Review of Image Security approaches: Concepts, Issues, Challenges and Applications

Shashikant S. Radke
Research Scholar,
Department of Computer Engineering,
MPSTME, Mumbai, NMIMS University,
s.s.radke@gmail.com

Dhirendra S. Mishra
Professor,
Department of Computer Engineering,
MPSTME, Mumbai, NMIMS University,
dhirendra.mishra@nmims.edu

Abstract - Currently digital images are widely used in different applications to represent distinguishable contents. Also, diagnosing diseases using medical images became vital and crucial and if the data in these images are liable for unauthorized usage, this may lead to severe problems. The security of these data has become an urgent and serious problem and needs immediate attention. Traditional encryption and decryption algorithms are not sufficient to secure digital images. Especially, image encryption and decryption algorithms are needed. Securing image data with effective encryption approaches can be more useful for applications. This article aims to comparatively study the different digital image encryption algorithms. In the current Pandemic scenario of COVID-19, the variety of research work can be communicated through the encrypted images among researchers to avoid the leakage of information. These image encryption algorithms are having applications to secure image data and stored and share them in the network environments.

Keywords: Image encryption, medical images, security,

[I] Introduction

A digital image is an image composed of picture elements, also known as pixels, each with finite, discrete quantities of numeric representation for its intensity or gray level that is an output from its two-dimensional functions fed as input by its spatial coordinates denoted with x, y on the x-axis and y-axis, respectively. Depending on whether the image resolution is fixed, it may be of vector or raster type. By itself, the term "digital image" usually refers to raster images or bitmapped images (as opposed to vector images). [22]

The digital images are widely used in different applications to represent distinguishable contents. In the healthcare field, major disease diagnosis using medical images become practically convenient. If the data in these images are liable for unauthorized usage, this may lead to severe problems. The unauthorized access may tamper the image and add false information. The false information means possibly false diagnosis that may lead to the death of the patient. The security of these data has become a challenge and needs immediate attention. Also, the image encryption techniques are different from the data encryption techniques. Traditional encryption and decryption algorithms are not sufficient to secure digital images as they contain more redundant and highly correlated information. Therefore, these particular security problems have attracted many researchers to work and contributed in solving these problems. Many researchers have identified issues and challenges. They have proposed, experimented, analyzed and published results and solutions for the researchers' academics, industries and society for future use.

Robust algorithms need to be developed in order to design the secured computational system considering all of its vulnerabilities. Security has many distinct aspects. The smallest defect in the design and processes affects the whole system security.

There are different approaches to image security. Image encryption is one of the techniques to secure an image by converting the original image into another image called an encrypted/cipher image, which is difficult to identify and understand from the original image by the unauthorized users. Only the owner, authorized and intended user will be able to get back original image from encrypted image. There are many image encryption algorithms by worldwide researchers' invented and made available to use. These algorithms can be grouped into three broad categories: transposition (position-permutation) based algorithms, value-substitution (transformation) based algorithms, and position-substitution based algorithms. [21]

a. ***Transposition (position-permutation) based algorithm.*** Transposition means rearranging elements of the plain image. This rearrangement of elements shall be done by bit-level, pixel-pixel, and/or block wise. The permutation of bits decreases the perceptual information, whereas the permutation of pixels and blocks produce higher level security. In the bit permutation technique, the bits in each pixel are permuted using the permutation keys with the key length equal to 8. In the pixel permutation, 8 pixels are taken as a group and permuted with the same size key. In this investigation the combination of block, bit, and pixel permutation are used respectively. [21]
b. ***Value-substitution (transformation) based algorithm.*** Values substitution based algorithm is the technique which changes each pixel value to some other value. The new value of the pixel is computed by applying some complex computation algorithm on the pixel. Value-transformation based algorithms are Digital Signatures and Lossless Image Compression and Encryption Using SCAN, Image Cryptosystems, Color Image Encryption Using Double Random Phase Encoding, Image Encryption Using Block-Based Transformation Algorithm etc. [21]
c. ***Position-substitution based algorithm.*** This

technique is a combination of both position permutation and value transformation. In this technique first pixels are reordered and then a key generator is used to substitute the pixel values. [21]

The combination of cryptography, signal and image processing is an interesting research field. Image encryption is defined as a combination of image processing and cryptography. Image encryption techniques are used to enforce content access control, identity verification and authentication, and privacy protection.

