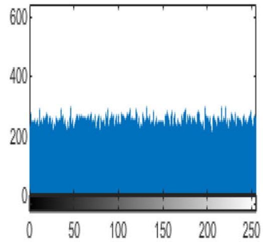
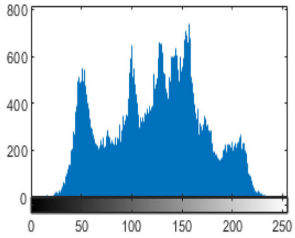
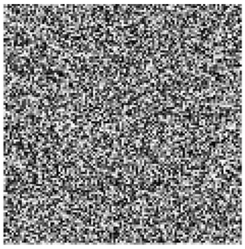
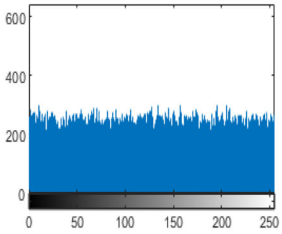
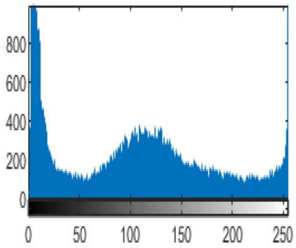
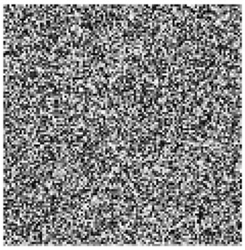
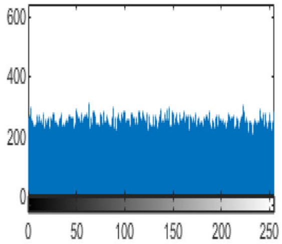
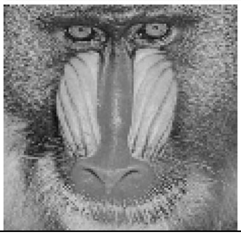
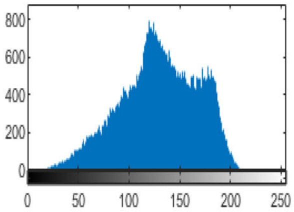
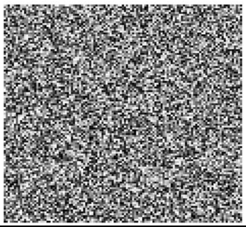
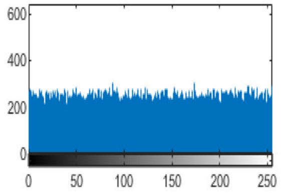
Dataset	Original Image (8 Bits gray scale image with 256 × 256 size)	Image Histogram	Encrypted Image	Encrypted Data Histogram
Fundus1				
Fundus2				
Fundus3				
MRI1				
MRI2				
MRI3				

Table 4 continued

Lena				
Panda				
Baboon				

difference, signifying it robustness towards high attack resilience.

In addition to the above discussed visual and statistical characterization we have examined efficacy of our proposed multimedia (data) security model in terms of the Number of Changing Pixel Rates (NPCR) and the Unified Average Channel Intensity (UACI) in Table 7. Typically, high value of NPCR and UACI signifies higher randomness and hence high resilience against any differential attack probability [73]. The randomness test results with higher value of NPCR backs up the attack resiliency nature of the proposed system. Similarly, UACI too confirms satisfactory performance. The detailed discussion of NPCR and UACI conditions for image randomness during encryption can be found in [73]. Thus, the above discussed robustness confirms suitability of the proposed security model for any real-time multimedia communication, including our intended cloud communication purposes.

The encryption time is depicted in Table 8. Noticeably; the proposed model can be executed over more advanced processors such as Intel-i5 and i8 to achieve better time efficiency.

5.2 Qualitative assessment

In previous section the performance of the proposed security system was examined in terms of the different statistical as well as visual parameters. The simulation results affirmed that the proposed model accomplishes optimal performance while retaining high security with low visual perception and entropy, confirming suitability of the proposed security system for cloud computing environment. Now, realizing the need to characterize efficacy in terms of attack-resiliency, we performed qualitative assessment, where the proposed model has been examined for its robustness towards any breach-probability caused due to linear and differential cryptanalysis (Ex. RS analysis), Interpolation attacks, Weak key combination, square attacks and related key attack conditions.

