

¹Morarjee Kolla²Dr. K. Rajendra Prasad³Dr. K Sreenivasulu⁴Dr. Y. Rama Mohan⁵Chatakunta Praveen Kumar

Secure Image Encryption Techniques with Fuzzy based Operation Modes for Trustworthy Accessing in Communication Devices



Abstract: - Digital networks present a number of interesting research problems, one of which is the secure image transfer through various channels of communication. In these circumstances, cryptography algorithms are commonly employed to securely encrypt and decode data at both the sending and receiving ends. To determine the most effective method of image encryption, a wide range of modern algorithms are analysed and compared. In this study, we describe several fuzzy modes of operation for image encryption. It guarantees the safety of digital image transfer. The work's goal is to provide the most trustworthy image encryption possible; This is achieved by integrating image encryption methods into a hybrid fuzzy based architecture. The proposed composite fuzzy-based encrypted systems (CFES) are recommended for use in order to ensure the security of data on various communications media. The composite fuzzy-based encrypted systems provide strong security while yet protecting users' privacy while viewing image content.

Keywords: Fuzzy Concept, Image Encryption, Fuzzy operation modes, Cryptography Methods, Image Privacy.

I. INTRODUCTION

Images, audio, and video data [1] can be transmitted securely with the help of cryptographic algorithms [2] and access control mechanisms [3]. It has become crucial for reliable apps or cloud services [4] to allow users to safely share and save their multimedia files in intelligent applications [5]. Healthcare image encryption [6], [7] is one of emerging applications that rely on image encryption. The development of secure scientific applications [8], space image map to defence [10], weather image and predictions [11], and software-defined image network analysis [12] all rely on the use of multimedia encryption. The corporate, governmental, and nonprofit sectors all have a need for image cryptography for various security-related applications. There have been several advancements in the field of image cryptography over the past decade, as evidenced by the proliferation of image encryption methods. Raster images store information in blocks of pixels all of the same size and shape [13]. In this way, images sent via insecure channels can be encrypted and decrypted quickly and easily using these pixels. Medical photographs, infrared photos, logos, etc. can all benefit from its image encryption capabilities. Currently, RC6 (Rivest Cypher 6) [15], [21] is the most used method for encrypting images, and it is used in a variety of fuzzy architecture modes [16], which are, cypher feedback (CFB), cypher block chaining (CBC), electronic codebook (ECB), output feedback (OFB). In addition to DES [23] and AES, the most widely employed encryption methods for protecting images are RSA [24] and the advanced encryption standard (AES) [17], [18], [19], [20], [22]. All across the world, private

¹ Associate Professor, Department of CSE, Chaitanya Bharathi Institute of Technology, Hyderabad, Telangana, India

morarjeek_cse@cbit.ac.in

²Professor, Department of CSE, Institute of Aeronautical Engineering, Dundigal, Hyderabad, Telangana, India

krprgm@gmail.com

³Professor of CSE, G. Pullaiah college of Engineering and Technology, Kurnool

sreenu.kutala@gmail.com

⁴Associate Professor in CSE Dept, G. Pulla Reddy Engineering College, Kurnool

yrm.ecs@gprec.ac.in

⁵Assistant Professor, Dept. of CSE, Institute of Aeronautical Engineering, Dundigal, Hyderabad, Telangana, India

c.praveenkumar@iare.ac.in

information is encrypted using software and hardware that adhere to the Advanced Encryption Standard (AES). The following section of this study introduces these state-of-the-art picture encryption methods and describes how they are put into practice [25], [26], [27]. An experimental investigation of the four modes (ECB, CBC, OFB, and CFB) is provided to discover which is best suited to encrypting images. At this stage in the routing process, every node of a cluster checks its degree to see if it should retransmit the route request message. This evaluation is performed by taking into account a variety of characteristics, including the amount of distance travelled, the amount of residual energy, the connection quality, and the total number of steps [28], [29], [30]. During the period designated for communication security, symmetric cryptography is used to ensure the safety of intra-cluster communication.

The following is a brief overview for the contributions of the paper:

1. Illustrate the impact of fuzzy operations in ECB, CBC, OFB, and CFB on image encryption.
2. Describe the composite fuzzy-based encrypted systems, which combine the best features of both traditional image encryption techniques and fuzzy logic modes of operation.
3. Determine the best efficient image encryption pictures for use in image security and privacy applications.
4. Examine the performance of composite fuzzy-based encrypted systems (CFES)
5. Carry out an empirical investigation of the different methods of encryption by using the selected group of reference photos

The following is an outline of the many parts included in the paper: In the second section, the modes of operation of several encryption schemes are presented. In the third section, we take a high-level look at the various picture encryption methods that are currently in use. In the following section, compare and contrast the effectiveness of several image encryption methods. In Section 5, we present the results and the entirety of our work.