Chaos based image encryption and decryption algorithms have become increasingly popular these days and most of these algorithms are often based on cryptanalysis driven design techniques. Therefore, the security of these algorithms is doubtful and the threat of attack continues. This problem has drawn the attention of researchers [2]. Authors have designed an approach for the transformation of a computationally difficult problem into a cryptographic protocol.

In the real world, the processes and systems actually have order and symmetry. The rich dynamics of chaotic systems makes chaos theory a crucial topic to understand these order and symmetrical behavior. A notable application of these systems is statistical randomness. Especially in random number generators designed based on the discrete time chaotic systems, an important design parameter affecting the success of the generator with statistical randomness properties is the initial conditions of chaotic maps. Obtaining different initial conditions that will meet the statistical requirements is important in terms of generating different random number sequences.[3]

The design problem in chaos-based random number generators is that there are an infinite number of possibilities to select initial conditions. This design problem is inherently an NP problem. Optimization algorithms can be used to find an approximate solution to this problem. Optimization algorithms have several computational difficulties. The problem is determining the most suitable initial conditions of chaotic systems that will provide statistical randomness in the best way. In order to determine the initial conditions, an algorithm that updates the initial conditions depending on the number of successful statistical tests is to be design. In article [3], a method that attempts to solve the success achieved with optimization algorithms using a simpler method is designed, discussed, experimented and analyzed.

This article is the comparative study of image encryption algorithms from those three categories. The rest of the article is organized as follows. In Section II, the existing recent image encryption algorithms with respect to concepts, issues, challenges and applications are discussed. In Section III, different ways to analyze security performances of the algorithm have been evaluated. The obtained conclusions are discussed in the last section IV.

[II] Discussion

General block diagram for securing the digital image data is shown in Figure 1 given below.

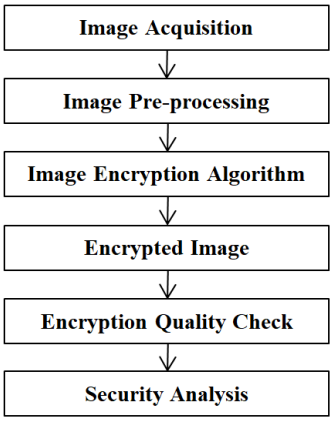

Figure 1. General block diagram of the image encryption.

a. Image Acquisition. Image is the input to the image encryption algorithm that will be converted into the encrypted output which is not correlated with input plain image. To deal with images and before analyzing them the image acquisition is very important and majorly the first step of any digital image processing systems. Image Acquisition is achieved by suitable image sensor(s). After the image has been captured, various processing can be applied to the image to make it suitable for the operations of the required application.

b. Image pre-processing. If the image has not been acquired satisfactorily then the intended operations may not be achievable, even with the aid of some form of image enhancement. Also, pre-processing can be performed to improve the image data that suppresses undesired distortions or enhances some image features relevant for further processing and analysis. The possible image pre-processing operations are illumination corrections, blur and focus corrections, filtering and noise removal, thresholding, edge enhancements, morphology, segmentation, region processing and filters, point processing, math and statistical processing, color space conversions, etc.

c. Image Encryption Algorithm. The algorithm has input a plain digital image and should output an encrypted image with close to zero correlation with input image. This stage is the step-by-step solution for the problem identified and formulated through research gaps by the researcher. We will discuss algorithms by different researchers with respect to concepts, advantages, issues, challenges and applications.

The algorithm [1] is a combination of unpredictable and random-like features of chaotic systems and cryptographic primitives. It is more resistant to application attacks than mathematical designs and thus, used successfully in many applications related to security of digital images.