Typically, the prime objective of cipher in security system is to ensure attack-resiliency and protection of the plaintext. In classical cloud environment, attacker often intercepts the cipher-text being transmitted through or over multimedia data and intends to extract or recover the text, though the target data or information can be in other form as well such as image bits or multimedia specific text presentation. Functionally, a cipher can be stated to be breached in case the attacker gets access or becomes able to retrieve the secret key. The situation when an attacker

Table 5 Image entropy analysis

Dataset	Original image entropy	Encrypted image entropy
Fundus1	6.3510	7.9898
Fundus2	6.2515	7.9913
Fundus3	5.4312	7.9936
MRI1	6.0468	7.1053
MRI2	6.3670	7.9514
MRI3	6.1031	7.8990
Lena	7.3904	7.6730
Panda	7.4938	7.9968
Baboon	7.1020	7.8993

Table 6 Correlation analysis

Dataset	Original image correlation	Correlation post-encryption
Fundus1	0.9920	0.0076
Fundus2	0.9918	0.0072
Fundus3	0.9883	0.0036
MRI1	0.9763	0.0336
MRI2	0.9929	0.0100
MRI3	0.8628	0.0031
Lena	0.9743	0.0041
Panda	0.9811	0.0003
Baboon	0.8198	0.0039

Table 7 NPCR and UACI randomness test

Dataset	NPCR (%)	UACI (%)
Fundus1	99.60	25.77
Fundus2	99.63	28.32
Fundus3	99.63	23.81
MRI1	99.59	36.61
MRI2	99.43	28.60
MRI3	99.63	41.06
Lena	99.52	14.87
Panda	99.62	13.31
Baboon	99.62	22.62

Table 8 Execution time (system configuration Intel dual core)

Dataset	Time (ms)
Fundus1	87.97
Fundus2	72.60
Fundus3	70.63
MRI1	89.45
MRI2	71.06
MRI3	77.64
Lena	89.40
Panda	88.48
Baboon	82.26

becomes capable enough to decrypt the cipher-text without estimating the secret key, the cipher is hypothesized to be breached partially. Considering cloud communication environment, we hypothesize that the attacker possesses unobstructed access of the data under transmission across the channel. Additionally, the attacker can also have key information; however to assess the security of a cipher, it is significant to consider computational efficacy of the attacker. Unlike classical crypto-models, our proposed model inherits the strength of both Uniform Substitution and Permutation model as well as Feistel structure (with multiple rounds) it strengthens attack resilience. The robustness of the proposed model can be characterized in terms of its efficacy to avoid the following attack conditions.

5.2.1 Differential and linear (regular and singular) cryptanalysis

As already discussed in the previous section the KEBF function is developed based on the suggestions provided in [73], which itself justifies its robustness to avoid any kind of Differential and Linear (Regular and Singular) Cryptanalysis, our proposed security model can be considered to be robust enough to avoid any aforesaid attack probability. Moreover, as depicted in above discussion the correlation in between the original image data and the cipher data is significantly large even if the linear approximation is performed for two rounds. Since, we performed five distinct rounds of computation; it strengthened the proposed model to exhibit high correlation and hence more attack resilience. Additionally, since the (each) round transformation is maintained uniform which enables treating each bit similar and hence facilitates resilience to the differential attack. The results obtained in terms of NPCR and UACI, as discussed above reveals that the proposed security model can have sufficient resilience to avoid any kind of differential attacks problems in cloud environment. To be noted, correlation test, NPCR and UACI assessment are especially designed approach for differential attack analysis. The comparative performance assessment of the proposed security system as well as other existing approaches is given in Section C (Inter-Model Performance Assessment).

5.2.2 Weak key combination

In cloud computing environment users make a common mistake by keeping poor or weak key combination that helps attacker to get easy access to the ciphers. On contrary, the cipher information where the non-linear operations usually rely on the key value maps the block cipher in such manner that it causes detectable weakness. On the other hand, looking into the proposed security model where it avoids using the same (actual) key in the cipher (due to multiple round key manipulation and/or exchange by XORing the actual key followed by KEBF for five rounds). It makes proposed system robust enough to avoid any kind of weak-key attack probability. On the other hand, in the proposed KEBF function non-linearity is fixed significantly and thus there becomes no limitation on the key-selection.

5.2.3 Related keys combination trial attack

This is the matter of fact that the attack can be made with the help of certain partially known or unknown keys as well. The related keys primarily depend on either slow diffusion or possessing symmetry in key expansion block, as discussed in the previous section. In our proposed security model, we crafted the key expansion mechanism in such manner that it retains fast computation and non-linear diffusion, especially for the cipher key difference in comparison to the round keys that makes significant confusion to assess related key for data attack.

5.2.4 Square-attack

To assess efficacy of a security model, different attack modules are applied to investigate attack-resiliency by the proposed approach. Some of the key approaches applied in cloud-sensitive security models are the RS-Analysis and Square Attack. Considering Square Attack condition, it is capable enough to retrieve one byte of the last key combination and intends to retrieve or recover rest of the keys by repeating the attack iteratively. Let, such repetition be eight times, then also to achieve above stated information, the attacker needs to identify 28 keys precisely by 28 plaintexts which is equivalent to 216- S-box lookups. This becomes highly complicate and thus our proposed model avoids such attack probability.

