**Selective Region Hybrid Multiple Key Validation System for Effectively Authenticating Digital Images**

Pratyush Kumar, Vishnu Shetty Belanje, Aju D

School of Computer Science and Engineering,

Vellore Institute of Technology, Vellore.

daju@vit.ac.in

**ABSTRACT**

*In the modern day, pictures and multimedia data have become a common part of life and it is very important that they are safely secured and visible only to those who have the authority to view the data. At the same time, it can be observed that the whole image is not sensitive. A hybrid encryption algorithm that uses a two-step encryption mechanism and only encrypts the sensitive regions of an image is proposed. The proposed method aims to improve upon the existing RSA algorithm by incorporating a modified CBC algorithm, to produce an improvement in encryption/decryption time by 40%, as well as a 90% decrease in the correlation of the encrypted image with respect to the RSA algorithm*.

**KEYWORDS**

Information Security, Partial Image encryption, Sensitive Region Detection, Hash Function, PBKDF2, RSA Mapping, Non-linear CBC, and Image Scrambling.

**INTRODUCTION**

Multimedia use has boomed in the past 20-30 years. Many new kinds of multimedia formats are used to transmit data between users in various applications over the Internet or wireless connection, posing security risks. The main challenges in delivering multimedia data are speed, the ethical use of the material, and secure transfer. Attempts to tackle such challenges contribute to a better knowledge of this complicated technology as well as the development of new solutions. In general, concealment techniques such as digital watermarking and encryption are used in multimedia authenticity/security solutions.

Multimedia encryption's main goal is to stop unauthorized access to sensitive multimedia data while it's in storage or transit. The task of MME is to convert multimedia content (plaintext message) into a distorted and incoherent data flow. The encrypted message (data stream) is also sometimes known as ciphertext. The most basic method for multimedia encryption would be to interpret the protected multimedia signal as a standard digital stream of data, such as a video or audio file. To encrypt the whole data stream, an application-centric classical algorithm and key management system should be used. The encrypted data (ciphertext digital data) would be deciphered upon reception, and recapitulation may begin on the client’s end.

RSA is an encryption algorithm and is highly secure as it is based on the fact that it is very costly to factorize the product of two very big positive prime integers. Asymmetric algorithms such as RSA are ones in which the encryption is used by the sender; a public key is different from the key used by the receiver; a private key. RSA encryption carries out the encryption operation using a key known as the public key which is known to all users. To decrypt an encrypted communication, both keys are required. This is because of the intricate mathematical concepts of the RSA algorithm. A key pair is made up of each RSA user's public and private keys. The private key must be kept private.

Before utilizing the encryption key, the initial block of plaintext is XORed and the result is encrypted in the Cipher Block Chaining (CBC) mode. CBC incorporates an initialization vector (IV). The IV is a chunk of text composed entirely of random bits. The first chunk of the ciphertext is the resulting block. Before encryption, a procedure known as "chaining" involves XORing each block of plaintext with the block of ciphertext that came before it. This XOR method is used to avoid generating the same ciphertext by the same plaintext again. Decryption happens in a reverse way. To retrieve the original plaintext, the final block of ciphertext which results after decryption is XORed with the block of ciphertext which came before it. The CBC mode is used in hash algorithms. When used for this purpose, all earlier blocks are removed, and the last block is kept as the final hash.

**LITERATURE SURVEY**

A technique for leveraging FF1 and FF3-1 to partially encrypt sensitive data in images [1] has been suggested which eliminates unused storage space by encrypting sensitive data without growing the data size. Through studies, the authors have demonstrated that the suggested technique is just as secure as AES-based encryption. The suggested approach can be used in a variety of picture-using contexts, including IoT devices, drones, and CCTV. A novel hybrid encryption approach based on chaos [2] is described for secure and potent image encryption. This study has come up with a CS-AES framework whicthatmore secure than the standard algorithms adopting the same ideology. It is also quick and less computation intensive, making it suitable for image encryption systems that require security and speed.