In paper [4], an image encryption algorithm having higher security based on 2D-CIMM chaotic map uses the hash values of the original image to update its initial value in real time. And, the permutation and diffusion of the encryption process are all performed in bit-level to enhance the algorithm security. This algorithm has the correlation coefficient between adjacent pixels close to zero, and has random and uniform statistical characteristics in the encrypted image, and the algorithm has good ability to resist differential attacks and known/chosen plaintext attacks.

Sura F. Yousif, Ali J. Abboud, and Hussein Y. Radhi [5] have introduced an image security approach to secure digital images by utilizing a scan mechanism, the El-Gamal asymmetric key cryptosystem and chaotic systems. The Lorenz chaotic system is adopted for the resulting permutated images to confuse the relation between the grey image pixels by changing their locations, whereas the Rössler chaotic system is applied to the obtained confused images to diffuse the image pixels through varying their values to achieve a second layer of encryption. This approach can effectively resist statistical, differential, and exhaustive attacks and it has potent immunity to most widespread attacks.

An image encryption scheme [19] based on chaotic standard map and bit level permutation not only changes the locations of the image pixels, but also modifies their values to enhance the randomness. The bit level permutation features provide a bit level confusion and dependent diffusion to enhance the security of cryptosystem.

The article [6] gives an image encryption and decryption algorithm based on bit-level permutation and dynamic overlap diffusion. Firstly, the plain image is scrambled in the bit-level, changing the pixel position of the image while changing the pixel value using controlled Arnold transform and get the permutation image. Then, according to the encryption security requirements, dynamic overlap diffusion is performed on the permutation image. At the same time, the plaintext information entropy and variance are used to update the diffusion key in the five dimensional hyper-chaotic systems to achieve the plaintext correlation of the encryption key. Arnold transforms and dynamic overlap diffusion are used to ensure that the different key streams are generated when encrypting different images. Hence, the attacker cannot crack this algorithm via known-plaintext and chosen-plaintext attacks.

In research work [7], a one-dimensional chaotic system (1DSCS) having good chaotic characteristics and large parameters space is introduced and based on the same an image encryption scheme is discussed and tested. This 1DSCS is used to generate chaotic sequence. Based on 1DSCS, a hybrid scrambling method and a dynamic diffusion method are applied to encrypt image. This algorithm has a good encryption effect and can resist common attacks.

An image encryption scheme shall be vulnerable to a variety of cryptanalysis attacks like chosen-plaintext attacks, chosen-cipher-text attacks, etc. The article [8] presented an efficient algorithm for constructing secure dynamic S-boxes derived from Henon map. The dynamic S-box is applied to construct an image encryption scheme that includes a combination of security features to resist chosen-plaintext and chosen-cipher-text attacks. Also, the encryption keys are protected against cryptanalysis using elliptic curve cryptography (ECC). Therefore, the recovery of secret keys is as hard as the elliptic curve discrete logarithm problem even in the unlikely case of the recovery of the temporary S-box or key-stream.

An adaptive color image encryption algorithm [9] based on one-dimensional hybrid chaotic mapping and cross-diffusion is discussed. The first uses the one-dimensional chaotic map to generate the key stream. The secondly, applies an adaptive strategy to select the key stream such that the generated scrambling sequence is associated with the image data content. Finally, the three components of R, G and B are cross-diffused by adaptively selecting different encryption methods, and the pixel gray values are modified to destroy the strong correlation between adjacent pixels. By applying an adaptive strategy in the scrambling and spreading phase to associate the key stream with the image data, the encryption algorithm is robust against known/selected plaintext attacks.

The article [10] have proposed an image encryption algorithm using dynamic spiral scrambling algorithm in combination with the random pixel value filling operation and Deoxyribonucleic Acid (DNA) operation. The dynamic spiral scrambling algorithm dynamically combines the chaotic sequences with the plaintext image, and scrambles the pixel values of the plaintext image. This operation makes the scrambling algorithm not fixed, and position changes are highly sensitive to the chaotic sequences, any slight change will give a completely different result. Then, the result combines with Deoxyribonucleic Acid (DNA) coding and manipulates to further confuse pixel values. This algorithm has good encryption effects and can resist common attacks such as select plaintext attacks, cropping, and noise attacks.