5.2.5 Interpolation attack

In general, such kinds of attacks primarily rely on the generic architecture of the cipher components which could generate certain rational expression with relatively low complexity. However, as already discussed the S-box expression of the proposed security system with diffusion characteristics strengthen it to avoid such limitations and thus makes it impracticable enough to avoid attack.

5.3 Inter-model performance assessment

Though, the proposed multimedia data security model encompasses novelties at the different level of computation, to assess its relative performance we considered some researches functional on the same motive "lightweight-encryption". To achieve it, we referred a work done by Noura et al. [58], who applied dynamic structure based lightweight encryption system, titled "A new efficient lightweight and secure image cipher scheme". As dynamic structure solution, authors applied forward and backward chaining block (FBC) that in conjunction with a permutation block enabled image encryption. In their proposed model, authors enabled change of the key for each input, which were applied subsequently to generate cipher layer. Noticeably, their proposed cipher layer comprised a binary diffusion matrix, substitution box and permutation box, in sequence. Authors [57, 58] stated that their proposed model with binary diffusion matrix, substitution and permutation table could achieve better performance (with two-rounds). Considering a common test case of "Lena.jpg" image data, which has been considered in our proposed model as well, we examined peak signal to noise ratio (PSNR) performance for the proposed security model as well as the existing [57] one in Table 9. Mathematically, we estimated PSNR using function.

$$PSNR = 10\log_{10}\frac{M \times N \times 255^2}{\sum_{i,j} y_{i,j} - {x_{i,j}}^2}$$

In (19), the variable M and N states the image dimensions, while x and y are the before and after encryption positions. To assess performance, we considered maximum (Max) PSNR to assess relative performance.

Observing the result, it can easily be found that our proposed multimedia security model retains higher PSNR than the both existing methods [57, 58]. Similar to [58, 59], authors [61] developed a dynamic approach for a lightweight and secure cipher for medical images. Authors at first identified sensitive region as well as non-sensitive regions over the target image based on average of the sub-matrix in reference to a predefined threshold level.

Table 9 PSNR assessment

Data	PNSR		
Lena.jpg	[57]	[58]	Proposed
	9.2604	8.6054	9.8610

Towards encryption of the image, authors applied dynamic structure-based concept. In fact, most of the key contributions of this work was same as [58]; though authors assess performance over different medical images. In their simulation, authors could achieve NPCR between the original and the cipher image as 50.1029, while UACI for the same sample was obtained as 99.6460. Entropy performance was found to be within the range of 7 to 7.3. Observing these results, our proposed system seems to be superior with lower entropy and differential attack resilience. Similar to the work in [57, 58], authors developed a dynamic structure-based encryption model for fingerprint security [59]. In this method, authors [59] where applied shifting concept for image encryption. Since, the exiting work [59] and our proposed model applied different data, direct comparison can't be done; however as relative performance analysis it can be found that the entropy of our proposed security model (Minimum observed entropy = 7.1053) is lower than the existing method ([59], 7.6448). In [60] as well authors claimed their approach as "lightweight" where chaos and Deoxyribo Nucleic Acid (DNA) computing (it states a dynamic structure model) for image encryption. Authors [60] considered benchmark Lena.jpg image for system test, where they obtained performance outcome in terms of NPCR, UACI and entropy (characterizing differential attack assessment).

Observing above results (Table 10) it can easily be found that the proposed image encryption model outperforms existing approaches by maintaining lower entropy with satisfactory higher correlation performance to avoid differential attack condition over cloud platforms. The NPCR and UACI results affirms the robustness of the proposed multimedia data (image) security model towards (differential) attack-resilience. Thus, observing overall performance and corresponding inferences, it can be affirmed that the proposed multimedia encryption model is more efficient than the other existing approaches. It enables our proposed security model to be applied in real-world cloud computing environment.

The overall research inference and conclusion is given in the subsequent section.

Table 10 Comparative assessment

Data	Method	Entropy	Correlation	NPCR	UACI
Lena.jpg	[60]	7.9992	0.0011	99.7570	0.3912
	Proposed	7.6730	0.0041	99.5200	0.1487
Baboon.jpg	[60]	7.9993	0.0015	98.0961	0.7702
	Proposed	7.8993	0.0039	99.6200	0.2262