II. MODES OF THE OPERATIONS OF ENCRYPTION TECHNIQUES

Any approach for encrypting pictures will execute encryption and decryption for images by taking into account individual image blocks rather than the complete image. Numerous cryptographic algorithms use a method called block-based ciphering as a means of achieving higher authentication levels and greater levels of secrecy. Techniques for encrypting information need to make advantage of unique modes of operation regarding block cyphers. Encryption and decryption must both use the same mode of operation for any technology to be considered secure. The most recent study on picture security discovered that four fuzzy modes, which are utilised often, have a tremendous amount of success. These modes are referred to as CFES based operation modes (i.e. CFES-ECB, CFES-CBC, CFES-CFB, and CFES-OFB)

2.1. Composite Fuzzy-based Encrypted Systems -Electronic codebook (CFES-ECB)

The data is first divided into uniform chunks of size one and encrypted independently in this method of operation. Due to the lack of connection between encrypted blocks, faults are less likely to spread. A single block's fault may not propagate to the rest of the chain. The affected section is limited to the one block. Due to its error-preventing mode of operation, the ECB will not allow the mistake in one block's fuzzy membership values to spread to other blocks. The equations Eqn. (1) and (2) depict its action in detail. Equal-sized blocks of the source data (S.D.) are created (SD_1, SD_2, \dots), and Ciphred blocks (CSD_1, CSD_2, \dots).

$$CSD_i = E_K(SD_i) \quad (1)$$

$$SD_i = D_K(CSD_i) \quad (2)$$

When the same key ('K') is considered in ECB, the divided blocks undergo the same protocol transformation to become cypher blocks. In order to decode a partitioned block, the key 'K' must be used on all partitions. Therefore, ECB may not always ensure the safety of data transfer through the internet. In spite of this, it is now widely considered to be one of the least popular error access control encrypted systems. With ECP in operation, a codebook may be built using the same encryption and decryption procedures for recurrent picture blocks. It may not be able to protect the encrypted data from assaults using the ECB. In this case, the following operational modes are used.

Using a symmetric key and algorithm, a block cypher encrypts and decrypts data in blocks. Adding an initialization vector (IV) to the input plaintext of a block cypher expands the cypher's keyspace, making brute-force key derivation more challenging. This makes it harder to duplicate the key.

2.2 Composite Fuzzy-based Encrypted Systems -Cipher blockchain (CFES-CBC)

Another form of operation, bits XOR operation of data, may solve the ECB image encryption issue. The XORing with fuzzy membership values is performed between the source block and the previously encrypted block of data. It's a loop that only ends when the XOR operation is performed on the data from the most recent block with the encrypted data from the prior block. Image encryption and decryption using XOR bits is shown in Eqn. (3)–(5), which represent the 'CBC' operating mode.

$$CD_0 = IVec \quad (3)$$

$$CD_j = E_K(CD_{j-1} XOR SD_j) \quad (4)$$

$$SD_j = D_k(CD_j) XOR CD_{j-1} \quad (5)$$

XORing together the currently encrypted block with the previously encrypted block yields the decrypted block in CBC mode. The first cypher data (denoted 'CD0') is derived from a randomly chosen initialization vector (IVec). Data block 'DB1' is used to generate encipher data 'CD1' for the block of 'SD1' by applying XOR to the original cypher data (or IVec). It continues in this fashion until all of the data has been encrypted, at which point the final encipher block is acquired.

2.3 Composite Fuzzy-based Encrypted Systems -Cipher Feedback (CFES-CFB)

Initial encrypted data is produced by the CFB operating mode using the initialization vector (IVec). The equation given in Eqn. (6) provides a good description of it.

$$CD_0 = IVec \quad (7)$$

$$ENC_j = E_K(CD_{j-1}), j = 1, 2, \dots \quad (8)$$

$$CD_j = SD_j XOR ENC_j \quad (9)$$

$$SD_j = CD_j XOR SD_j \quad (10)$$

The first data block (SD1) and initial IVec are encrypted, and their resulting encrypted data is applied using an XOR operation in the subsequent recursive phases. These iterative encryption and decryption procedures are carried out in accordance with the aforementioned modelling phases for the data blocks (SD1, SD2,.....), as illustrated in Eqn. (7) through Eqn. (10). The encrypted data blocks (CD1, CD2,.....) are obtained by applying the encrypted key K to the original data blocks (SD1, SD2,.....).

If an error of at least one bit is discovered in either the current or prior data block, it has the potential to propagate through the CFB mode and into the subsequent fuzzy based ciphered blocks. This technique of encryption is not the most secure.

2.4 Composite Fuzzy-based Encrypted Systems -Output Feedback (CFES-OFB)

In OFB's method of operation, the data blocks are collected at varying sizes.

$$I_0 = IVec \quad (11)$$

$$I_j = E_K(I_{j-1}), j = 1, 2, \dots \quad (12)$$

$$CD_j = SD_j XOR I_j \quad (13)$$

$$SD_j = I_j XOR SD_j \quad (14)$$

In contrast to the CFB mode, the OFB mode uses the encryption function as feedback rather than cypher data in an effort to solve the fuzzy synchronised stream ciphering issue. Except for the feedback function, OFB is modelled similarly to CFB. Eqn. (11)–(14) are the equations used to model OFB.

III. IMAGE ENCRYPTION TECHNIQUES

Image encryption is used to conceal information about the pictures themselves, block by block. These are outlined, and the steps involved in implementing them are covered. The RC6 algorithm [19] is a cutting-edge method for encrypting images; it provides robust protection for picture blocks in each of the modes discussed above.

A. Existing RC6 for Image Encryption

The RC6 method divides the original picture into smaller, more manageable chunks (say, 128-bit data blocks). These divided blocks must not overlap, and once obtained, they are sent on to the first RC6 encipherment stage. In the enciphering step, the original picture is decrypted using one of four operating modes: EBC, CBC, CFB, or OFB. After then, the encrypted picture is built by piecing together all the encrypted pieces. The picture is encrypted before transmission for further security. Once the encrypted picture reaches the receiving end, it is once again separated into blocks of the same size as the original 128-bit block. Send all partitioned encrypted blocks that do not overlap to the RC6 decryption step. At the decoding stage, the blocks are presented in the same operating modes that were used during enciphering. At the end, the decrypted picture is constructed by combining blocks that have already been received after decryption. The stages involved in these methods of procedure are shown in Fig. 1.

