Soft Computing
https://doi.org/10.1007/s00500-023-08360-0

FOCUS

An efficient hybrid fuzzy image encryption models for the secured cloud accessing in portable robotics devices

K. Subba Reddy[1] · K. Rajendra Prasad[2] · K. Nageswara Reddy[1] · P. Anjaiah[2]

Accepted: 29 April 2023

Abstract
Secure sharing of image data through different communication channels is a challenging research issue in digital networks. In such cases, cryptography algorithms are widely used to encrypt and decrypt the information reliably at both ends of source and target destinations. Various state-of-the-art image encryption algorithms are surveyed and investigated to assess the best image encryption. In this paper, image encryption is described with various fuzzy operation modes. It ensures secure image transmission over to the digital channels. Most reliable image encryption is the aim of the work, and it is achieved through developing a hybrid fuzzy-based framework that composites the techniques of image encryption methods and fuzzy operation modes. Proposed hybrid fuzzy-based models are highly recommended to maintain secure information on portable robotics devices, communication channels, and routing devices. These hybrid encrypted models provide the users' privacy to access the image data with reliable security mechanisms.

Keywords Image encryption · Access control mechanisms · Fuzzy operation modes · Cryptographic algorithms · Security

1 Introduction

Sharing and providing security of multimedia data in intelligent applications (Huang and Fang 2008) or digital networks (Duan et al. 2017) has become the most important for trustworthy applications or cloud services (Liu et al. 2021). Cryptographic techniques (Ogunseyi and Yang 2018) are access control mechanisms (Aftab et al. 2022) to communicate images, audio, and video data (Prasad and Reddy 2013). Image encryption (Ferdush et al. 2021) is one of the essential cryptographic techniques for the emerging applications like medical images (El-Shafai et al. 2021) or healthcare (Sarosh et al. 2022; Prasad et al. 2021; Rajendra Prasad et al. 2021; Subba Reddy et al. 2022), spatial maps for defense (Lin et al. 2011), satellite image analysis (Al-Khasawneh et al. 2020), secure scientific applications (Sarfraz et al. 2013), software-defined image networks analysis (Ahmed et al. 2022). Information is the most valuable for the business organization, industry sectors, and governments. Protecting sensitive information through implementing access control mechanisms ensures data privacy and security. Two classifications of cryptographic techniques used for data privacy and security are symmetric and asymmetric (Kumar et al. 2020). In asymmetric cryptography, both the sender and receiver use the shared key for encryption and decryption, whereas in asymmetric, public and private keys are used for the same process. Image cryptography is one of the social needs for security-related applications in all private and public sectors. Various image encryption algorithms have evolved in the last decade, indicating the progressive developments in the era

✉ K. Subba Reddy
mrsubbareddy@yahoo.com

K. Rajendra Prasad
krprgm@gmail.com

K. Nageswara Reddy
knreddy221@gmail.com

P. Anjaiah
anjaiah.pole@gmail.com

[1] Department of Computer Science and Engineering, Rajeev Gandhi Memorial College of Engineering and Technology, Nandyal, Andhra Pradesh, India

[2] Department of Computer Science and Engineering, Institute of Aeronautical Engineering, Dundigal, Hyderabad, Telangana, India

Published online: 15 May 2023

of image cryptography. Image data is contained in the form of raster pixels that have a large-sized block of pixels with the same property (Praveen Kumar and Rajendra Prasad 2021). With these pixels, encryption and decryption can be performed efficiently to secure images over the transmissions in the communication channels. Its image encryption techniques are applied to images like medical images, infrared images, logo images, etc. Presently, the most successful image encryption technique is RC6 (Rivest Cipher 6) (Faragallah et al. 2021), and it is applied in different modes (Elashry et al. 2012), electronic codebook (ECB), cipher block chaining (CBC), output feedback (OFB), cipher feedback (CFB). Other encryption methods, advanced encryption standards (AES) (Gladman 2003), data encryption standards (DES) (Tang et al. 2018), and Rivest-Shamir-Adleman (RSA) (Imam et al. 2021), are also the most commonly used image encryption techniques. The Advanced Encryption Standard (AES) is utilized in both software and hardware across the globe to encrypt sensitive data. It is absolutely necessary for the protection of electronic data, computer systems, and cybersecurity in the government. This paper presents this state-of-the-art image encryption algorithms and their procedural details in the following sections. An experimental study of image encryption techniques underlying the four modes, ECB, CBC, OFB, and CFB, is presented to find the best image encryption technique. In the routing phase, each cluster head node determines whether or not to rebroadcast the route request (RREQ) message by calculating its degree based on several parameters, including distance, residual energy, link quality, and the number of steps. Intra-cluster communications are secured with symmetric cryptography during the communication security phase.

The overall summary of the paper is presented as follows:

1. Illustrate the fuzzy operations of four modes, ECB, CBC, OFB, and CFB, for the image encryption
2. Present the hybrid image encryption techniques with the composition of image encryption methods and fuzzy-based operation modes
3. Find the best image encrypted images for the image privacy and security applications
4. Evaluate the performance of hybrid image encryption models with the parameters of crucial entropy, correlation coefficient, histogram deviation, and other parameters.
5. Perform an empirical analysis of the encryption techniques by using the subset of benchmarked images

Various sections of the paper are organized as follows: Sect. 2 presents the modes of the operations of encryption techniques. Section 3 shows an overview of the state-of-the-art of image encryption techniques. Section 4 describes the performance and comparative study of image encryption algorithms. Section 5 presents the conclusion and scope of the work.

2 Modes of the operations of encryption techniques

Any image encryption technique performs the encryption and decryption for the images with the consideration of blocks wise instead of taking the entire image. Block-based ciphering is performed in many cryptographic algorithms for enforcing higher authentication and gaining confidentiality. Encrypted techniques must use distinct modes of operations concerning the block ciphers. Any encryption technique must employ encryption and decryption with the same mode of operations. The current research in image security found that four fuzzy (Subba and Rajendra 2021) modes are frequently used and succeeded wildly. These modes are fuzzy-ECB, fuzzy-CBC, fuzzy-CFB, and fuzzy-OFB, and operational details are described as follows.