A quick AES-based picture cryptosystem [3] is verified. The user-provided image is divided into 128-bit chunks of data. The results of the simulations demonstrate the security and the speed of this image cryptosystem, which might serve as the standard for newly proposed chaotic system-based image cryptosystems. It is necessary to improve picture cryptosystems whose encryption/decryption speeds are lower than those of the AES-based architecture on the same system. A new-fangled image encryption system that uses the RSA algorithm and an extended Arnold map [4] has been put forward. The recommended asymmetric picture encryption technique is secure, effective, has high key responsiveness ,and is quite resistant to attacks, according to experimental findings and tests. To keep image transfer secure, the key is generated by the RSA algorithm and isutilizedd in the image encryption system. Concerning data encryption, a useful and effective discussion on RSA and ECC with DES, 3DES, AES, Blowfish, Twofish, and Threefish, are popular asymmetric encryption techniques. Also, concerning data encryption methods, a study that discusses and contrasts the RSA and ECC algorithms along with other standard asymmetric key cryptographic calculations is presented. As a result, the use of elliptic curve encryption in Bitcoin, SSH, and TLS has been investigated.

An image encryption-decryption technique that utilizes the Chaotic map along with the Blowfish algorithm has been put forward. The suggested approach, which makes use of the robust operations supported by modern computers, offers significantly better security and performance than the conventional Blowfish algorithm. It is suggested to use a unique image encryption technique that combines the chaotic sequence and the altered AES algorithm [7]. According to the simulation results, even little modifications to the original picture or key cause substantial modifications in the encrypted image, rendering the original image inaccessible. Additionally, this feature stops uunauthorizedindividuals from decrypting the encrypted picture. The chaotic performance of a newly suggested two-dimensional redesigned Henon map (2D-MHM) [8] is studied. The devised algorithm provides more security than ordinary encryption techniques. A comparison between several (conventional and modern) ccipherschemes [9] for images depending on certain criteria like Histogram, Correlation, NPCR, UACI, PSNR, Entropy, and Time complexity has been conducted. Chaotic encryption algorithms, particularly hyper-chaotic ones, are the most effective of all of them, according to an examination of simulation findings.

An image encryption algorithm [10] based on the ideology of random walk and two hyperchaotic techniques has been proposed. The location of pixels inside a section of a picture is randomly altered using the random walk technique. The proposed encoding system is highly secured based on the findings of the various experiments and analyses. Cosine transform is utilized as a nonlinear transform in the initial proposal of the CTBCS, a cosine-transform-based chaotic system [11] that produces new chaotic maps with sophisticated chaos performance. Furthermore, it is observed that this research has the potential to advance chaos theory and chaos-based encryption. It has been shown that a quick AES-based picture cryptosystem is feasible [12]. The outcomes of the simulations show how quick and secure the image encryption system is. A practical approach for creating safe image encryption and decryption methods [13] has been put forth. With the use of AES libraries, the safety of the image in this encryption process has improved. Several test photographs of varying sizes are used to show how well the encryption method works. The overall goal of this study is to demonstrate the impact of employing several keys of different sizes for the algorithm's security.

Data in the form of images is used here and is encrypted and protected from hackers [14] using a variety of encryption techniques. Numerous encryption techniques have been thoroughly analyzed. The study shows that AES has the greatest MSE value. Although watermarking has the highest PSNR, it also has the lowest MSE, making it a less secure method. The uncompressed image will encode the content using the encryption key in this study since reversible information hiding encryption [15] is utilized. The algorithmic rule granted here gives logical guidance for the Triple DES calculation to enter the broad information concealing calculation in terms of secure correspondence. Based on a variety of parameters which includes PSNR, UACI Histogram, Entropy, NPCR, Correlation, and Time Complexity [16], a comparison between several cipher techniques (classic and modern) for images has been performed. Overall, it is observed that the most effective encryption method is chaotic encryption, particularly hyper-chaotic encryption. The Diffie Hellman algorithm and Blowfish algorithm [17] ideas are used to achieve the suggested technique. By offering a 2-level safety system and addressing the majority of the issues with existing algorithms, the suggested solution makes sure that only authorized users can view the information.