Using membership functions, the fuzzy logic approach to edge linking may ascertain whether or not a given pixel is indeed part of an edge or a homogeneous area. This may be accomplished by comparing the pixel in question to its immediate neighbours. The membership function for each input of the edge is a Gaussian with zero mean.

In this research, we provide the technique that provides substantial support for the increased user level security. The proposed approach generates random keys that are both secure and computationally efficient. Fuzzy logic is responsible for the development of this secure picture data access system.

B. RSA Image encryption Technique

Since the public key and private key are used for encryption and decryption on opposite sides of the connection, RSA [20] is considered an asymmetric encryption method. Symmetric methods encrypt and decode with the same key. Since the transmitter and receiver share the same secret, symmetric cryptography is not as effective as asymmetric cryptography in preventing hacker attacks. RSA shows how to decipher an RSA encrypted message by locating the public and private keys.

Encryption is the process of encoding a communication in a way that renders it unintelligible to an eavesdropper. One of the most essential ideas in cryptography is encryption. Caesar was the first to use this practise in order to encrypt his communications using the Caesar cypher.

C. Advanced Encryption Standards (AES) Technique towards Image Encryption

It is a kind of symmetric block cypher that falls within that category. It works well with encrypted picture data of varying lengths. The AES [21] is built with varying key lengths; these variants include the AES-256, AES-192, and AES-128 methods [22]. These techniques provide deciphering results after 10, 12, and 14 iterations, respectively. There are four separate steps involved in each cycle: key addition, row shift, column mix, and sub-byte. In AES-128, for instance, there are ten rounds total, and although all four transformations may be tried in the first nine rounds, only the mix-transformation is prohibited in the final round. To decode the message, we employ reverse operations such as "inverse replace bytes," "inverse shift rows," and "inverse mix columns." For the purpose of the sub-byte transformation, the 8-bit substitution box is used to convert each 8-bit (byte) data block into a unique variant.

D. Data Encryption Standards (DES) Technique towards Image Encryption

Data in both the public and private sectors may benefit from this kind of protection, making it the most popular of its kind. The tiny amount of the data, however, makes it vulnerable to a brute force assault. The DES [23] uses a 64-bit key and a 56-bit critical length. Assume that a weak key is employed, which leaves the system open to attack since it limits the key length to 56 bits. The method is thought to be protected by yet another DES variant, known as Triple-DES [24]. Moreover, several theoretical counterarguments show it.

IV. EXPERIMENTAL DESCRIPTION AND RESULTS COMPARATIVE ANALYSIS

CFES-CBC, fuzzy-EBC, CFES-CFB, and CFES-OFB are the four fuzzy-based operating modes used in the proposed work to encrypt images using AES, RC6, DES, and Triple DES. The 'pycryptodome' [25] developed python libraries that were used to implement the proposed CFES based fuzzy models. The Advanced Encryption Standard (AES) generates symmetric keys of either 256 bits, 192 bits, or 128 bits in length. The U.S. government regards AES as the best encryption method available and suggests that all nations use it. Only keys of a length of 256 bits will be accepted by the AES algorithm. Using the Nike logo, a medical picture from the first set, a medical image from the second set, the C.S. logo, and a chessboard, these composite hybrid models are tested. Figure 1 displays the experimental images used in the research and performance evaluation of proposed CFES based fuzzy models.


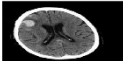
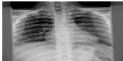
















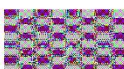














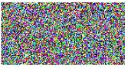
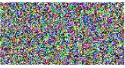
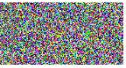




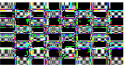
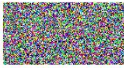


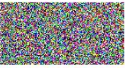


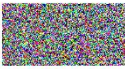
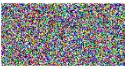
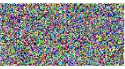
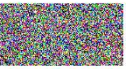
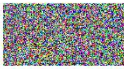
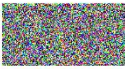
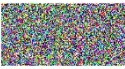
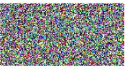
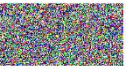
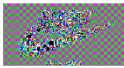


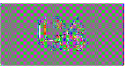
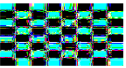

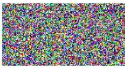

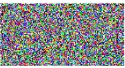
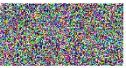
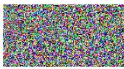

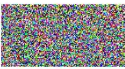
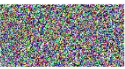
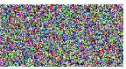


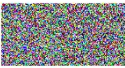



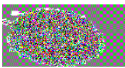

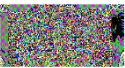
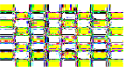
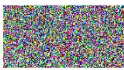




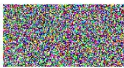
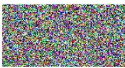


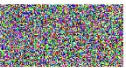



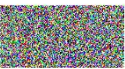

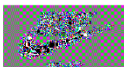



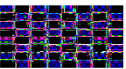





(a) Nike Image (b) Medical Image 1 (c) Medical Image 2 (d) CS Logo (e) Chess board

Figure 1 Test Images for Performance Evaluation of Image Encryption Techniques

Image encryption systems are evaluated using quality metrics such as the entropy measure, correlation coefficient, histogram deviation, number of pixels changing at a given rate (NPCR), peak signal to noise ratio test (PSNR), and feature similarity test (FST) [14]. Image encryption is simulated in MATLAB to evaluate the quality. The many modes of operation used in image encryption (ECB, CBC, CFB, and OFB) are shown graphically via visual inspection (VI). There is a bottleneck in applying well-performing enciphering techniques because of the encryption of such pattern blocks to similarly enciphered blocks, which is used to process and characterise picture information. Table 1 displays the VI for the various hybrid image encryption models that have been presented.