The paper [11], have introduced a fractional order two dimensional (2D) map with very complex chaotic behavior and distinct large positive values of Lyapunov exponents over wide range of parameters, compared with other 2D maps from literature. And, a new reliable secure, image encryption scheme combining the associated chaotic pseudo-orbits of the fractional order 2D map with the advantages of elliptic curves in public key cryptography is suggested and applied to color images. This hybrid scheme is capable to confirm reliable secret keys exchange in addition to highly obscure and hide transmitted information messages.

The paper [12] proposed a color image encryption algorithm based on a double-chaos system and DNA computation at the bit level. This algorithm has used the Arnold algorithm to scramble the three color components of the plaintext image, and the number of iterations is determined by the pixel average of each component, which improved the scrambling effect of Arnold algorithm. Then, using the improved double-chaos system composed of Lorenz chaotic mapping with variable parameters and fourth-order Rossler hyper-chaotic mapping, three sets of chaotic sequences were generated for the diffusion operation of three sets of scrambled components. Then, DNA coding and DNA computing is used to diffuse the three groups of images and finally merged the three groups of cipher-text components to obtain the final cipher-text image.

Feifei Yang, Jun Mou, Yinghong Cao and Ran Chu [13] have proposed a color image compression encryption algorithm based on BP neural network and fractional-order hyper-chaotic system. The dynamical characteristic of

fractional-order hyper-chaotic system shows large parameters range and good randomness. Therefore, fractional-order system is more suitable for image encryption algorithm. The use of BP neural network can compress the image effectively. So, this image compression and encryption algorithm is an effective for the safe transmission of image information in practical communication applications.

Based on compressive sensing and fractional-order simplest memristive chaotic system, the paper [14] has described an image compression and encryption scheme. Firstly, a fractional-order simplest memristive chaotic circuit system is designed and analyzed to determine the parameters and pseudo-random sequences used in the encryption scheme. Secondly, an encryption scheme based on compressive sensing is designed to compress the image twice to fully reduce the storage cost, and scrambles the pixel matrix twice through block scrambling and zigzag transformation, and then uses chaotic pseudo-random sequence and GF (17) domain diffusion image matrix to obtain the final cipher image.

The algorithm proposed in the paper [15] encrypts the image based on chaotic sequences and cross-diffusion of bits. The pseudo-random sequences generated by the 2D-LSCM system scrambles the position pixels of image, and the pseudo-random sequence generated by the logistic system diffuses the pixels of image. In the encryption scheme, the scrambling and cross-diffusion is effectively enhancing resistance to differential attack, exhaustive attacks, and statistical analysis. This scheme shall be used to protect image information.

A method based on a new designed S-Box based DNA-like techniques and CFI; and combined with hyper-chaotic maps, is suggested in [17] article. In this method, some considerations were taken to ensure resistance against attacks. The first one was to uses CFI to develop four random sequences. To create the initial input, a secret image key and a finite length key were used. The second consideration was basing the four different FZ S-boxes on CFI. The third consideration was using a DNA-inspired technique and applying it through a control code to select four of the eight DNA rules, one per each FZ S-box. The fourth one was extracting four sub-images from the plain image, through down-sampling. The fifth one was changing the values of the sub-images with values of the four DNAFZ S-boxes. The sixth consideration was diffusing each of the DNAFZ sub-images using a random DNA sequence extracted from Chen's hyper-chaotic map. The final consideration was combining the four DNAFZ/chaotic sub-images, to form the cipher image. This algorithm is effective and secure through tests and security analyses.

The paper [18] presents an encryption algorithm having image splitting technique based on image blocks, the image blocks scrambled using a zigzag pattern, rotation, and random permutation and then, a chaotic logistic map generates a key to diffuse the scrambled image. This algorithm is effective for encrypting both grey and color medical images.

d. Encrypted Image. It is the output of the image encryption algorithm. Any digital image has more data, redundant data and strongly correlated data. The algorithm should disturb the correlation between the pixel, so that there should not be any visible as well as computation resemblance between original image and encrypted image.