6 Conclusion

Considering the significance of a secure multimedia communication environment over cloud environment, which has gained widespread attention globally, this research focused on designing a lightweight and robust "multimedia data security system". Unlike classical researches where to enhance security level authors have either increased key size or have exploited hybrid cryptosystems. Unfortunately, such approaches impose significantly high computational overheads and complexity. On contrary, cloud computing demands lightweight and computationally efficient security solution, especially for multimedia data transmission. Considering it as motive, in this research paper a robust multimedia data security model was developed by exploiting efficacy of the block cipher approach using substitution and permutation network (SPN) and Feistel structure. Similar to the block-cipher approaches such as AES, Grasshopper, SAFER, SHARK and Square attack methods etc., our proposed model employs SPN network in which the use of multiple-round or iterative substitution and transposition enabled Shannon's confusion and diffusion conditions. It enabled changing the cipher text in certain pseudo-random paradigm. To achieve it, this method applied Feistel architecture, which performs both encryption as well as decryption in similar manner. Thus, the use of Feistel architecture and SPN network provided a hybrid security system which applied 64-bit key processing with most robust attack-resiliency for multimedia data communication over cloud. The qualitative and quantitative assessment of the proposed security model affirms its suitability towards secure multimedia data communication over cloud computing environment while assuring low computational overheads and complexity. The proposed model also ensures different attack resiliency and hence is robust enough to be used under uncertain cloud environment.

References

1. Sajjad, M., Muhammad, K., Baik, S. W., et al. (2017). Mobile-cloud assisted framework for selective encryption of medical images with steganography for resource-constrained devices. *Multimed Tools Appl, 76,* 3519–3536. https://doi.org/10.1007/s11042-016-3811-6
2. Darwish, A., Hassanien, A. E., Elhoseny, M., et al. (2019). The impact of the hybrid platform of internet of things and cloud computing on healthcare systems: opportunities, challenges, and open problems. *J Ambient Intell Human Comput, 10,* 4151–4166. https://doi.org/10.1007/s12652-017-0659-1
3. Anwar, A. S., Ghany, K. K. A., & El Mahdy, H. (2015). Improving the security of images transmission. *Int. J. Bio-Med. Inform. e-Health, 3*(4), 7–13.