Table 1: Encrypted Images Using Variant CFES-based Fuzzy Models

Encryption Method					
AES- CFES-CBC					
AES-CFES-CFB					
AES-CFES-ECB					
AES-CFES-OFB					
ARC2-CFES-CBC					

ARC2-CFES-CFB					
ARC2-CFES-ECB					
ARC2-CFES-OFB					
Blowfish-CFES-CBC					
Blowfish-CFES-CFB					
Blowfish-CFES-ECB					
Blowfish-CFES-OFB					
Triple DES- CFES-CBC					
Triple DES- CFES-CFB					
Triple DES-fuzzy-ECB					
Triple DES - CFES-OFB					
SingleDES-CFES-CBC					
SingleDES-CFES-CFB					
SingleDES-CFES-ECB					
SingleDES-CFES-OFB					

RC6-CFES-CBC					
RC6—CFES-ECB					
RC6-cfb					
RC6-ofb					
RSA-image					

The findings of the image encryption experiment showed that the proposed model using the "ECB" was less successful than the other operation modes. Composite fuzzy encryption system (CFES) using CBC, CFB, and OFB yields the best-ciphered pictures. The original picture has been encrypted more effectively using hybrid models, such as AES-CFES-OFB, DES-CFES-OFB, RC2-CFES-OFB, and Triple DES-CFES-OFB which also provide the most dissimilar ciphered image to the matching original image. Five standard test pictures are used to analyse the encrypted output, and it is found that RC2 provides subpar encryption. In all CFES-based modes, composite also produced satisfactory encrypted images.

Table 2: Performance Analysis of Image Encryption Methods for the Sample Image “Nike”

Name of the Encryption Technique	Value of Entropy	Value of Correlation	Value of Histogram Deviation	Value of NCPR	Value of UACI	Value of PSNR
AES-CFES-CBC	0.824948	0.389868	3.770321	0.361844	0.265292	7.347743
AES-CFES-CFB	0.825529	0.38654	3.774426	0.362446	0.265908	7.326152
AES-CFES-ECB	0.669234	0.545	2.82777	0.294893	0.199263	9.185229
AES-CFES-OFB	0.822093	0.387317	3.750225	0.361356	0.264279	7.361529
ARC2-CFES-CBC	0.824628	0.389345	3.768063	0.361622	0.265015	7.356835
ARC2-CFES-CFB	0.82189	0.389398	3.748806	0.360901	0.263913	7.376159
ARC2-CFES-ECB	0.890912	0.215931	5.629452	0.501028	0.397601	5.037096
ARC2-CFES-OFB	0.823033	0.391343	3.756832	0.361328	0.264522	7.361172
Blowfish-CFES-CBC	0.822667	0.386149	3.754253	0.361649	0.264736	7.347077
Blowfish-CFES-CFB	0.825585	0.386372	3.774822	0.362634	0.265879	7.328138
Blowfish-CFES-ECB	0.825656	0.461362	3.775326	0.36168	0.264472	7.393998
Blowfish-CFES-OFB	0.827754	0.385425	3.790203	0.363139	0.266683	7.316366
Triple DES – CFES-CBC	0.824928	0.391876	3.770184	0.362047	0.265104	7.356196

Triple DES – CFES-CFB	0.824924	0.386697	3.770153	0.362105	0.265513	7.337312
Triple DES –fuzzy-ecb	0.830154	0.509293	3.807308	0.362482	0.263591	7.488985
Triple DES – CFES-OFB	0.825622	0.389185	3.775082	0.362386	0.265696	7.336975
DES-CFES-CBC	0.82289	0.383853	3.755825	0.361832	0.264918	7.341225
DES-CFES-CFB	0.824626	0.388654	3.768047	0.362222	0.265273	7.344897
DES-CFES-ECB	0.833826	0.489933	3.83366	0.36256	0.26608	7.415763
DES-CFES-OFB-image	0.826922	0.395085	3.784298	0.362518	0.265775	7.348414
RC6-CFES-CBC	0.853313	0.310334	0.524356	0.363423	0.263443	7.857773
RC6-CFES-ECB	0.832222	0.324513	0.510977	0.387863	0.264552	7.853445
RC6-CFES-CFB	0.833322	0.312224	0.488783	0.323422	0.263323	7.632223
RC6-CFES-OFB	0.835224	0.325422	0.335223	0.373224	0.263457	7.977224
RSA	0.843442	0.313346	0.332323	0.366533	0.262323	7.752335

Performance results for the sample Nike picture used in the necessary demonstration of hybrid encryption models are shown in Table 2. The examined images consist of a Nike logo, two medical images, a cs logo, and a chessboard; the effectiveness of the hybrid encryption models is assessed by calculating entropy parameters, correlation coefficients, histogram deviations, NCPRs, UACIs, and PSNRs. The best encrypted image is achieved when the entropy, correlation coefficient, histogram deviation, and NCPR and UACI values are all high. All composite models outperformed RSA, as shown in the study and the visual evidence in Table 1. Furthermore, it shown that CFES based on RC6 encryption were superior than the alternatives.