2.1 Fuzzy-based electronic codebook (fuzzy-ECB)

In this operation mode, initially, the data are partitioned into distinct blocks of the same size, in which each partitioned block is encrypted separately. There is no association among the encrypted blocks so it would be most advantageous in less propagation of errors. If an error is found in a block, it may not affect other blocks. Error is limited to only the associated block. The ECB will not propagate the error to other blocks with the fuzzy membership values, and its operation mode prevents the propagation of errors for accurate data. Its operation details are illustrated in equations Eq. (1) to (2). The source data ’S.D.’ is divided into blocks with equal sizes (SD_1, SD_2,……), and Ciphered blocks (CSD_1, CSD_2,…..) are obtained based on the ‘K’.

$$\mathrm{CSD}_i = E_{\mathrm{K}}(\mathrm{SD}_i) \tag{1}$$

$$\mathrm{SD}_i = D_{\mathrm{K}}(\mathrm{CSD}_{i)} \tag{2}$$

In ECB, the portioned blocks are transformed to cipher blocks using the same protocol when considering the key ‘K’. All the partitioned blocks are decrypted using the same key ‘K’. Thus, sometimes ECB may not provide security in all aspects of data transmission across the communication networks. However, it has become one of the less propagated error access control encrypted mechanisms. Using the operation mode of ECP, there is possible to construct the codebook with the same encryption and decryption methods for the repeated similar blocks of the images. With the ECB, preventing attacks while accessing the enciphered data may not be possible. This situation is handled with the following operation modes.

A block of data can be encrypted and decrypted with the use of a block cipher by utilizing a symmetric key and algorithm. In order to enlarge the keyspace of the cipher and make it more difficult to break the key using brute force, a block cipher requires an initialization vector (IV), which is added to the input plaintext. This makes it more difficult to break the key.

2.2 Fuzzy-based-Cipher blockchain (Fuzzy-CBC)

It is another operation mode that can effectively handle the image encryption problem of ECB with the bits XOR operation of the data. The fuzzy membership values for the XORing are applied between the source block of the data and the encrypted data of the previous block. It is a repeated process and stopped until performing the XORing process between the last block data and encrypted data of the previous block (of the last block). Equations (3)–(5) show operation mode 'CBC' processing with the XOR bits operations for the image encryption and decryption.

$$\mathrm{CD}_0 = \mathrm{IVec} \tag{3}$$

$$\mathrm{CD}_j = E_{\mathrm{K}}\left(\mathrm{CD}_{j-1}\mathrm{XORSD}_j\right) \tag{4}$$

$$\mathrm{SD}_j = D_{\mathrm{k}}\left(\mathrm{CD}_j\right)\mathrm{XORCD}_{j-1} \tag{5}$$

In CBC operation mode, the decrypted data block is obtained by applying the XOR between present and prior encipher data blocks. Initially, the initialization vector (IVec) is randomly selected and considered as initial cipher data 'CD_0'. The XOR is applied among the initial cipher data (or IVec) and the initial data block 'DB_1' for obtaining encipher data 'CD_1' for the block of 'SD_1'. Similarly, other encipher blocks, like CD_2, CD_2,…, are obtained until the last data block is enciphered.

2.3 Fuzzy-based-Cipher feedback (fuzzy-CFB)

The CFB operation mode also uses the initialization vector (IVec) to generate initial encrypted data. It can be described in the formula shown in Eq. (6).

$$\mathrm{CD}_0 = \mathrm{IVec} \tag{6}$$

$$\mathrm{ENC}_j = E_{\mathrm{K}}\left(\mathrm{CD}_{j-1}\right), j = 1, 2, \ldots\ldots \tag{7}$$

$$\mathrm{CD}_j = \mathrm{SD}_j\mathrm{XORENC}_j \tag{8}$$

$$\mathrm{SD}_j = \mathrm{CD}_j\mathrm{XORSD}_j \tag{9}$$

In the next recursive steps, derived encrypted data of initial IVec and first data block (SD_1) are applied together with XOR operation. These recursive encrypted and decrypted steps are performed as per mentioned modeling steps for the data blocks (SD_1, SD_2,……), which can be shown in Eqs. (6)–(9). Encipher data are obtained for the data blocks of (SD_1, SD_2,……), which are (CD_1, CD_2,……) by applying the encrypted key K.

In CFB mode, there is a chance to propagate the errors in consequence fuzzy-based ciphered blocks if any error is found at least a single bit in present or previous data blocks. The encryption under this mode is not the most error-free.

2.4 Fuzzy-based-Output feedback (fuzzy-OFB)

The data blocks are taken in different sizes in the operation mode of OFB.

$$I_0 = \mathrm{IVec} \tag{10}$$

$$I_j = E_{\mathrm{K}}\left(I_{j-1}\right), j = 1, 2, \ldots\ldots \tag{11}$$

$$\mathrm{CD}_j = \mathrm{SD}_j\mathrm{XOR}I_j \tag{12}$$

$$\mathrm{SD}_j = I_j\mathrm{XORSD}_j \tag{13}$$

The OFB operation mode attempts the fuzzy synchronized stream ciphering problem by passing the encryption function as feedback instead of cipher data, unlike the CFB mode. The basic modeling of OFB is similar to CFB except for the feedback function. The modeling of OFB is represented in Eqs. (10)–(13)

3 Image encryption techniques

The encryption of block-wise details of the images is performed by image encryption. These are stated, and their procedural details are discussed in this section. One of the state-of-the-art image encryption techniques is the RC6 algorithm (Faragallah et al. 2020), which greatly encrypts the image blocks data under the different modes described in an earlier section. A block cipher is a type of encryption that can only function on entire data blocks at one time and creates ciphertext blocks of the same size. The Data Encryption Standard (DES) is a block cipher that can decrypt data blocks that are 64 bits in length. The DES algorithm utilizes a key that is 64 bits long; however, the real key length is 56 bits because it includes one bit for parity.