e. Encryption Quality Check. Visual check is not sufficient on deciding the quality of encrypted images. Many metrics are used to evaluate the quality of the encrypted image which is output of image encryption algorithms. Some of these metrics includes the histogram analysis, the correlation coefficient analysis, the information entropy analysis, the number of pixel change rate (NPCR) and unified average change intensity (UACI) etc. of the encrypted image. Image histogram depicts how pixels are distributed in an image. The flat histogram level is similar to a noise-image. The algorithm should output encrypted image with more flat and fairly uniform histogram. The correlation coefficient is calculated between adjacent pixels of encrypted image and should be as low as possible (close to zero). Information entropy of an encrypted image is a criterion used to illustrate the randomness of the image pixels and it should be close to 8 bits per pixel. A greater value of information entropy shows a more uniform/random distribution of image pixels. NPCR can also be defined as variance rate of pixels in the encrypted image caused by the change of a single pixel in the original image. For better algorithm NPCR value should be high. UACI determines the average intensity of differences between the two images. For good quality UACI value should be high.

f. Security Analysis. Now, it is very important to see whether the encrypted image is secured, securing and not revealing any information of the original image. The encrypted image should not have any visible as well as computation resemblance with the original image. Also, perform the checks for the possible attacks on encrypted images like differential, cipher-text only, known plain-text, chosen plain-text and chosen cipher-text attacks etc. These attacks should not reveal any information of original image. We will discuss the different analysis approaches in further session of this article.

Figure 2 depicts that the encryption algorithm should be invertible to get back the original image from the encrypted image.

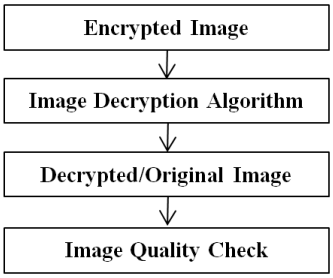

Figure 2. General block diagram of the image decryption.

a. Image Decryption Algorithm. An encrypted image produced by image encryption algorithm is the input to the respective image decryption algorithm. This algorithm should be the conjugate algorithm to respective image encryption algorithm to convert an encrypted image to its

original image with allowable error or loss of data if any.

b. Decrypted Image. This is an original image and the output of an image decryption algorithm applied on encrypted image. This image must match with the original image with permissible error or loss of data if any.

c. Image Quality Check. Decrypted image quality needs to be check to assure presence of original data and no tampering of data. To check quality of decrypted image many analysis techniques are used and some of the common techniques are number of pixel change rate (NPCR), unified average change intensity (UACI) and peak signal to noise ratio (PSNR) etc.

- ***NPCR*** [1,4-15,17-19]: For better decryption algorithm NPCR value should be low.
- ***UACI*** [1,4-15,17-19]: For good decrypted image quality UACI value should be low.
- ***PSNR*** [5,6,10,13,14,17,18]: The larger the PSNR value, the more similar the decrypted image is to the original image.

(2) Issues

Digital images are one of the most important types of information media used effectively in digital environments. It is known that traditional and classical encryption algorithms are insufficient to provide information security due to their obvious features.

To achieve image security goals, the robust primitives of modern cryptology are combined with the unique features of the chaos theory, DNA encoding, S-box, Quantum computing etc.

There are many issues in image security algorithms, approaches, methods and techniques. These issues needs careful studies and have to handle with great care. Therefore, researchers are attracted in doing research on alternative solution, suggestions and proposals. These issues are listed below.

- High correlation between pixel values
- More data redundancy
- Modify the pixel gray value to destroy the strong correlation between adjacent pixels.
- Distribution of pixel values to have a uniform distribution.
- Statistical tests alone will not be sufficient to analyze image security
- Obtaining different initial conditions that will meet the statistical requirements to create secret key
- Most of the algorithms are often based on cryptanalysis driven design technique
- Image encryption schemes can be vulnerable to a variety of cryptanalysis attacks.
- The random pixel value filling operation is to generate some random values and fill them around the plain image. These values can influence all the pixels after the confusion and diffusion operations.
- Rapidly changing networked/internet environments
- Images are transmitted through the network; they need a high level of protection. If the data in these images are liable for unauthorized usage, this may lead to severe problems.
- To evaluate security & performance, key space analysis, key sensitivity analysis, correlation coefficient, histogram, information entropy, NPCR, UACI,

The issues mentioned above will be analyzed and discussed as follows.