The picture encryption method has been given a better logistic map [18]. The respective algorithm has limitless key size, and the key responsiveness is reasonably strong, which can withstand the assault of exhaustion method analysis. This could be observed and understood based on the experimental simulation findings and analysis. Therefore, the improved Logistic map may be used to guard against picture encryption, and the technique is straightforward, quick, and has a wide range of real-world applications. The FF1 technique which is the format-preserving encryption [19] has been examined in this study. Using the appropriate dataset, an encryption model was constructed, through which several tests were executed, including histogram analysis, NPCR (Number of Pixel Changing Rate) scores, and computing cost. Given that the size and quantity of photos may be minimal enough to carry out all necessary encryptions in an acceptable amount of time, this may be used in a biometric database together with an Identity-Based model. An advanced strategy of well-known encryption methods such as AES, Genetic Algorithm, and RSA algorithm [20] to encode it and protect the information from hackers or intruders were employed, making it very challenging and time-consuming to decrypt the image without utilizing the key. According to experimental findings, the model produces random cipher images with high MSE, AD, MD, and PSNR values, making it challenging to decipher the original picture without the key.

**PROPOSED ARCHITECTURE**



*Figure 1: Proposed Architecture*

The original image is taken from the user and is passed through the proposed selective encryption algorithm. The sensitive region is identified and sent for further encryption, leaving the rest of the image untouched. For the encryption process, the hash value is generated for the user-provided key using the pbkdf2 algorithm. A chain of pixels is generated from the sensitive region based on this hash value and a nonlinear CBC operation is performed on the pixels. This is followed up by a modified RSA encryption using a computer-generated public and private key, where each pixel value obtained from the previous step is mapped to a unique value based on the hash array, and RSA is performed on this unique value. Since the RSA values could be greater than 255, they are again mapped back to values between 0 to 255 by storing the RSA values in an array, shuffling them, and taking their index in the array as their pixel value. Scrambling is performed on the resultant image to change the locality of the pixels. The encrypted image is stored in the location of the sensitive region. For the decryption process, the same steps are performed in reverse order to obtain the original image.

**Architectural Diagram**



*Figure 2: Architecture Diagram*

**PROPOSED METHODOLOGY**

A method that identifies and separates the sensitive region in a digital image into a bounded box and subsequently performs the encryption method based on the CBC-RSA algorithm is proposed. The steps of the method are elaborated below.

**1. Identification of sensitive region:**

This is the preliminary step that takes place before encryption. The sensitive regions of the image are identified by the use of computer vision models and are provided for the encryption process. The four corners of the bounded box around the sensitive region are stored in a file and are later used during the decryption process.

**2. Encryption of the image:**

1. User provided key:

A key is obtained from the user and passed through a key extension hash function (PBKDF2) to enhance the security of the respective key. Each character is extracted from the resulting hash value and stored in a temporary array. To further improve the uniqueness of the key value, five consecutive temporary array values are added to obtain the final key value that is stored in an array called the key array. The resultant key array obtained from this step is utilized in the consequent steps of the encryption process.



*Figure 3: Hash Function*

1. Perform nonlinear CBC on the sensitive region:

A nonlinear CBC algorithm is proposed, where the chain of pixels is chosen based on the key array. All the pixels are stored in an array and each pixel is added to the CBC chain based on the traversed key value. Once a pixel is added to the chain, it is removed from the array to avoid duplication. This process continues until the number of pixels in the array reaches zero. Once this process is completed, a chain of pixels is obtained that is unique to the key provided by the user. The first pixel in the chain is XORed with the first element of the key array. Subsequently, the encrypted value of each pixel in the chain is obtained by XORing the encrypted value of the previous pixel as well as the key value. CBC ensures that pixels with similar values do not have the same encrypted value by XORing with the previous pixel. By creating a chain of pixels based on the key value, the encryption takes place in a nonlinear fashion which further increases the security.



*Figure 4: Non-linear CBC*

1. Optimized RSA Encryption:

A modified RSA encryption is proposed after performing the nonlinear CBC to add multiple layers of security to the encryption algorithm. The RSA algorithm provides encryption based on a private and public key generated by the system using pseudo-random prime numbers. Since the pixel values range from 0 to 255, the RSA values are precomputed to ensure quick encryption. If RSA is performed directly on the pixel values, 0 and 1 give the same RSA encrypted value, thus it becomes a vulnerability. To improve upon this, first, a mapping of each pixel value to a unique number based on the user-provided key is performed. RSA is performed on this mapped number for each pixel value to ensure maximum security. After the RSA values are computed, since the RSA values will be greater than the 255 value that can be accommodated in the image, the RSA value has to be mapped to a number between 0 to 255. This final mapping will be completely random and to ensure this randomness the computed RSA values are stored in an array and shuffled randomly. Based on the position of the RSA value in the array the respective pixel value is mapped. The RSA array will be stored to be used in the decryption process. The RSA mapping process is maintained as a table for easy encryption. The RSA table has four columns such as the original pixel value, the pixel mapped unique value, the RSA value of the mapped pixel, and lastly the RSA mapped pixel value so that the encrypted value can be depicted as a pixel in the image. The pixel values obtained after performing CBC are compared with the RSA table and the respective RSA encrypted value of the pixel is stored in its location.