4. Bairagi, A. K., Khondoker, R., & Islam, R. (2016). An efficient steganographic approach for protecting communication in the Internet of Things (IoT) critical infrastructures. *Information Security Journal: A Global Perspective, 25*(4–6), 197–212. https://doi.org/10.1080/19393555.2016.1206640
5. Paschou, M., Sakkopoulos, E., Sourla, E., & Tsakalidis, A. (2013). Health Internet of Things: Metrics and methods for efficient data transfer. *Simulation Modelling Practice and Theory, 34,* 186–199. https://doi.org/10.1016/j.simpat.2012.08.002
6. Parah S.A., Sheikh J.A., Ahad F., Bhat G.M. (2018) High Capacity and Secure Electronic Patient Record (EPR) Embedding in Color Images for IoT Driven Healthcare Systems. In: Dey N., Hassanien A., Bhatt C., Ashour A., Satapathy S. (eds) Internet of Things and Big Data Analytics Toward Next-Generation Intelligence. Studies in Big Data, vol 30. Springer, Cham. https://doi.org/https://doi.org/10.1007/978-3-319-60435-0_17
7. Li, L., Hossain, M. S., El-Latif, A. A. A., et al. (2019). Distortion less secret image sharing scheme for Internet of Things system. *Cluster Comput, 22,* 2293–2307. https://doi.org/10.1007/s10586-017-1345-y
8. Gupta, R. K., & Singh, P. (2013). "A new way to design and implementation of hybrid crypto system for security of the information in public network", International Journal of Emergency. *Technology Advanced Engineering, 3*(8), 108–115.
9. Muhammad Sajjad, Mansoor Nasir, Khan Muhammad, Siraj Khan, Zahoor Jan, Arun Kumar Sangaiah, Mohamed Elhoseny, Sung Wook Baik, Raspberry Pi assisted face recognition framework for enhanced law-enforcement services in smart cities, Future Generation Computer Systems, Volume 108, 2020, Pages 995–1007, ISSN 0167–739X, https://doi.org/https://doi.org/10.1016/j.future.2017.11.013.
10. Laskar, S. (2012). High Capacity data hiding using LSB Steganography and Encryption. *International Journal of Database Management Systems., 4,* 57–68. https://doi.org/10.5121/ijdms.2012.4605
11. B. Xue, X. Li and Z. Guo, "A New SDCS-based Content-adaptive Steganography Using Iterative Noise-Level Estimation," 2015 International Conference on Intelligent Information Hiding and Multimedia Signal Processing (IIH-MSP), Adelaide, SA, 2015, pp. 68–71, doi: https://doi.org/10.1109/IIH-MSP.2015.80.
12. Vipula Madhukar Wajgade, "Enhancing Data Security Using Video Steganography," International Journal of Emerging Technology and Advanced Engineering Volume 3, Issue 4, April 2013.
13. Lokesh Kumar, "Novel Security Scheme for Image Steganography using Cryptography technique", International Journal of Advanced Research in Computer Science and Software Engineering , Volume 2, Issue 4, April 2012 ISSN: 2277 128X.
14. Marwa E. Saleh, Abdelmgeid A. Aly and Fatma A. Omara, "Data Security Using Cryptography and Steganography Techniques" International Journal of Advanced Computer Science and Applications (IJACSA), 7(6), 2016. http://dx.doi.org/https://doi.org/10.14569/IJACSA.2016.070651
15. M. E. Saleh, A. A. Aly, and F. A. Omara, "Enhancing Pixel Value Difference (PVD) Image Steganography by Using Mobile Phone Keypad (MPK) Coding," International Journal of Computer Science and Security (IJCSS), Volume (9), Issue (2), pp. 397 - 397, 2015
16. A. Duluta, S. Mocanu, R. Pietraru, D. Merezeanu and D. Saru, "Secure Communication Method Based on Encryption and Steganography," 2017 21st International Conference on Control Systems and Computer Science (CSCS), Bucharest, 2017, pp. 453–458, doi: https://doi.org/10.1109/CSCS.2017.70.
17. Dhvani Panchal, "An Approach Providing Two Phase Security of Images Using Encryption and Steganography in Image Processing", 2015 IJEDR, Volume 3, Issue 4, ISSN: 2321–9939.
18. Y. Leung and R. Y. Hou, "Unequal security protection for secure multimedia communication," 2015 IEEE 4th Global Conference on Consumer Electronics (GCCE), Osaka, 2015, pp. 570–571, doi: https://doi.org/10.1109/GCCE.2015.7398667.
19. Mukhedkar, M., Powar, P., Gaikwad, P., & "Secure non real time image encryption algorithm development using cryptography & steganography", . (2015). Annual IEEE India Conference (INDICON). *New Delhi, 2015,* 1–6. https://doi.org/10.1109/INDICON.2015.7443808
20. Li, J., Guo, X., Yu, Y., Tu, Q., Men, A., & "A robust and low-complexity video fingerprint for multimedia security", . (2014). International Symposium on Wireless Personal Multimedia Communications (WPMC). *Sydney, NSW, 2014,* 97–102. https://doi.org/10.1109/WPMC.2014.7014798
21. D. E. M. Ahmed and O. O. Khalifa, "Robust and Secure Image Steganography Based on Elliptic Curve Cryptography," 2014 International Conference on Computer and Communication Engineering, Kuala Lumpur, 2014, pp. 288–291, doi: https://doi.org/10.1109/ICCCE.2014.88.
22. Hajduk, V., Broda, M., Kovac, O., Levicky, D., & "Image steganography with using QR code and cryptography." (2016). 26th International Conference Radioelektronika (RADIOELEKTRONIKA). *Kosice, 2016,* 350–353. https://doi.org/10.1109/RADIOELEK.2016.7477370
23. M. S. Alam, "Secure M-commerce data using post quantum cryptography," 2017 IEEE International Conference on Power, Control, Signals and Instrumentation Engineering (ICPCSI), Chennai, 2017, pp. 649–654, doi: https://doi.org/10.1109/ICPCSI.2017.8391793.
24. N. Kumar and S. Agrawal, "An efficient and effective lossless symmetric key cryptography algorithm for an image," 2014 International Conference on Advances in Engineering & Technology Research (ICAETR - 2014), Unnao, 2014, pp. 1–5, doi: https://doi.org/10.1109/ICAETR.2014.7012788.
25. D. Sharma and D. Sharma, "Steganography of the keys into an encrypted speech signal using Matlab," 2016 3rd International Conference on Computing for Sustainable Global Development (INDIACom), New Delhi, 2016, pp. 721–724.
26. Z. Wang, J. Liu, W. Wan, J. Sun, J. Bo and Y. Liu, "Security Monitoring by Watermarking and Hashing for Multimedia Service on Internet Platform," 2014 Tenth International Conference on Intelligent Information Hiding and Multimedia Signal Processing, Kitakyushu, 2014, pp. 630–633, doi: https://doi.org/10.1109/IIH-MSP.2014.163.
27. A. A. Zaher, "A cryptography algorithm for transmitting multimedia data using quadruple-state CSK," 2015 International Conference on Computer, Communications, and Control Technology (I4CT), Kuching, 2015, pp. 87–92, doi: https://doi.org/10.1109/I4CT.2015.7219543.
28. M. B. Hossain, M. T. Rahman, A. B. M. S. Rahman and S. Islam, "A new approach of image encryption using 3D chaotic map to enhance security of multimedia component," 2014 International Conference on Informatics, Electronics & Vision (ICIEV), Dhaka, 2014, pp. 1–6, doi: https://doi.org/10.1109/ICIEV.2014.6850856.
29. P. Saxena, D. Shahane, S. Rai and R. Boghey, "Enhancing image security using data compression and spread spectrum watermarking technique," 2017 7th International Conference on Communication Systems and Network Technologies (CSNT), Nagpur, 2017, pp. 215–219, doi: https://doi.org/10.1109/CSNT.2017.8418540.
30. S. Gupta and R. Jain, "An innovative method of Text Steganography," 2015 Third International Conference on Image Information Processing (ICIIP), Waknaghat, 2015, pp. 60–64, doi: https://doi.org/10.1109/ICIIP.2015.7414741.