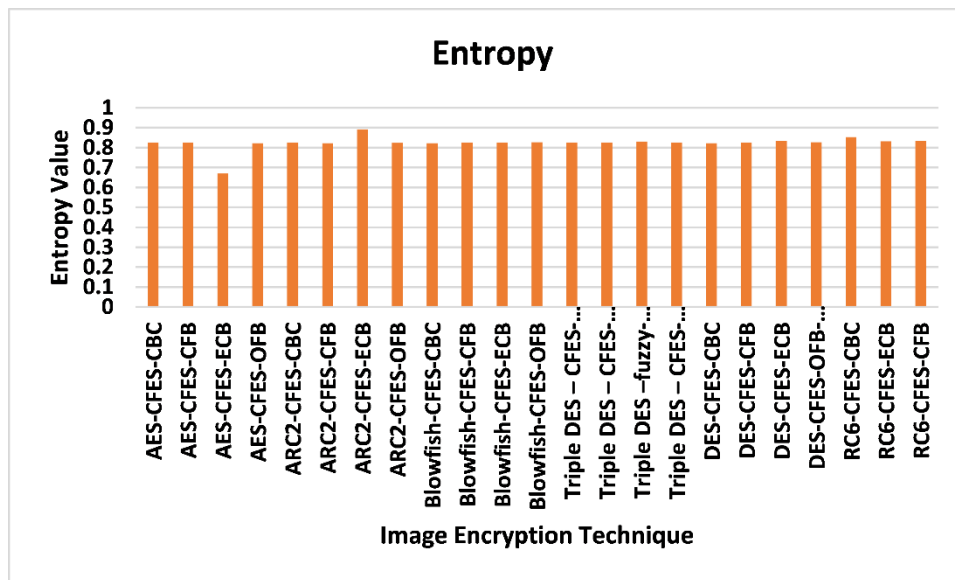


Figure 2 Performance Comparison Using Entropy

Proposed encryption techniques (CFES-CBC, CFES-CFB, CFES-ECB, and CFES-OFB) have been experimented using benchmarked images. During the evaluation process, the best encryption is chosen based on the following five metrics:

1. The best encryption uses a higher value of entropy
2. For optimal encryption, the degree of similarity between the original and encrypted versions of an image should be low.
3. For the best encrypted image, the histogram divergence between the original and encrypted versions should be maximised.

4. The well-defined encryptions should place when good value of NPCR and UACI, which
5. When trying to find the best encrypted version of the original image, PSNR values tend to be low.