*Figure 5: Optimised RSA*

1. Scrambling:

With the completion of the RSA encryption, the diffusion process of encryption is complete. Next, the position of the pixels has to be changed by performing scrambling. In the proposed method, the row and column rotation on pixels is performed on the key array. Initially, the row rotation on each row has been performed. The direction of the rotation is based on the key array element mod 2 value, if it is 1, the row is rotated right, else rotated left. The number of rotations depends on the key value. Similarly, column rotation is performed, where the direction of rotation is determined by the array element mod 2 value, and the number of rotations is based on the key value. After performing row and column rotation sequentially two times, a perfectly scrambled image is obtained. Thus, the scrambling is unique to each key and is a simple yet very powerful step that makes the algorithm more secure. With this step, the encryption process is completed.

**3. Replacing the Encrypted image in place of the sensitive region:**

After the encryption process is complete, the encrypted image must replace the pixels of the sensitive region in the original image. Thus, a novel method has been proposed that implements a selective region multi-key encryption and decryption algorithm by hybridizing and optimizing the CBC and RSA algorithms. The micro-level integration of the CBC and RSA algorithms ensures that the original image cannot be decrypted even if one of the keys (RSA or user-provided key) is not provided. CBC (symmetric encryption technique) synergizes perfectly with RSA (an asymmetric algorithm) to provide a two-layer security mechanism that further enhances the robustness of the encryption algorithm. Thus by the end of the process, only the sensitive parts (i.e. face) of the image are encrypted while the surroundings are still visible to everyone.

**ALGORITHM**

1. Encryption



*Figure 6: Encryption Algorithm*

1. Decryption



*Figure 7: Decryption Algorithm*

**RESULTS**

1. Original images:

|  |  |  |
| --- | --- | --- |
| *(i)* | *(ii)* | *(iii)* |

*Figure 8: Original Images: (i) 4.1.01, (ii) 4.2.05 and (iii) 4.2.06*

1. RSA encrypted images:

|  |  |  |
| --- | --- | --- |
| *(i)* | *(ii)* | *(iii)* |

*Figure 9: Results of full encryption using RSA: (i) 4.1.01, (ii) 4.2.05 and (iii) 4.2.06*

1. Proposed method’s encrypted images:

|  |  |  |
| --- | --- | --- |
| *(i)* | *(ii)* | *(iii)* |

*Figure 10: Results of full encryption using proposed method:(i) 4.1.01, (ii) 4.2.05 and (iii) 4.2.06*

**EVALUATION**

1. Time:

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| |  |  |  | | --- | --- | --- | | **RSA** | **Proposed** | **CBC** | | 2.4499 s | 1.6246 s | 0.4219 s | | 2.6087 s | 1.6495 s | 0.4259 s | | 2.4787 s | 1.5888 s | 0.4391 s | | 2.5271 s | 1.6022 s | 0.4296 s | | 2.485 s | 1.6222 s | 0.42 s | | 2.6046 s | 1.6245 s | 0.45 s |   *Table 1: Encryption and Decryption Time* | *Fig 11: Encryption and Decryption Time* |

The proposed algorithm performs encryption and decryption, on average 40% faster than the existing RSA algorithm. This can be attributed to the RSA mapping function proposed in the paper. The mapping function reduces repeated calculation of the RSA values of the pixels thereby saving time. This improvement is achieved without sacrificing the security provided by the RSA algorithm. CBC algorithm does encrypt and decrypt at a faster rate, but the proposed algorithm adds an extra layer of security and hence takes slightly more time.