31. Ashwini, Bhadane et al. "A Hybrid Approach for Enhancing Data Security by Combining Encryption and Steganography." (2014).
32. J. Joshi, K. Nair, M. Warde, V. Rawalgaonkar and J. Kulkarni, "Secure semi-blind steganography using chaotic transforms," 2016 3rd International Conference on Computing for Sustainable Global Development (INDIACom), New Delhi, 2016, pp. 2669–2673.
33. N. Rashmi and K. Jyothi, "An improved method for reversible data hiding steganography combined with cryptography," 2018 2nd International Conference on Inventive Systems and Control (ICISC), Coimbatore, 2018, pp. 81–84, doi: https://doi.org/10.1109/ICISC.2018.8398946.
34. R. S. Phadte and R. Dhanaraj, "Enhanced blend of image steganography and cryptography," 2017 International Conference on Computing Methodologies and Communication (ICCMC), Erode, 2017, pp. 230–235, doi: https://doi.org/10.1109/ICCMC.2017.8282682.
35. Saraireh, S. (2013). A Secure Data Communication System Using Cryptogaphy And Steganography. *International journal of Computer Networks & Communications., 5,* 125–137. https://doi.org/10.5121/ijcnc.2013.5310
36. G.Sateesh, E.Sai Lakshmi, M.Ramanamma, K.Jairam, A.Yeswanth "Assured Data Communication Using Cryptography and Steganography" International Journal of Latest Technology in Engineering, Management & Applied Science-IJLTEMAS vol.5 issue 3, pp.102–106 2016.
37. Shamim Ahmed Laskar, "Secure Data Transmission Using Steganography and Encryption Technique", International Journal on Cryptography and Information Security (IJCIS), Vol.2, No.3, September 2012.
38. S. D. Torvi, K. B. ShivaKumar and R. Das, "An unique data security using text steganography," 2016 3rd International Conference on Computing for Sustainable Global Development (INDIACom), New Delhi, 2016, pp. 3834–3838.
39. S. Pleshkova and D. Kinanev, "Method of design public key infrastructure for secure audio information transmission in multimedia systems," 2017 15th International Conference on Electrical Machines, Drives and Power Systems (ELMA), Sofia, 2017, pp. 195–198, doi: https://doi.org/10.1109/ELMA.2017.7955430.
40. T. P. Pai, M. E. Raghu and K. C. Ravishankar, "Video Encryption for Secure Multimedia Transmission - A Layered Approach," 2014 3rd International Conference on Eco-friendly Computing and Communication Systems, Mangalore, 2014, pp. 127–132, doi: https://doi.org/10.1109/Eco-friendly.2014.101.
41. H. Cui, X. Yuan and C. Wang, "Harnessing Encrypted Data in Cloud for Secure and Efficient Mobile Image Sharing", in IEEE Transactions on Mobile Computing, vol. 16, no. 5, pp. 1315–1329, 1 May 2017, doi: https://doi.org/10.1109/TMC.2016.2595573.
42. Usman, M., Jan, M. A., He, X., & Chen, J. (2019). P2DCA: A Privacy-Preserving-Based Data Collection and Analysis Framework for IoMT Applications. *IEEE Journal on Selected Areas in Communications, 37*(6), 1222–1230. https://doi.org/10.1109/JSAC.2019.2904349
43. Zheng, Y., Yuan, X., Wang, X., Jiang, J., Wang, C., & Gui, X. (2017). Toward Encrypted Cloud Media Center With Secure Deduplication. *IEEE Transactions on Multimedia, 19*(2), 251–265. https://doi.org/10.1109/TMM.2016.2612760
44. Abdul, W., Ali, Z., Ghouzali, S., Alfawaz, B., Muhammad, G., & Hossain, M. S. (2017). Biometric Security Through Visual Encryption for Fog Edge Computing. *IEEE Access, 5,* 5531–5538. https://doi.org/10.1109/ACCESS.2017.2693438
45. Li, X., Yuan, J., Ma, H., & Yao, W. (2018). Fast and Parallel Trust Computing Scheme Based on Big Data Analysis for Collaboration Cloud Service. *IEEE Transactions on Information Forensics and Security, 13*(8), 1917–1931. https://doi.org/10.1109/TIFS.2018.2806925