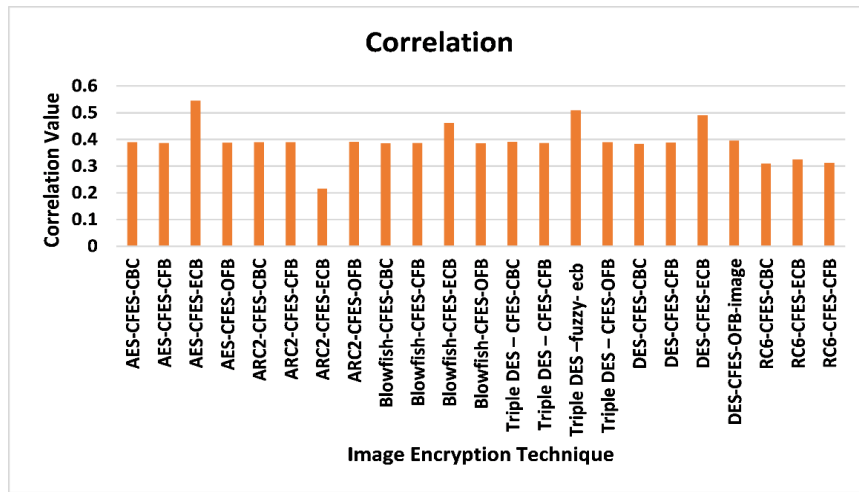


Figure 3 Performance Comparison Using Correlation

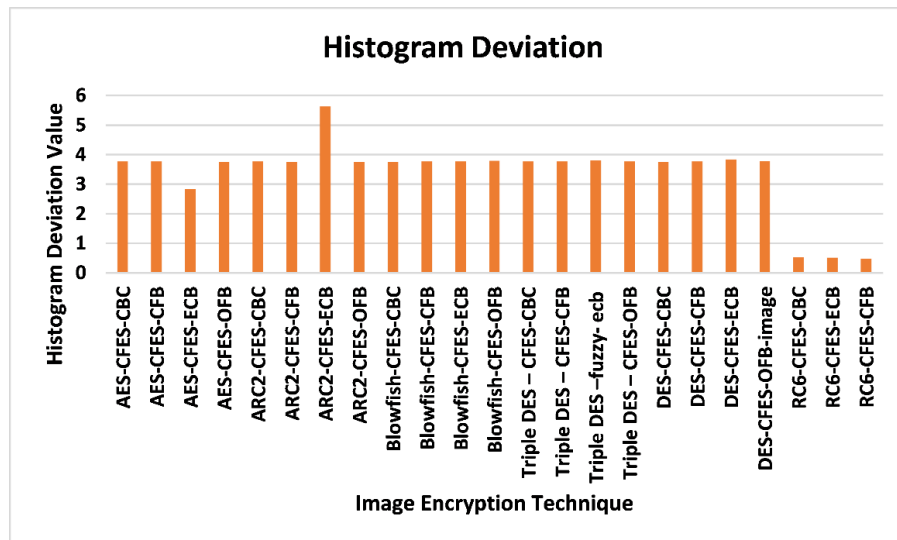


Figure 4 Performance Comparison Using Histogram Deviation

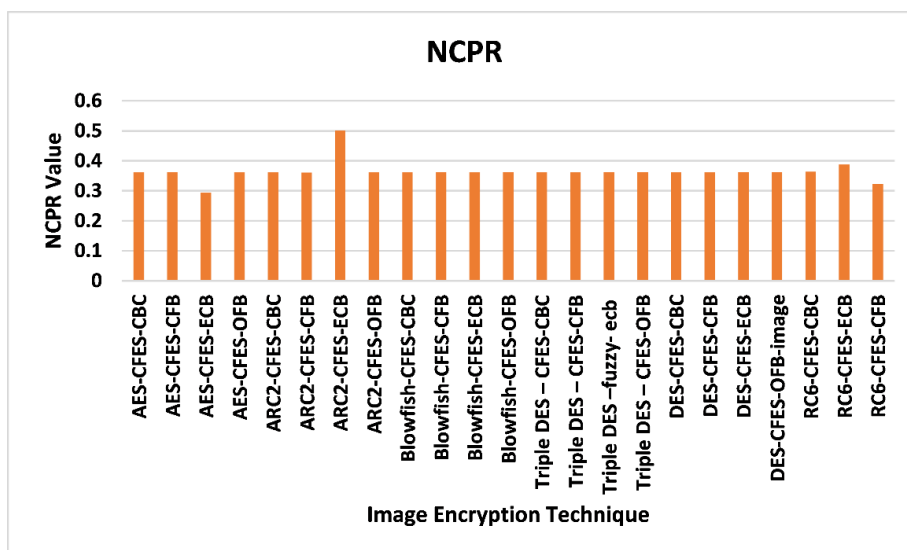


Figure. 5 Performance Comparison Using NPCR

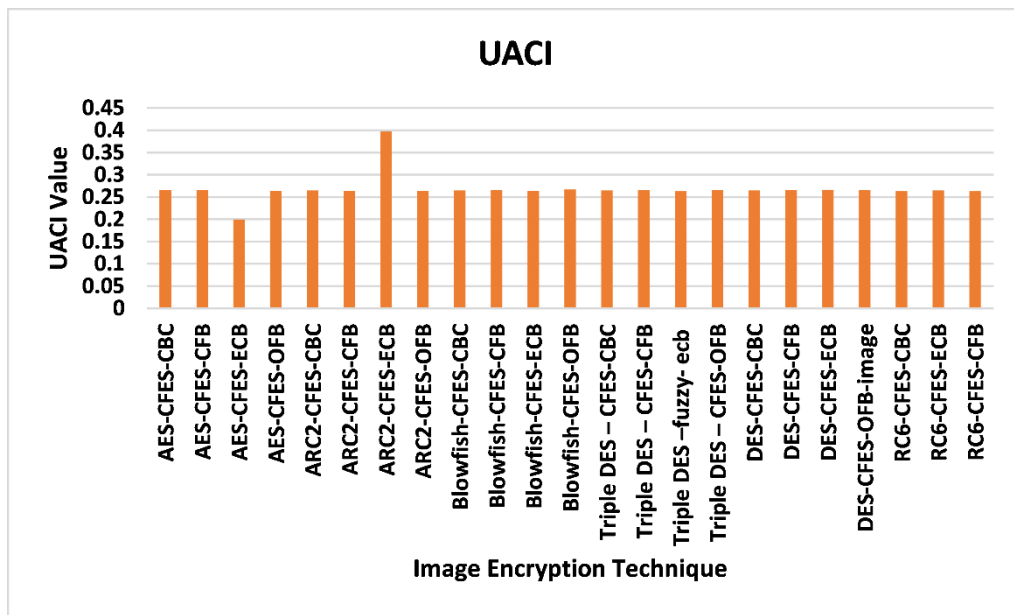


Figure. 6 Performance Comparison Using UACI

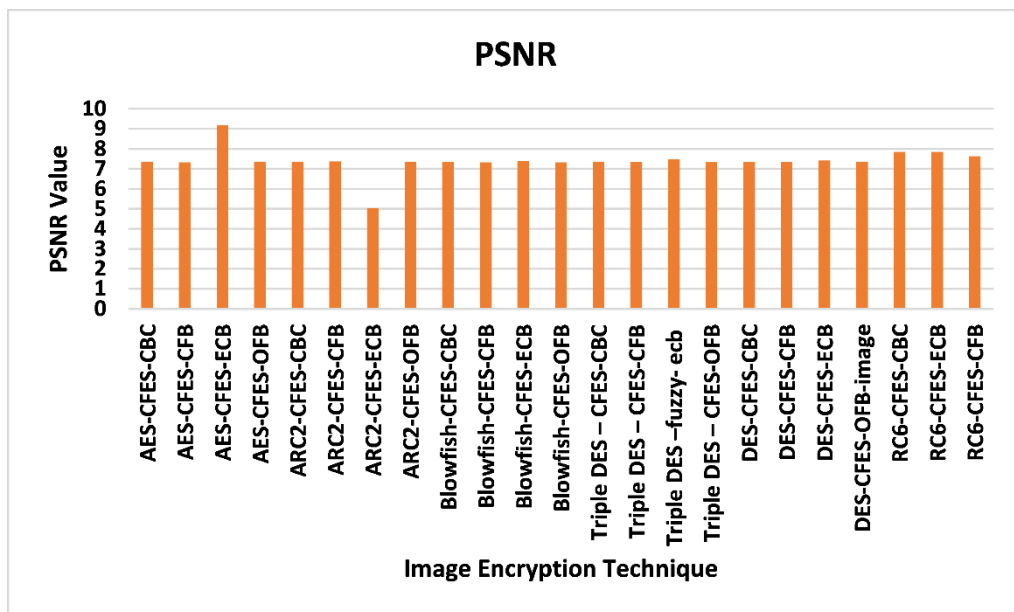


Figure. 7 Performance Comparison Using PCNR

Chess image, cslogo image, two medical photos, and a nike image are used in the experiments. The whole set of comparative findings for encryption performance is shown in Figs. 2–7. The best encrypted results were seen using the CFES modes, cbc, cfb, and ofb when using the encryption algorithms AES and Triple DES. The best results are achieved by using ARC2 or Single DES with CFES-ECB operating modes. In the CFES-ECB mode of operation, these methods provide satisfactory encrypted pictures. The highest level of encryption is necessary for the safety of portable devices based on robotics. All modalities of fuzzy operation often aid all forms of encryption. When sending sensitive multimedia data to a robotics device hosted in the cloud, it is best to use a hybrid encryption method. Fig. 2 to Fig. 7 shows the evaluation of image encryption method using the measures of entropy, correlation, histogram deviation, NCPR, UACI, and PCNR respectively. These comparative graphs shown that proposed CFES under ECB mode produced the optimal values than others. That is, CFES with ECB mode is more efficient image encryption model than others.

V. CONCLUSION AND SCOPE OF THE WORK

There is a growing need for image encryption in real-time communication channels that poses valid access to sensitive data. By applying image encryption methods to the source images, cypher images may be created. Compositive fuzzy encryption systems is proposed in this paper that scheme rely on a completely arbitrary method of key generation. In order to encrypt a message or image, the data must first be split into many blocks. However, these approaches are insufficient for generating cypher images with improved secure mode annotations through random keys. This is why encrypted image and operation mode hybrid models are being created. The results of the experiments showed that while using OFB mode, the composite model produced more secure encrypted images than RSA. Under the CFB operation mode, no encryption method yields images with a high degree of difference in ciphertext. As per the experimental results, it is concluded that CFES with ECB may be made more effective for bio-accessing purposes by using asymmetric image encryption methods.

In future, the proposed CFES is to be extended for handling the encryption for real time video streaming encryption for preserving the security in cloud storage devices.

REFERENCES

- [1] Kuckartz, U., Rädiker, S. (2019). Coding Video Data, Audio Data, and Images. In: Analyzing Qualitative Data with MAXQDA. Springer, Cham. https://doi.org/10.1007/978-3-030-15671-8_7