3.1 RC6 Image encryption technique

The RC6 technique partition the source image into different blocks with suitable sizes (for example, take the data block with 128-bit blocks. These partitioned blocks should be non-overlapped; then, attained blocks are passed to the first phase of RC6 (RC6 enciphering phase). Any one of four operation modes, EBC, CBC, CFB, and OFB, is used in the enciphering phase to obtain the original image's enciphered blocks. Later, all the enciphered blocks are assembled for the final construction of the encrypted image of the original image. The encrypted image is transmitted to the receiver on another end for securing purposes. After reaching the encrypted image at the receiver side, the encrypted image is again divided into blocks of the same size as the 128-bit block. Pass the all non-overlapped partitioned encrypted blocks to the second phase of RC6, i.e., the RC6 deciphering phase. The blocks are submitted at the deciphering phase in the same operation modes earlier used in enciphering phase. Finally, deciphered blocks are obtained and merged to obtain the decrypted image at the receiver side. These procedural technique steps are mentioned in Fig. 1.

The fuzzy logic method to edge linking makes it possible to employ membership functions to determine the degree to which a pixel belongs to an edge or a uniform region. This can be done by comparing the pixel to the surrounding pixels. Each input of the edge has its own membership function given, and that function is a zero-mean Gaussian.

This paper presents the algorithm that greatly supports the higher degree of security at user level. Proposed algorithm provides both the security and processing levels by generated random keys. The fuzzy logic creates this facility for accessing the image data with reliable security implementations.

3.2 RSA Image encryption technique

The RSA (Giraud Sept. 2006) is an asymmetric encryption technique since it uses two different keys, i.e., the public key and private key, for the encryption and decryption of the data at two different ends. The symmetric technique uses the same key for both encryption and decryption.

Algorithm 1: RSA Encryption Technique.

1. Determine the two large primary keys, p, and q, randomly, and $p \neq q$
2. Compute the n values using $n = p \times q$
3. Find the $\varphi(n) = (p-1) \times (q-1)$
4. Select the e value, such that $\gcd(\varphi(n), e) = 1$ and $1 < e < \varphi(n)$
5. Select d such that $d = e^{-1} \bmod \varphi(n)$, and d is considered as the private
6. Generate the public key Public_Key = {e,n}
7. Generate the private key Private_Key = {d, n}
8. Find the encrypted data for the data block
   Enciphered data = data block^{e} mod n.
9. Find the decrypted data for the enciphered data
   Deciphered data = enciphered data^{d} mod n.

It cannot prevent hackers' attacks more efficiently than the asymmetric technique because it uses the same key at both ends of the sender and receiver. Finding the public and private keys using the RSA encryption technique is illustrated in Algorithm 1.

The process of encrypting a message involves encoding it in a format that cannot be read or understood by an eavesdropper. Encryption is one of the most important concepts in cryptography. Caesar was the initial one to ever adopt this method, and he did so in order to encrypt his messages using the Caesar cipher.

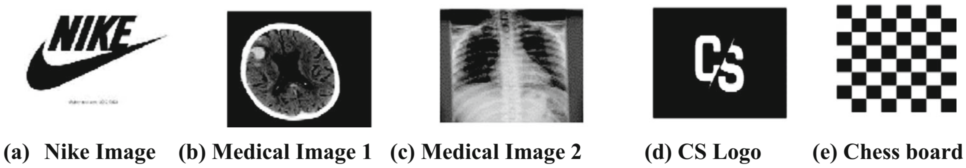
3.3 Advanced encryption standards (AES) for the image encryption

It comes under the classification of symmetric block cipher technique. It excellently supports the different lengths of image data encryptions. The AES (Hammad et al. 2012) is designed with variant key lengths, i.e., 128, 192, and 256 bits; their versions are AES-128, AES-192, and AES-256 encryption techniques (Dunkelman et al. 2015). These methods deliver the final cipher text with the number of rounds of 10, 12, and 14, respectively. Every round performs the four transformations: sub-byte, shift rows, mix columns, and add round key (for the counting purpose). For example, AES-128 is done with ten rounds, in which all the four transformations are performed in the first nine rounds, and the last round (10th), only mix-transformation cannot be attempted. The decryption is performed with the following reverser functions: inverse substitute bytes, inverse shift rows, and inverse mix columns. The sub-byte transformation uses the 8-bit substitution box and transforms each 8-bit (byte) data block into another variant of the data block.

3.4 Data encryption standards (DES) for the image encryption

It is also the most commonly used security technique that can be applied to the private and government sectors' data.

Fig. 1 Test Images for Performance Evaluation of Image Encryption Techniques



(a) Nike Image (b) Medical Image 1 (c) Medical Image 2 (d) CS Logo (e) Chess board