46. Li, Q., Tian, Y., Zhang, Y., Shen, L., & Guo, J. (2019). Efficient Privacy-Preserving Access Control of Mobile Multimedia Data in Cloud Computing. *IEEE Access, 7,* 131534–131542. https://doi.org/10.1109/ACCESS.2019.2939299
47. H. A. Al Hamid, S. M. M. Rahman, M. S. Hossain, A. Almogren and A. Alamri, "A Security Model for Preserving the Privacy of Medical Big Data in a Healthcare Cloud Using a Fog Computing Facility With Pairing-Based Cryptography," in IEEE Access, vol. 5, pp. 22313–22328, 2017,doi: https://doi.org/10.1109/ACCESS.2017.2757844.
48. Khedr, A., & Gulak, G. (2018). SecureMed: Secure Medical Computation Using GPU-Accelerated Homomorphic Encryption Scheme. *IEEE Journal of Biomedical and Health Informatics, 22*(2), 597–606. https://doi.org/10.1109/JBHI.2017.2657458
49. Zhu, L., Song, H., Zhang, X., Yan, M., Zhang, L., & Yan, T. (2019). A Novel Image Encryption Scheme Based on Nonuniform Sampling in Block Compressive Sensing. *IEEE Access, 7,* 22161–22174. https://doi.org/10.1109/ACCESS.2019.2897721
50. Zhang, X., & Wang, X. (2018). Digital Image Encryption Algorithm Based on Elliptic Curve Public Cryptosystem. *IEEE Access, 6,* 70025–70034. https://doi.org/10.1109/ACCESS.2018.2879844
51. Tawalbeh, L., Mowafi, M., & Aljoby, W. (2013). Use of elliptic curve cryptography for multimedia encryption. *IET Information Security, 7*(2), 67–74. https://doi.org/10.1049/iet-ifs.2012.0147
52. M. Guan, X. Yang and W. Hu, "Chaotic image encryption algorithm using frequency-domain DNA encoding," in IET Image Processing, vol. 13, no. 9, pp. 1535–1539, 18 7 2019, doi: https://doi.org/10.1049/iet-ipr.2019.0051.
53. He, J., Huang, S., Tang, S., & Huang, J. (2018). JPEG Image Encryption With Improved Format Compatibility and File Size Preservation. *IEEE Transactions on Multimedia, 20*(10), 2645–2658. https://doi.org/10.1109/TMM.2018.2817065
54. R. Hamza, K. Muhammad, A. N. and G. RamiRez-GonzaLez, "Hash Based Encryption for Keyframes of Diagnostic Hysteroscopy," in IEEE Access, vol. 6, pp. 60160–60170, 2018, doi: https://doi.org/10.1109/ACCESS.2017.2762405.
55. Z. Xia, Y. Zhu, X. Sun, Z. Qin and K. Ren, "Towards Privacy-Preserving Content-Based Image Retrieval in Cloud Computing," in IEEE Transactions on Cloud Computing, vol. 6, no. 1, pp. 276–286, 1 Jan.-March 2018, doi: https://doi.org/10.1109/TCC.2015.2491933.
56. Xu, Y., Zhao, X., & Gong, J. (2019). A Large-Scale Secure Image Retrieval Method in Cloud Environment. *IEEE Access, 7,* 160082–160090. https://doi.org/10.1109/ACCESS.2019.2951175
57. Zeinab Fawaz, Hassan Noura, Ahmed Mostefaoui, An efficient and secure cipher scheme for images confidentiality preservation, Signal Processing: Image Communication, Volume 42, 2016, Pages 90–108, ISSN 0923–5965, https://doi.org/https://doi.org/10.1016/j.image.2016.01.009.
58. Noura, H., Sleem, L., Noura, M., et al. (2018). A new efficient lightweight and secure image cipher scheme. *Multimed Tools Appl, 77,* 15457–15484. https://doi.org/10.1007/s11042-017-5124-9
59. Visalakshi, B., & Meyappan, T. (2017). Image Encryption and Decryption using Shifting Technique. *International Journal of Engineering Science and Computing, 7*(6), 12668–12671.
60. Bhaskar Mondal, Tarni Mandal, A light weight secure image encryption scheme based on chaos & DNA computing, Journal of King Saud University - Computer and Information Sciences, Volume 29, Issue 4, 2017, Pages 499–504, ISSN 1319–1578, https://doi.org/https://doi.org/10.1016/j.jksuci.2016.02.003.
61. Noura, M., Noura, H., Chehab, A., et al. (2018). A dynamic approach for a lightweight and secure cipher for medical images.