- [2] Ogunseyi, T.B., 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
- [3] Muhammad Umar Aftab, Ali Hamza, Ariyo Oluwasanmi, Xuyun Nie, Muhammad Shahzad Sarfraz, Danish Shehzad, Zhiguang Qin, Ammar Rafiq, "Traditional and Hybrid Access Control Models: A Detailed Survey", Security and Communication Networks, vol. 2022,
- [4] X. Duan, R. P. Giddings, S. Mansoor and J. M. Tang, "Experimental demonstration of upstream transmission in digital filter multiple access pons with real-time reconfigurable optical network units," in Journal of Optical Communications and Networking, vol. 9, no. 1, pp. 45-52, Jan. 2017, DOI: 10.1364/JOCN.9.000045.
- [5] H. Huang and W. Fang, "Intelligent Multimedia Data Hiding Techniques and Applications," 2008 International Conference on Information Security and Assurance (isa 2008), 2008, pp. 477-482, DOI: 10.1109/ISA.2008.83.
- [6] El-Shafai, W., Khallaf, F., El-Rabaie, ES.M. et al. Robust medical image encryption based on DNA-chaos cryptosystem for secure telemedicine and healthcare applications. J Ambient Intell Human Comput 12, 9007–9035 (2021). <https://doi.org/10.1007/s12652-020-02597-5>
- [7] Sarosh, P., Parah, S.A. & Bhat, G.M. An efficient image encryption scheme for healthcare applications. Multimed Tools Appl 81, 7253–7270 (2022). <https://doi.org/10.1007/s11042-021-11812-0>
- [8] Sarfraz, M.I., 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
- [9] Ahmed, N., Bakar, K.A., Zuhra, F.T. et al. Security & Privacy in Software Defined Networks, Issues, Challenges and Cost of Developed Solutions: A Systematic Literature Review. Int J Wireless Inf Networks (2022). <https://doi.org/10.1007/s10776-022-00561-y>
- [10] H. Lin, Y. Bo, J. Wang and X. Jia, "Landscape structure based super-resolution mapping from remotely sensed imagery," 2011 IEEE International Geoscience and Remote Sensing Symposium, 2011, pp. 79-82, DOI: 10.1109/IGARSS.2011.6048902.
- [11] M. A. Al-Khasawneh, W. Abu-Ulbeh and A. M. Khasawneh, "Satellite images encryption Review," 2020 International Conference on Intelligent Computing and Human-Computer Interaction (ICHCI), 2020, pp. 121-125, DOI: 10.1109/ICHCI51889.2020.00034.
- [12] Q. Liu, Y. Peng, J. Wu, T. Wang and G. Wang, "Secure Multi-keyword Fuzzy Searches With Enhanced Service Quality in Cloud Computing," in IEEE Transactions on Network and Service Management, vol. 18, no. 2, pp. 2046-2062, June 2021, DOI: 10.1109/TNSM.2020.3045467.
- [13] Subba Reddy K. & Rajendra Prasad K. (2021). An Extended Fuzzy C-Means Segmentation for an Efficient BTM With the Region of Interest of SCP. International Journal of Information Technology Project Management (IJITPM), 12(4), 11-24. <http://doi.org/10.4018/IJITPM.2021100102>
- [14] Jannatul Ferdush, Mahbuba Begum, Mohammad Shorif Uddin, "Chaotic Lightweight Cryptosystem for Image Encryption", Advances in Multimedia, vol. 2021, Article ID 5527295, 16 pages, 2021. <https://doi.org/10.1155/2021/5527295>