Table 1 Obtained encrypted images using AES, RC2, blowfish, DES, triple DES

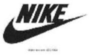
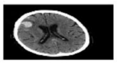
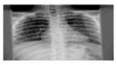
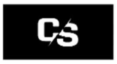
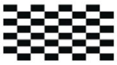
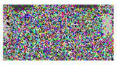
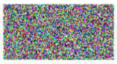
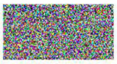
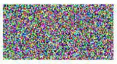
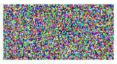
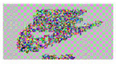
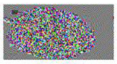
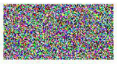
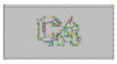
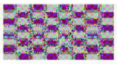
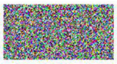
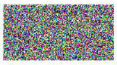
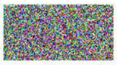
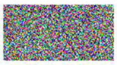
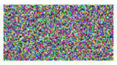
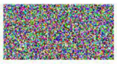
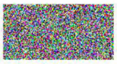
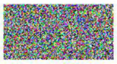
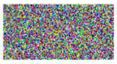
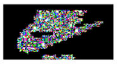
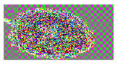
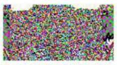
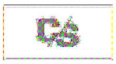
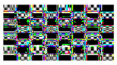
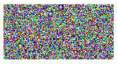
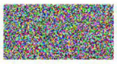
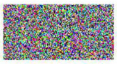
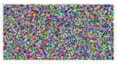
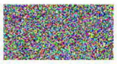
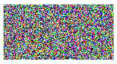
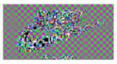
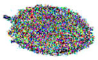
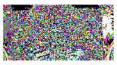
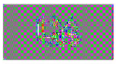
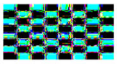
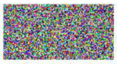
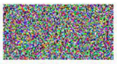
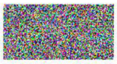
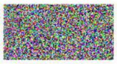
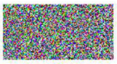
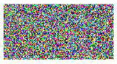
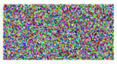
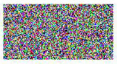
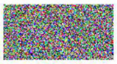
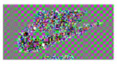
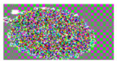
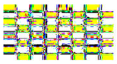
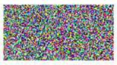
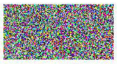
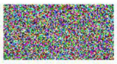
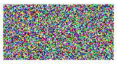
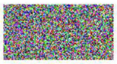
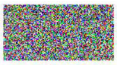
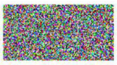
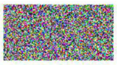
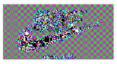
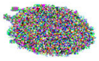
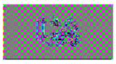
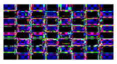
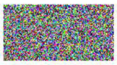
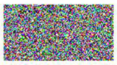
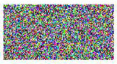
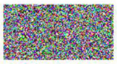
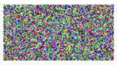
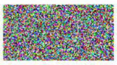
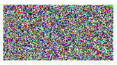
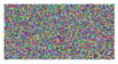
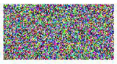
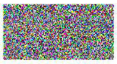
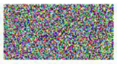
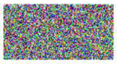
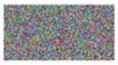
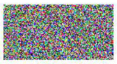
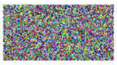
Encryption Method	Nike Image 	Medical Image1 	Medical Image2 	Logo Image 	Chessboard Image 
AES-fuzz-cbc-image					
AES-fuzzy-cfb-image					
AES-fuzzy-ecb-image					
AES-fuzzy-ofb-image					
ARC2-fuzzy-cbc-image					
ARC2-fuzzy-cfb-image					
ARC2-fuzzy-ecb-image					
ARC2-fuzzy-ofb-image					
Blowfish-fuzzy-cbc-image					
Blowfish-fuzzy-cfb-image					
Blowfish-fuzzy-ecb-image					
Blowfish-fuzzy-ofb-image					
Triple DES – fuzzy-cbc - image					

Table 1 continued

Triple DES – fuzzy-cfb - image					
Triple DES –fuzzy- ECB - image					
Triple DES – fuzzy-ofb - image					
SingleDES-fuzzy-cbc-image					
SingleDES-fuzzy-cfb-image					
SingleDES-fuzzy-ecb-image					
SingleDES-fuzzy-ofb-image					
RC6-fuzzy-cbc image					
RC6—fuzzy-ecb-image					
RC6-cfb-fuzzy-image					
RC6-ofb-fuzzy-image					
RSA-image					

However, it is unsecured for the reason that the data is a small size and causes to brute force attack. The DES (Standard and (DES) and Advanced Encryption Standard (AES) xxxx) takes the data size as 64-bit and the critical length as 56 bits. Suppose a weak key is used; it causes a vulnerable attack since it restricts the key length to 56-bit. The DES is also applied using the four operation codes (i.e., CBC, EBC, CFB, and OFB) for the encryption and decryption of the data. The algorithm is believed to be secured with another extension of the DES, i.e., Triple DES (Mitchell 2016). It is also proved with many theoretical attacks.

Table 2 Performance analysis of image encryption methods for the sample image "Nike"

Encryption method	Entropy	Correlation coefficient	Histogram deviation	NCPR	UACI	PSNR
AES-fuzzy-cbc-image	0.723847	0.288767	3.66922	0.260743	0.164191	7.246642
AES-fuzzy-cfb-image	0.724428	0.285439	3.673325	0.261345	0.164807	7.225051
AES-fuzzy-ecb-image	0.568133	0.443899	2.726669	0.193792	0.098162	9.084128
AES-fuzzy-ofb-image	0.720992	0.286216	3.649124	0.260255	0.163178	7.260428
ARC2-fuzzy-cbc-image	0.723527	0.288244	3.666962	0.260521	0.163914	7.255734
ARC2-fuzzy-cfb-image	0.720789	0.288297	3.647705	0.2598	0.162812	7.275058
ARC2-fuzzy-ecb-image	0.918129	0.11483	5.528351	0.399927	0.2965	4.935995
ARC2-fuzzy-ofb-image	0.721932	0.290242	3.655731	0.260227	0.163421	7.260071
Blowfish-fuzzy-cbc-image	0.721566	0.285048	3.653152	0.260548	0.163635	7.245976
Blowfish-fuzzy-cfb-image	0.724484	0.285271	3.673721	0.261533	0.164778	7.227037
Blowfish-fuzzy-ecb-image	0.724555	0.360261	3.674225	0.260579	0.163371	7.292897
Blowfish-fuzzy-ofb-image	0.726653	0.284324	3.689102	0.262038	0.165582	7.215265
Triple DES-fuzzy-cbc -image	0.723827	0.290775	3.669083	0.260946	0.164003	7.255095
Triple DES-fuzzy-cfb -image	0.723823	0.285596	3.669052	0.261004	0.164412	7.236211
Triple DES-fuzzy- ecb -image	0.729053	0.408192	3.706207	0.261381	0.16249	7.387884
Triple DES-fuzzy-ofb -image	0.724521	0.288084	3.673981	0.261285	0.164595	7.235874
Single DES-fuzzy-cbc-image	0.721789	0.282752	3.654724	0.260731	0.163817	7.240124
Single DES-fuzzy-cfb-image	0.723525	0.287553	3.666946	0.261121	0.164172	7.243796
Single DES-fuzzy-ecb-image	0.732725	0.388832	3.732559	0.261459	0.164979	7.314662
Single DES-fuzzy-ofb-image	0.725821	0.293984	3.683197	0.261417	0.164674	7.247313
RC6-fuzzy-cbc	0.752212	0.209233	0.423255	0.262322	0.162342	7.756672
RC6-fuzzy-ecb	0.731121	0.223412	0.409876	0.286762	0.163451	7.752344
RC6-fuzzy-cfb	0.732221	0.211123	0.387682	0.222321	0.162222	7.531122
RC6-fuzzy-ofb	0.734123	0.224321	0.234122	0.272123	0.162356	7.876123
RSA	0.742341	0.212245	0.231222	0.265432	0.161222	7.651234