1. Key Space [1,4-8,10-15,18,19]: Key space is the total number of different keys. The key space of a good image encryption algorithm should be at least 2^{100} to resist brute-force attacks.
2. Key Sensitivity [4-12,14,15,17-19]: A cryptographic system should be sensitive to all secret keys. The proposed encryption algorithm shall be sensitive to a small change in the secret keys.
3. Histogram analysis [1,4-12,14,15,17-19]: Information obtained from histogram is enormous. Encrypted image must have a uniform histogram distribution.
4. Correlation Coefficients [1,4-15,17-19]: For a plain image, each pixel is highly correlated with its neighbor and adjacent pixels either in horizontal, vertical or diagonal direction. However, an efficient image cryptosystem should produce the cipher image with sufficiently low correlation (close to zero) in the adjacent pixels.
5. Information Entropy [1,4-12,14,15,17-19]: Entropy of a source gives idea about self-information. Information entropy is the main feature of uncertainty. In case if entropy is less than 8 bits, then there exists a certain degree of predictability. For a cryptosystem to resist the entropy attacks, the entropy of the cryptosystem should be close to ideal value 8.
6. Diffusion Characteristic: A good cryptosystem must ensure a good diffusion, that is, if one bit of the plaintext is changed, then the cipher text should change completely, in an unpredictable manner.
   a. Number of Pixel Change Rate (NPCR) [1,4-15,17-19]: NPCR can also be defined as variance rate of pixels in the encrypted image caused by the change of a single pixel in the original image. For better algorithm NPCR value should be high.
   b. Unified Average Change Intensity (UACI) [1,4-15,17-19]: Unified Average Change Intensity (UACI) determines the average intensity of differences between the two images. For good quality UACI value should be high.
7. Differential Attack [1,4-15,17-19]: The differential attack depends on guessing information about an image by making a slight change in the plain image and encrypting both images using the same algorithm. We compare both images to detect a correlation between the plain image and the encrypted image. Using a practical algorithm, any slight change in the plain image should produce a different encrypted image. Study algorithm's effectiveness in resisting differential attacks by recording the NPCR and UACI values. The ideal value of NPCR is 99.6094%, and of UACI is 33.4635%.
8. Encryption Efficiency: Peak signal to noise ratio (PSNR) [5,6,10,13,14,17,18] is used to measure the difference between the original image and the encrypted image. Also, the PSNR is usually used to assess the

performance of image reconstruction. The lower values of PSNR indicate a significant difference between the original and the encrypted image and larger the PSNR value, the more similar the image is to the original image.