1. NPCR and UACI:

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| |  |  |  | | --- | --- | --- | | **CBC NPCR** | **Proposed NPCR** | **RSA NPCR** | | 99.629720 | 99.618021 | 96.005757 | | 99.613952 | 99.598185 | 99.993896 | | 99.619547 | 99.614969 | 99.036153 | | 99.617513 | 99.608866 | 97.323608 | | 99.610392 | 99.604288 | 99.992370 | | 99.625651 | 99.600728 | 99.962870 |   *Table 2: NPCR Comparison*    *Figure 12: NPCR comparison* | |  |  |  | | --- | --- | --- | | **CBC UACI** | **Proposed UACI** | **RSA UACI** | | 31.448304 | 31.016390 | 25.396830 | | 21.081692 | 18.608272 | 14.246072 | | 22.503745 | 22.715771 | 22.347801 | | 23.804764 | 23.851862 | 20.878505 | | 28.053546 | 27.798366 | 26.704263 | | 26.582288 | 26.667354 | 27.328784 |   *Table 2: UACI Comparison*    *Figure 13: UACI Comparison* |

The proposed algorithm has NPCR and UACI values comparable to the CBC algorithm. RSA on the other hand is very volatile and its NPCR and UACI values fluctuate rapidly. RSA encryption depends on the private, public key pair generated by the computer at the time of encryption. The encrypted pixel values depend on these private and public key pairs. Every pair provides unique encryption and hence the NPCR and UACI values vary accordingly. An image encrypted with two different pairs of RSA keys provides widely different encrypted values and hence a huge variation in the NPCR and UACI values. The proposed algorithm overcomes this fluctuation caused by the RSA algorithm and stabilizes it by combining it with the CBC algorithm which is shown to have a more consistent NPCR and UACI value.

1. Correlation:

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| |  |  |  | | --- | --- | --- | | **Proposed Correlation** | **RSA Correlation** | **CBC Correlation** | | 0.009624 | 0.121260 | 0.013541 | | 0.012254 | 0.102741 | 0.013198 | | 0.007523 | 0.166735 | 0.014707 | | 0.013220 | 0.178086 | 0.010011 | | 0.011934 | 0.151025 | 0.010267 | | 0.008524 | 0.065062 | 0.014626 |   *Table 5: Correlation* | *Figure 14: Encrypted Correlation* |

The correlation of pixels in the images encrypted is 90% lesser than the average correlation obtained while using the RSA algorithm. This lower correlation is due to the improvements suggested in the proposed algorithm over the existing algorithms. The non-linear nature of the proposed CBC algorithm coupled with the proposed RSA mapping technique reduces the correlation of the pixels thereby making the encrypted image unrecognizable to the human eye. The proposed algorithm successfully incorporates the two algorithms to provide an even lower correlation than either of the existing algorithms.

1. Histogram:

The below images visualize the values of pixels in an image, the more uniform the distribution the more secure the algorithm. The RSA algorithm has a sparse distribution, spiking at a few pixel values with more intensity. As encrypted pixel values are concentrated at certain values, it makes the RSA algorithm more vulnerable to attacks. CBC on the other hand has a uniform distribution of pixel values from 0 to 256. The proposed algorithm improves on the existing RSA algorithm and produces a uniform pixel distribution increasing the overall security of the algorithm.

|  |  |  |
| --- | --- | --- |
| *(i)* | *(ii)* | *(iii)* |

*Figure 15: Histogram analysis:(i) RSA Enc, (ii) Proposed Enc. and (iii) CBC Enc.*

**CONCLUSION**

In this paper, a hybrid algorithm that identifies and encrypts only the sensitive regions of an image is proposed. It improves upon the existing RSA algorithm by incorporating a modified CBC algorithm, producing a 40% improvement in encryption/decryption time, as well as a 90% decrease in the correlation of the encrypted image with respect to the RSA algorithm. By selectively encrypting the sensitive parts of the image redundant operations are avoided, saving time and space. Thus, the proposed method is more secure in comparison with the existing RSA algorithm and is more efficient than encrypting the entire image. The paper focused primarily on identifying the faces and encrypting them, but the concept can be adapted for other applications, such as encrypting signatures of documents, number plates of cars, and other such sensitive parts of an image.

**REFERENCES**

[1] Janwg, W., & Lee, S. Y. (2020). Partial image encryption using format-preserving encryption in image processing systems for the Internet of things environment. International Journal of Distributed Sensor Networks, 16(3), 1550147720914779.