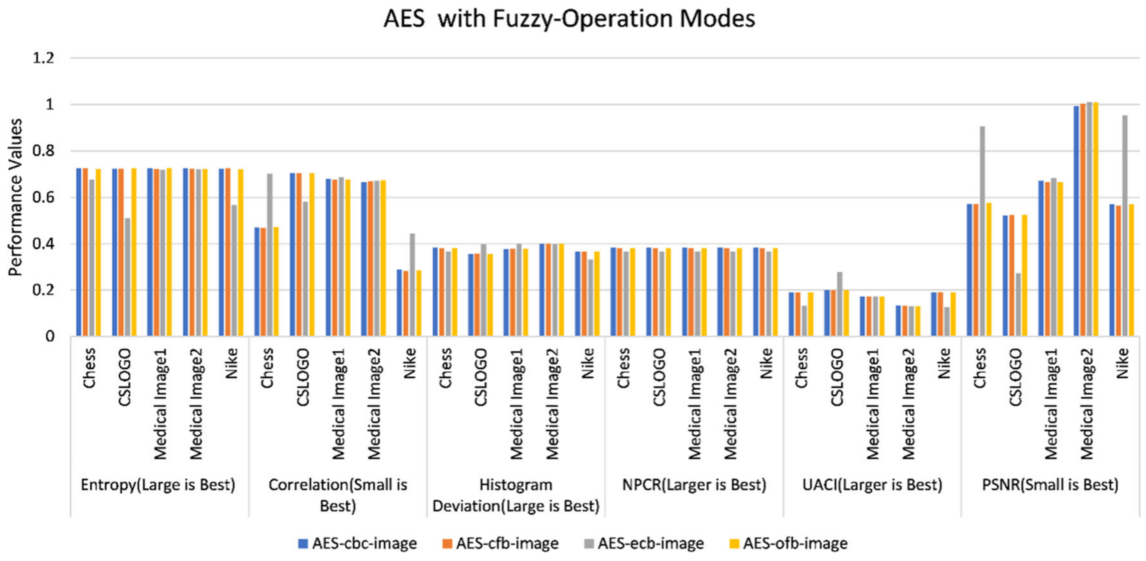


Fig. 2 AES Encryption Analysis with Proposed Four Fuzzy Modes

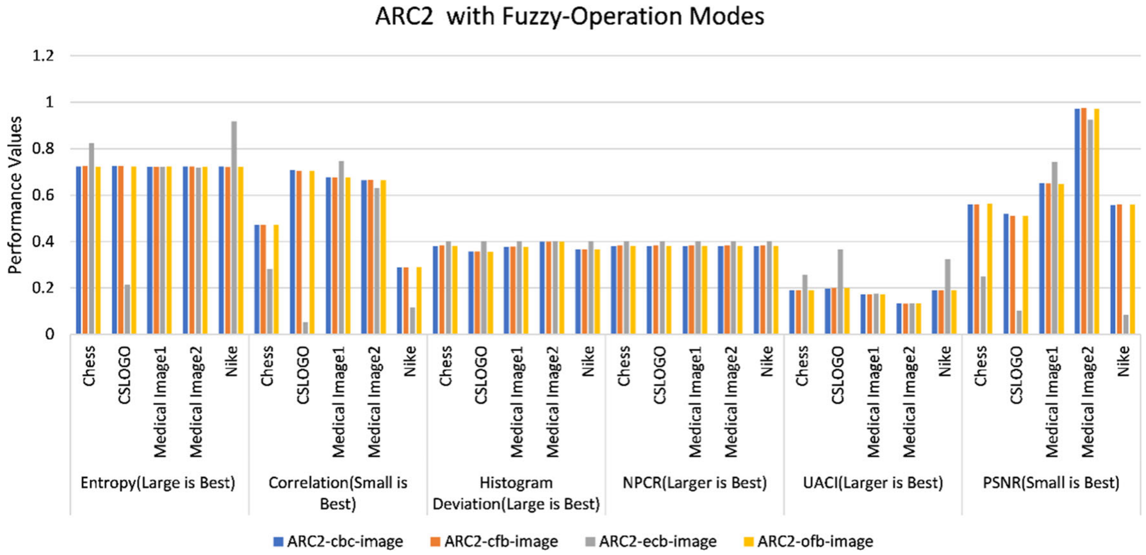


Fig. 3 ARC2 Encryption Analysis with Proposed Four Fuzzy Modes

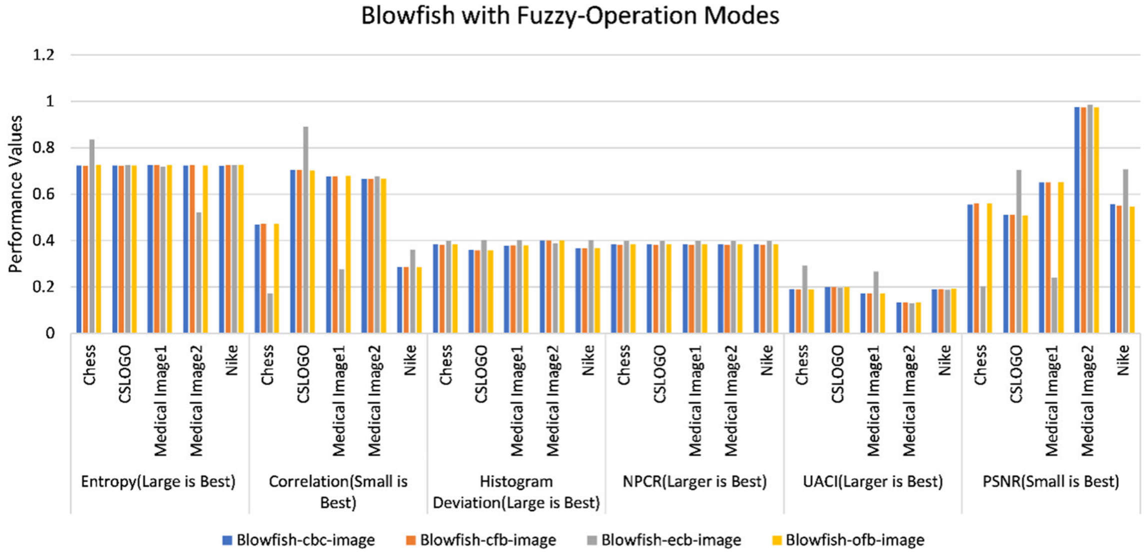


Fig. 4 Blowfish Encryption Analysis with Proposed Four Fuzzy Modes

4 Performance and comparative study of image encryption models

In the proposed work, the image encryption techniques AES, RC2, DES, Triple DES, and RC6 are composed of four fuzzy-based operation modes: fuzzy-CBC, fuzzy-EBC, fuzzy-CFB, and fuzzy-OFB. Proposed hybrid image encryption models are implemented using the python libraries, which are defined in ’pycryptodome’ (PyCryptodomen 2019). Keys generated using the Advanced Encryption Standard (AES) are symmetric keys that can have one of three possible lengths: 256, 192, or 128 bits. The United States government recognizes AES as the gold standard for encryption and recommends that other countries do the same. The AES algorithm will only accept keys that are 256 bits long. These composite hybrid models are experimented with using the benchmarked greyscale images, i.e., Nike, medical image 1, medical image 2, C.S. logo, and chessboard. Figure 1 shows the experimental images for the performance analysis and the extensive study of hybrid image encryption models.

The performance of image encryption techniques is evaluated by the quality measures, which are as follows: entropy measure, correlation coefficient, histogram deviation, number of pixels change rate analysis (NPCR), the peak signal to noise ratio test (PSNR), and feature similarity test (FST) (Faragallah et al. 2021). The quality is assessed by simulating the image encryption technique in