Multimed Tools Appl, 77, 31397–31426. https://doi.org/10.1007/s11042-018-6051-0

62. S. Belguith , A. Jemai , R. Attia , Enhancing data security in cloud computing using a lightweight cryptographic algorithm, in: ICAS 2015 : The Eleventh International Conference on Autonomic and Autonomous Systems, IARIA, 2015, pp. 98–103 .
63. Daniel, E., & Vasanthi, N. A. (2019). LDAP: a lightweight deduplication and auditing protocol for secure data storage in cloud environment. *Cluster Comput, 22,* 1247–1258. https://doi.org/10.1007/s10586-017-1382-6
64. P. Rad, M. Muppidi, S. S. Agaian and M. Jamshidi, "Secure image processing inside cloud file sharing environment using lightweight containers," 2015 IEEE International Conference on Imaging Systems and Techniques (IST), Macau, 2015, pp. 1–6, doi: https://doi.org/10.1109/IST.2015.7294578.
65. Xiong, J., Zhang, Y., Li, X., et al. (2018). RSE-PoW: a Role Symmetric Encryption PoW Scheme with Authorized Deduplication for Multimedia Data. *Mobile Netw Appl, 23,* 650–663. https://doi.org/10.1007/s11036-017-0975-x
66. Gupta, B. B., Yamaguchi, S., & Agrawal, D. P. (2018). Advances in Security and Privacy of Multimedia Big Data in Mobile and Cloud Computing. *Multimed Tools Appl, 77,* 9203–9208. https://doi.org/10.1007/s11042-017-5301-x
67. Alassaf, N., Gutub, A., Parah, S. A., et al. (2019). Enhancing speed of SIMON: A light-weight-cryptographic algorithm for IoT applications. *Multimed Tools Appl, 78,* 32633–32657. https://doi.org/10.1007/s11042-018-6801-z
68. Shifa A, Asghar MN, Noor S, Gohar N, Fleury M. Lightweight Cipher for H.264 Videos in the Internet of Multimedia Things with Encryption Space Ratio Diagnostics. Sensors. 2019; 19(5):1228. https://doi.org/https://doi.org/10.3390/s19051228
69. Liang, C., Ning Ye, R., & Malekian and Ruchuan Wang, "The hybrid encryption algorithm of lightweight data in cloud storage", . (2016). 2nd International Symposium on Agent, Multi-Agent Systems and Robotics (ISAMSR). *Bangi, Malaysia, 2016,* 160–166. https://doi.org/10.1109/ISAMSR.2016.7810021
70. Noura, H., Chehab, A., Sleem, L., et al. (2018). One round cipher algorithm for multimedia IoT devices. *Multimed Tools Appl, 77,* 18383–18413. https://doi.org/10.1007/s11042-018-5660-y
71. P. Barreto and V. Rijmen, "The khazad legacy-level block cipher," Primitive submitted to NESSIE, vol. 97, 2000.
72. J. Daemen, "Cipher and hash function design strategies based on linear and differential cryptanalysis," Ph.D. dissertation, Doctoral Dissertation, March 1995, KU Leuven, 1995.
73. Y. Wu, J. Noonan and S. Agaian, "NPCR and UACI Randomness Tests for Image Encryption," Cyber Journals: Multidisciplinary, Journals in Science and Technology, Journal of Selected Areas in Telecommunications (JSAT), 2011, pp. 31–38.
74. May Zaw, Z., & Phyo, S. W. (2015). Security Enhancement System Based on the Integration of Cryptography and Steganography. *International Journal of Computer (IJC), 19*(1), 26–39.
75. L. Yu, Z. Wang and W. Wang, "The Application of Hybrid Encryption Algorithm in Software Security," 2012 Fourth International Conference on Computational Intelligence and Communication Networks, Mathura, 2012, pp. 762–765, doi: https://doi.org/10.1109/CICN.2012.195.

Publisher's Note Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.

Denis Rayappan has obtained Bachelor of Science (B.Sc.) from Loyola College (Autonomous), Madras University, Chennai, TN, India and Master of Computer Applications (MCA) from Sacred Heart College (Autonomous), Tirupattur in the year 2006 and 2009 respectively. Presently, he is a Assistant Professor at PG Department of Computer Science, Sacred Heart College (Autonomous) and also pursuing his Ph.D. in Computer Science at Periyar University, Salem, TN, India. He has over 10 years of teaching experience and published research papers in peer reviewed Journals and conferences, one Indian Patent, and authored two books (Java Programming – for Core and Advanced Users, ISBN: 9789386235329 | Year: 2018 & Constructive Java Programming ISBN: 9789389211771 | Year: 2020–2021) by Universities Press (India) Pvt. Ltd, Hyderabad. His research interests include Data Security and Privacy, Cryptography Algorithms, Big Data Analytics, Data Mining and Bio-inspired algorithms.

Madhubala Pandiyan obtained Ph.D. in Computer Science from Mother Teresa Women's University, kodaikanal, TN, India in the year 2017. She is currently a Assistant Professor at Research Department of Computer Science, Don Bosco College of Arts and Science, Dharmapuri, TN, India since 2007. Also she is the University nominee for Board of Studies of BCA department at Sacred Heart College (Autonomous), Thiruvalluvar University, Tirupattur, TN, India. She has published more than 13 research papers in peer reviewed international journals and conferences. Her research interests include Cloud Computing, Wireless Sensor Networking, Data security, advanced data mining and Artificial Intelligence. She has 19 years of teaching experience and 8 years of Research Experience. Currently she is guiding five Ph.D. students.