- [15] O. S. Faragallah et al., "Efficiently Encrypting Color Images With Few Details Based on RC6 and Different Operation Modes for Cybersecurity Applications," in *IEEE Access*, vol. 8, pp. 103200-103218, 2020, DOI: 10.1109/ACCESS.2020.2994583.
- [16] Faragallah, O.S., El-Sayed, H.S., Afifi, A. et al. Small Details Gray Scale Image Encryption Using RC6 Block Cipher. *Wireless Pers Commun* 118, 1559–1589 (2021). <https://doi.org/10.1007/s11277-021-08105-y>
- [17] Hammad, I., El-Sankary, K. and El-Masry, E. (2012). Advanced Encryption Standard (AES) Implementation in Embedded Systems. In *Embedded Systems*, K. Iniewski (Ed.). <https://doi.org/10.1002/9781118468654.ch13>
- [18] Dunkelman, O., Keller, N. & Shamir, A. Improved Single-Key Attacks on 8-Round AES-192 and AES-256. *J Cryptol* 28, 397–422 (2015). <https://doi.org/10.1007/s00145-013-9159-4>
- [19] 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
- [20] S. Kumar, B. K. Singh, Akshita, S. Pundir, S. Batra and R. Joshi, "A survey on Symmetric and Asymmetric Key based Image Encryption," *2nd International Conference on Data, Engineering and Applications (IDEA)*, 2020, pp. 1-5, DOI: 10.1109/IDEA49133.2020.9170703.
- [21] Elashry, I. F., Faragallah, O. S., Abbas, A. M., El-Rabaie, S., & Abd El-Samie, F. E. (2012). A new method for encrypting images with few details using Rijndael and RC6 block ciphers in the electronic codebook mode. *Information Security Journal: A Global Perspective*, 21, 193–205.
- [22] Gladman, B. (2003) A specification for Rijndael, the AES algorithm.
- [23] Suleman Basha, M., Mouleeswaran, S.K. & Rajendra Prasad, K. Hybrid visual computing models to discover the clusters assessment of high dimensional big data. *Soft Comput* 27, 4249–4262 (2023). <https://doi.org/10.1007/s00500-022-07092-x>
- [24] H. Tang, Q. T. Sun, X. Yang and K. Long, "A Network Coding and DES Based Dynamic Encryption Scheme for Moving Target Defense," in *IEEE Access*, vol. 6, pp. 26059-26068, 2018, DOI: 10.1109/ACCESS.2018.2832854.
- [25] R. Imam, Q. M. Areeb, A. Alturki and F. Anwer, "Systematic and Critical Review of RSA Based Public Key Cryptographic Schemes: Past and Present Status," in *IEEE Access*, vol. 9, pp. 155949-155976, 2021, DOI: 10.1109/ACCESS.2021.3129224.
- [26] Subba Reddy, K., Rajendra Prasad, K., Kamatam, G.R. et al. An extended visual methods to perform data cluster assessment in distributed data systems. *J Supercomput* 78, 8810–8829 (2022). <https://doi.org/10.1007/s11227-021-04243-z>
- [27] Prasad, K.R. (2019). Big Data Sentiment Analysis Using Distributed Computing Approach. In: Bapi, R., Rao, K., Prasad, M. (eds) *First International Conference on Artificial Intelligence and Cognitive Computing . Advances in Intelligent Systems and Computing*, vol 815. Springer, Singapore. https://doi.org/10.1007/978-981-13-1580-0_66
- [28] C. Praveen Kumar & K. Rajendra Prasad (2021) Multi-ROI segmentation for effective texture features of mammogram images, *Journal of Discrete Mathematical Sciences and Cryptography*, 24:8, 2461-2469, DOI: 10.1080/09720529.2021.2016192
- [29] Basha, M.S., Mouleeswaran, S.K. & Prasad, K.R. Detection of pre-cluster nano-tendency through multi-viewpoints cosine-based similarity approach. *Nanotechnol. Environ. Eng.* 7, 259–268 (2022). <https://doi.org/10.1007/s41204-022-00222-8>
- [30] Subba Reddy K., and Rajendra Prasad K. "An Extended Fuzzy C-Means Segmentation for an Efficient BTD With the Region of Interest of SCP." *IJITPM* vol.12, no.4 2021: pp.11-24. <http://doi.org/10.4018/IJITPM.2021100102>