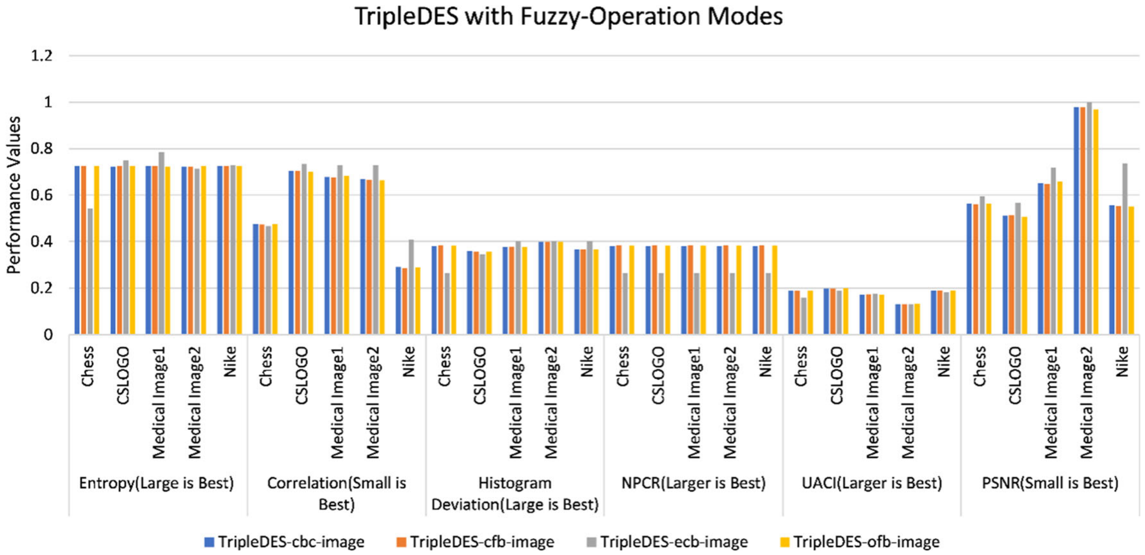


Fig. 5 Triple DES Encryption Analysis with Proposed Four Fuzzy Modes

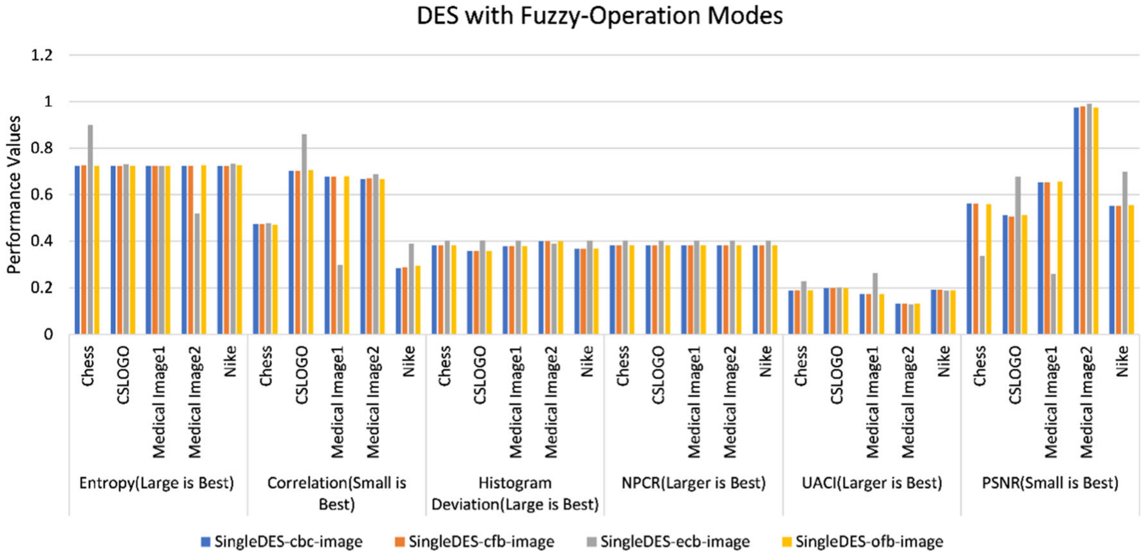


Fig. 6 Single DES Encryption Analysis with Proposed Four Fuzzy Modes

MATLAB. Visual inspection (VI) also illustrates underlying operation modes, i.e., ECB, CBC, CFB, and OFB, for the various image encryption techniques. Image details are processed and characterized using the patterns of similar image data blocks that show a bottleneck for applying the well-performed enciphering methods due to encrypting such pattern blocks to similar enciphered blocks. The VI for the proposed hybrid models of image encryption is shown in Table 1.

Image encryption results stated that hybrid model composition with the operation mode of "ECB" is not much succeeded compared to other operation modes. The best-ciphered images are obtained from hybrid model composition with the other operation modes CBC, CFB, and OFB. Hybrid models—AES-OFB, single DES-OFB, RC2-OFB, Triple DES-OFB, RC6-OFB, and RSA models have encrypted the original image more efficiently and deliver the most different ciphered image of the corresponding original image. The encrypted results are investigated based on five benchmarked test images and observed that RC2 performed as poor encryption. Other hybrid models obtained good encrypted images in the three operation modes, CBC, CFB, and OFB.

Table 2 presents the performance values for the sample Nike image to the required demonstration of hybrid encryption models. Hybrid encryption models' performance is evaluated using entropy parameters, correlation coefficient, histogram deviation, NCPR, UACI, and PSNR for the tested images Nike, two medical images, cs logo, and chessboard. High values of entropy, low values of the correlation coefficient, large values of histogram deviation, and high values of NCPR and UACI indicate that the best-encrypted image is obtained. According to this analysis and visual proof in Table 1, it is noted that all hybrid models performed better when compared to RSA. It also defined that RC6-based hybrid models outperformed the other encryption models.

Image encryption techniques, i.e., AES, ARC2, blowfish, Triple DES, and Single DES have experimented with the proposed fuzzy operation modes, i.e. fuzzy-cbc, fuzzy-cfb, fuzzy-ecb, and fuzzy-ofb. Five performance measures are taken in the experimental phase, and the best encryption is considered to be the following:

1. Entropy is high for the best encryption
2. The correlation between the original image and the encrypted image is to be small for the best encryption
3. Histogram deviation is to be maximized between the original and encrypted image for the best-encrypted case
4. NPCR and UACI should be significant for the well-defined encryptions
5. PSNR values are small when obtaining the best-encrypted image for the original image.