9. Encryption Quality: Maximum Deviation [18] - The quality of encryption is evaluated by measuring the difference in pixel values between the plain and encrypted images. The encryption algorithm is considered to be efficient if this difference is significant. The high value indicates the significant difference between the plain and the encrypted image.
10. Time Complexity (or Time Analysis or Computational Complexity) [5,7,10,14,18]: Estimate the time complexity in each step of the encryption process to evaluate proposed algorithm's total time complexity.
11. Contrast Analysis [7,17]: Contrast has to do with the difference in the brightness of an object. To test contrast, a contrast analysis is performed enabling users to see objects and identify information beneath. Also, to improve viewing, as well as visual effects, an adjustment of the contrast and brightness is performed, while processing an image.
12. Energy Analysis [7]: In an energy analysis, a calculation of the sum of the squared members of gray-level co-occurrence is made. Energy value is high, when high value pixels are found in certain areas of the plain image in the gray-level co-occurrence matrix. The energy of the encrypted image, as opposed to the plain image, is small, as these values are distributed.
13. Homogeneity Analysis [7]: In the gray-level co-occurrence matrix (GLCM), the intimacy of element distribution in the diagonal direction is known as homogeneity and its value essentially depends on the components existing on the diagonal of such a matrix. It is well-known that the smaller the value of homogeneity, the stronger the encryption algorithm.
14. NIST Test Suite Analysis [3,6,10,17]: NIST test is executed to check the randomness of the binary sequence in cipher images. It is a statistical group consists of 15 tests. All the tests have to pass successfully. In order to resist statistical attacks, the pixels of an ideal cipher image need to be evenly distributed.
15. Chi-square Test Analysis [3,17]: Chi-square test analysis is performed to measure the quantitatively of uniformity the gray value of pixel. Smaller the value of Chi-square indicates the higher uniformity of gray-scale.
16. Classical Types of Attacks [17]: Following are well-known attacks are utilized by attackers to break any cryptosystem.
    a) Cipher-text only Attack: The contender has access to the string of cipher-text.
    b) Known Plain-text Attack: The contender has access to the strings of both plain and cipher-text.
    c) Chosen Cipher-text Attack: The contender can choose the cipher-text string and obtains the corresponding plaintext string.
    d) Chosen Plaintext Attack: The contender can choose the plaintext string and obtains the corresponding cipher-text string.
17. Robustness Test against Noise, Occlusion Attack [7,12,14,15,17]: Several types of attacks were used to test the proposed algorithm, including salt and pepper noise, occlusion attack. PSNR is measured in this article to analyze the quality of the decrypted image in comparison with the plain-image. The greater value of PSNR results in minimal distortion in the plain-image.
18. Mean Structural Similarity (MSSIM) [5,14]: The MSSIM is an indicator that measures the degree of similarity between two images from three levels: brightness, contrast, and structure. The range of MSSIM values is 0 - 1. The larger the MSSIM values, the more similar the two images are. Also, the value of MSSIM changes with the change of compression ratios (CRs), and the quality of the image reconstructed as well.
19. Resistance to Cropping Attacks and Noise Attacks [6,10]: In many image encryption systems, the cropping attack and the noise attack need to be tested to verify that the algorithm has robustness against cropping and noise attacks. Because the attacker cannot correctly decrypt the encrypted image during the information transmission process. In this case, the attacker usually uses the means of interfering communication to achieve the effect of preventing the recipient from decrypting, thereby achieving the purpose of the attack.

(3) Challenges

The issues discussed in the last section will address following challenges.

- The traditional and classical encryption algorithms are insufficient to provide information security due to their obvious features like large data, more data redundancy, high correlation between pixel values, etc. The special image encryption algorithms need to be designed.
- Most of the image encryption algorithms are often based on cryptanalysis driven design technique and can be vulnerable to a variety of cryptanalysis attacks.
- Online image transfer systems allows to build better and deeper image sharing network applications, which in turn mean increased volumes and a more open platform for collaboration. Ultimately, remote or cloud-based image storage and sharing platforms are the popular choice in the applications development. Images are transmitted through the network and rapidly changing networked environment demands a high level of security.
- Unauthorized Access to image Data: If the images with sensitive data are liable for unauthorized usage, this may lead to severe problems.
- Lack of Accountability: If the system/scheme/algorithm is unable to track users' activities, then users cannot be held responsible for their actions. There must be some reliable way to monitor who is performing what operations on the image.
- Image Data Tampering. Data cannot be modified or viewed in transit. Networked environments bring with them the possibility that a malicious third party can perpetrate a computer crime by tampering with data as

it moves between applications/users/sites.

- Image Intrusion and Data Theft. Image data must be stored and transmitted securely over the network environments, so that sensitive information cannot be stolen. Network sniffers can easily be installed to eavesdrop on network traffic and can be designed to find and steal particular and sensitive information.

(4) Applications

Image encryption has applications in various fields including [20]:

- Internet communication
- Multimedia systems
- Medical imaging
- Tele-medicine
- Military communication
- Content archiving
- temper detection
- protection of copyright
- Meta-data insertion and monitoring of broadcast

[IV] Comparisons of different image encryption algorithms

All the article authors' have done different security analysis on encrypted images. The common analysis performed includes key-space, key sensitivity, histogram, information entropy, correlation coefficient, peak signal-to-noise ratio (PSNR) and differential attacks (number of changing pixel rate (NPCR), unified averaged changed intensity (UACI)). All the articles analysis has close to standard values. Thus, all the articles have pass analysis as shown in the Table 1.