[2] Çavuşoğlu, Ü., Kaçar, S., Zengin, A., & Pehlivan, I. (2018). A novel hybrid encryption algorithm based on chaos and S-AES algorithm. Nonlinear Dynamics, 92(4), 1745-1759.

[3] Zhang, X., Wang, L., Niu, Y., Cui, G., & Geng, S. (2019). Image Encryption Algorithm Based on the H-Fractal and Dynamic Self-Invertible Matrix. Computational intelligence and neuroscience, 2019.

[4] Jiao, K., Ye, G., Dong, Y., Huang, X., & He, J. (2020). Image encryption scheme based on a generalized arnold map and RSA algorithm. Security and Communication Networks, 2020.

[5] Patel, S., & Muthu, R. K. (2020). Image encryption decryption using chaotic logistic mapping and dna encoding. arXiv preprint arXiv:2003.06616.

[6] Jassem, A. H., Hashim, A. T., & Ali, S. A. (2019, December). Enhanced Blowfish algorithm for image encryption based on chaotic map. In 2019 First International Conference of Computer and Applied Sciences (CAS) (pp. 232-237). IEEE.

[7] Arab, A., Rostami, M. J., & Ghavami, B. (2019). An image encryption method based on chaos system and AES algorithm. The Journal of Supercomputing, 75(10), 6663-6682.

[8] Sheela, S. J., Suresh, K. V., & Tandur, D. (2018). Image encryption based on modified Henon map using hybrid chaotic shift transform. Multimedia Tools and Applications, 77(19), 25223-25251.

[9] Mohammad, O. F., Rahim, M. S. M., Zeebaree, S. R. M., & Ahmed, F. Y. (2017). A survey and analysis of the image encryption methods. International Journal of Applied Engineering Research, 12(23), 13265-13280.

[10] Xu, C., Sun, J., & Wang, C. (2020). An image encryption algorithm based on random walk and hyperchaotic systems. International Journal of Bifurcation and Chaos, 30(04), 2050060.

[11] Hua, Z., Zhou, Y., & Huang, H. (2019). Cosine-transform-based chaotic system for image encryption. Information Sciences, 480, 403-419.

[12] Alsaffar, D. M., Almutiri, A. S., Alqahtani, B., Alamri, R. M., Alqahtani, H. F., Alqahtani, N. N., & Ali, A. A. (2020, March). Image Encryption Based on AES and RSA Algorithms. In 2020 3rd International Conference on Computer Applications & Information Security (ICCAIS) (pp. 1-5). IEEE.

[13] Naik, R., Lathi, A., Pariani, S., Satpute, N., & Singh, A. (2021). Comparison of Different Encryption Algorithm and Proposing an Encryption Algorithm. Available at SSRN 3867982.

[14] Ray, A., Potnis, A., Dwivedy, P., Soofi, S., & Bhade, U. (2017, October). Comparative study of AES, RSA, genetic, affine transform with XOR operation, and watermarking for image encryption. In 2017 International Conference on Recent Innovations in Signal processing and Embedded Systems (RISE) (pp. 274-278). IEEE.

[15] Srivatsava, J. G. M., & Sheeja, M. R. (2020). Implementation of Triple DES ALGORITHM in Data Hiding and Image Encryption Techniques.

[16] Mohammad, O. F., Rahim, M. S. M., Zeebaree, S. R. M., & Ahmed, F. Y. (2017). A survey and analysis of the image encryption methods. International Journal of Applied Engineering Research, 12(23), 13265-13280.

[17] Hazra, T. K., Mahato, A., Mandal, A., & Chakraborty, A. K. (2017, August). A hybrid cryptosystem of image and text files using blowfish and Diffie-Hellman techniques. In 2017 8th Annual Industrial Automation and Electromechanical Engineering Conference (IEMECON) (pp. 137-141). IEEE.

[18] Han, C. (2019). An image encryption algorithm based on modified logistic chaotic map. Optik, 181, 779-785.

[19] Rodríguez César, H., Gayoso Martínez, V., Hernández Encinas, L., & Martín Muñoz, A. (2019). Format-Preserving Encryption: Image Encryption Under FF1 Scheme.

[20] Ray, A., Potnis, A., Dwivedy, P., & Soofi, S. An Advance Approach of Image Encryption using AES, Genetic Algorithm and RSA Algorithm.