Experiments are conducted using the five benchmarked images, chess image, cslogo image, two medical images, and Nike image. Figures 2, 3, 4, 5 and 6 show the complete encryption performance comparison results. It observed that the encryption techniques AES, and Triple DES achieve the best-encrypted results with the fuzzy operation modes of cbc, cfb, and ofb. With fuzzy-ECB operation modes, ARC2 and Single DES perform the best. These techniques present good encrypted images under the fuzzy-ecb operation modes. Robotics-based portable devices require the best encryption for maximum security. Most of the time, all fuzzy operation modes are helpful for all encryption techniques. Hybrid encryption techniques are the most recommended in secure multimedia data transfer to virtual cloud-based robotics devices. Cloud security may fall within the purview of the network team, the security team, the applications team, the compliance team, or the infrastructure team. However, both the larger organization and the cloud service provider have some degree of responsibility for cloud security.

5 Conclusion and scope of the work

Image encryption is an emerging need for secured data accessing applications. Ciphered images are obtained while applying the image encryption techniques to original images. Traditional image encryption algorithms depend on the random selection of the key. The message or image data are divided into several blocks, and the encryption process is applied at block levels. However, these methods fail to use the random keys effectively to generate ciphered images with more secured mode annotations. For this reason, hybrid encrypted models are developed with image encryption and operation modes. The experiment analysis concluded that the hybrid model generated more efficient ciphered images under OFB mode than RSA. Highly differed ciphered images are not obtained under the operation mode of CFB with all the encryption techniques. There is scope to improve the hybrid models with asymmetric image encryption techniques for bio-accessing-based applications.

Funding The authors have not disclosed any funding.

Data availability The raw data elaborated during the current research are publicly available.

Declarations

Conflict of interest The author declares that he has no conflict of interest.

Ethical approval This article does not contain any studies with human participants performed by any of the authors.

References

Aftab MU, Hamza A, Oluwasanmi A, Nie X, Sarfraz MS, Shehzad D, Qin Z, Rafiq A (2022) Traditional and hybrid access control models: a detailed survey. Secur Commun Netw 2022:1560885. https://doi.org/10.1155/2022/1560885

Ahmed N, Bakar KA, Zuhra FT et al (2022) Security & privacy in software defined networks, issues, challenges and cost of developed solutions: a systematic literature review. Int J Wireless Inf Networks. https://doi.org/10.1007/s10776-022-00561-y

Al-Khasawneh MA, Abu-Ulbeh W, Khasawneh AM (2020) Satellite images encryption Review. Int Conf Intell Comput Hum-Comput Interact (ICHCI) 2020:121–125. https://doi.org/10.1109/ICHCI51889.2020.00034

Duan X, Giddings RP, Mansoor S, Tang JM (2017) Experimental demonstration of upstream transmission in digital filter multiple access pons with real-time reconfigurable optical network units. J Opt Commun Netw 9(1):45–52. https://doi.org/10.1364/JOCN.9.000045

Dunkelman O, Keller N, Shamir A (2015) Improved Single-Key Attacks on 8-Round AES-192 and AES-256. J Cryptol 28:397–422. https://doi.org/10.1007/s00145-013-9159-4

Elashry IF, Faragallah OS, Abbas AM, El-Rabaie S, Abd El-Samie FE (2012) A new method for encrypting images with few details using Rijndael and RC6 block ciphers in the electronic codebook mode. Inf Secur JA Global Perspect 21:193–205

El-Shafai W, Khallaf F, El-Rabaie ESM et al (2021) Robust medical image encryption based on DNA-chaos cryptosystem for secure telemedicine and healthcare applications. J Ambient Intell Human Comput 12:9007–9035. https://doi.org/10.1007/s12652-020-02597-5

Faragallah OS et al (2020) Efficiently encrypting color images with few details based on RC6 and different operation modes for cybersecurity applications. IEEE Access 8:103200–103218. https://doi.org/10.1109/ACCESS.2020.2994583

Faragallah OS, El-Sayed HS, Afifi A et al (2021) Small details gray scale image encryption using RC6 block cipher. Wireless Pers Commun 118:1559–1589. https://doi.org/10.1007/s11277-021-08105-y

Ferdush J, Begum M, Uddin MS (2021) Chaotic lightweight cryptosystem for image encryption. Adv Multimed 2021:5527295. https://doi.org/10.1155/2021/5527295

Giraud C (2006) An RSA implementation resistant to fault attacks and to simple power analysis. IEEE Trans Comput 55(9):1116–1120. https://doi.org/10.1109/TC.2006.135

Gladman, B. (2003) A specification for Rijndael, the AES algorithm.

Hammad I, El-Sankary K, El-Masry E (2012) Advanced encryption standard (AES) implementation. In: embedded systems. In: Iniewski K (Ed) Embedded systems doi: https://doi.org/10.1002/9781118468654.ch13

Huang H, Fang W (2008) Intelligent multimedia data hiding techniques and applications. In: 2008 International conference on information security and assurance (ISA 2008), 2008, pp 477–482, DOI: https://doi.org/10.1109/ISA.2008.83.

Imam R, Areeb QM, Alturki A, Anwer F (2021) Systematic and critical review of RSA based public key cryptographic schemes: past and present status. IEEE Access 9:155949–155976. https://doi.org/10.1109/ACCESS.2021.3129224

Prasad KR, Reddy BE (2013) Assessment of clustering tendency through progressive random sampling and graph-based clustering results. In: 2013 3rd IEEE international advance computing conference (IACC), Ghaziabad, India, pp 726-731https://doi.org/10.1109/IAdCC.2013.6514316

Kumar S, Singh BK, Akshita, Pundir S, Batra S, Joshi R (2020) A survey on symmetric and asymmetric key based image encryption. In: 2nd International conference on data, engineering and applications (IDEA), pp 1–5, DOI: https://doi.org/10.1109/IDEA49133.2020.9170703

Lin H, Bo Y, Wang J, Jia X (2011) Landscape structure based super-resolution mapping from remotely sensed imagery. IEEE Int Geosci Remote Sens Sympos 2011:79–82. https://doi.org/10.1109/IGARSS.2011.6048902

Liu Q, Peng Y, Wu J, Wang T, Wang G (2021) Secure multi-keyword fuzzy searches with enhanced service quality in cloud computing. IEEE Trans Netw Serv Manage 18(2):2046–2062. https://doi.org/10.1109/TNSM.2020.3045467

Mitchell CJ (2016) On the security of 2-key triple DES. IEEE Trans Inf Theory 62(11):6260–6267. https://doi.org/10.1109/TIT.2016.2611003

Ogunseyi TB, Yang C (2018) Survey and analysis of cryptographic techniques for privacy protection in recommender systems. In: Sun X, Pan Z, Bertino E (eds) Cloud computing and security. ICCCS 2018. Lecture Notes in Computer Science, vol 11065. Springer, Cham. https://doi.org/10.1007/978-3-030-00012-7_63

Prasad KR, Reddy BE, Mohammed M (2021) An effective assessment of cluster tendency through sampling based multi-viewpoints visual method. J Ambient Intell Human Comput. https://doi.org/10.1007/s12652-020-02710-8

Praveen Kumar C, Rajendra Prasad K (2021) Multi-ROI segmentation for effective texture features of mammogram images. J Discrete Math Sci Cryptogr 24(8):2461–2469. https://doi.org/10.1080/09720529.2021.2016192

PyCryptodome: Welcome to PyCryptodome's documentation - PyCryptodome 3.8.2 documentation (2019), https://pycryptodome.readthedocs.in/en/stable/index.html

Rajendra Prasad K, Mohammed M, Narasimha Prasad LV et al (2021) An efficient sampling-based visualization technique for big data clustering with crisp partitions. Distrib Parallel Databases 39:813–832. https://doi.org/10.1007/s10619-021-07324-3

Sarfraz MI, Baker P, Xu J, Bertino E (2013) A comprehensive access control system for scientific applications. In: Lopez J, Huang X, Sandhu R (eds) Network and system security. NSS 2013. Lecture Notes in Computer Science, vol 7873. Springer, Berlin, Heidelberg. https://doi.org/10.1007/978-3-642-38631-2_66

Sarosh P, Parah SA, Bhat GM (2022) An efficient image encryption scheme for healthcare applications. Multimed Tools Appl 81:7253–7270. https://doi.org/10.1007/s11042-021-11812-0

Data Encryption Standard (DES) and Advanced Encryption Standard (AES). In: Furht, B. (eds) Encyclopedia of Multimedia. Springer, Boston, MA. https://doi.org/10.1007/978-0-387-78414-4_287

Subba RK, Rajendra PK (2021) An extended fuzzy C-means segmentation for an efficient BTD with the region of interest of SCP. Int J Inf Technol Project Manag (IJITPM) 12(4):11–24. https://doi.org/10.4018/IJITPM.2021100102

Subba Reddy K, Rajendra Prasad K, Kamatam GR et al (2022) An extended visual methods to perform data cluster assessment in distributed data systems. J Supercomput 78:8810–8829. https://doi.org/10.1007/s11227-021-04243-z

Tang H, Sun QT, Yang X, Long K (2018) A network coding and DES based dynamic encryption scheme for moving target defense. IEEE Access 6:26059–26068. https://doi.org/10.1109/ACCESS.2018.2832854

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