Table 1. Comparison of the recent image encryption algorithms studied.

Analysis	Standard Value	Articles (pass the test)
Key-space	Key size > 100 bits Key space > 2^{100}	[1,4,5,6,7,8,10,11,12,13,14,15,18,19]
Key Sensitivity	At-least 1 bit change in key and complete change in result	[4,5,6,7,8,9,10,11,12,14,15,17,18,19]
Histogram	Encrypted image must have a uniform histogram distribution.	[1,4,5,6,7,8,9,10,11,12,14,15,17,18,19]
Information Entropy	Close to ideal value 8	[1,4,5,6,7,8,9,10,11,12,14,15,17,18,19]
Correlation Coefficient	Close to zero	[1,4,5,6,7,8,9,10,11,12,13,14,15,17,18,19]
PSNR	Lower value	[5,6,10,13,14,17,18]
Differential Attacks	The ideal value of NPCR is 99.6094%, and of UACI is 33.4635%.	[1,4,5,6,7,8,9,10,11,12,13,14,15,17,18,19]

From the table, we have to note and make sure that the image encryption algorithm must pass the mentioned analysis test at-least. Then only we can say that algorithm can prevent various known attacks, and the algorithm security is high.

[V] Conclusion

In this paper, we have discussed general steps of image encryption and decryption. Also, we have studied the recent image encryption algorithms and approaches with concepts, issues, challenges and their applications. The study reveals that the image encryption techniques are very different from the data encryption techniques. The least analysis to be performed includes key-space, key sensitivity, histogram, information entropy, correlation coefficient, PSNR and differential attacks (NPCR, UACI) with close to standard values that ensure the image encryption algorithms can prevent various known attacks, and the algorithm security is high. The image encryption algorithms have applications in variety of fields such as internet communication, medical imaging, military communication, protection of copyright etc.

The studied technique has its own suitability, limitations and applications. But still, there are huge opportunities to design algorithms to protect images. A limitation of the image encryption algorithm is the high computation requirement. Designing a mathematical model having high resistance to the various possible attacks on encrypted image will help to protect the image data.

REFERENCES

[1] Z. M. Z. Muhammad and F. Özkaynak, "An Image Encryption Algorithm Based on Chaotic Selection of Robust Cryptographic Primitives," in *IEEE Access*, vol. 8, pp. 56581-56589, 2020, doi: 10.1109/ACCESS.2020.2982827.

[2] Z. M. Z. Muhammad and F. Özkaynak, "Security Problems of Chaotic Image Encryption Algorithms Based on Cryptanalysis Driven Design Technique," in *IEEE Access*, vol. 7, pp. 99945-99953, 2019, doi: 10.1109/ACCESS.2019.2930606.

[3] M. Ş. Açikkapi and F. Özkaynak, "A Method to Determine the Most Suitable Initial Conditions of Chaotic Map in Statistical Randomness Applications," in *IEEE Access*, vol. 9, pp. 1482-1494, 2021, doi: 10.1109/ACCESS.2020.3046470.

[4] C. Chen, K. Sun and Q. Xu, "A color image encryption algorithm based on 2D-CIMM chaotic map," in China Communications, vol. 17, no. 5, pp. 12-20, May 2020, doi: 10.23919/JCC.2020.05.002.

[5] S. F. Yousif, A. J. Abboud and H. Y. Radhi, "Robust Image Encryption With Scanning Technology, the El-Gamal Algorithm and Chaos Theory," in *IEEE Access*, vol. 8, pp. 155184-155209, 2020, doi: 10.1109/ACCESS.2020.3019216.

[6] J. Wang, J. Li, X. Di, J. Zhou and Z. Man, "Image Encryption Algorithm Based on Bit-Level Permutation and Dynamic Overlap Diffusion," in *IEEE Access*, vol. 8, pp. 160004-160024, 2020, doi: 10.1109/ACCESS.2020.3020187.

[7] X. Wang and P. Liu, "A New Image Encryption Scheme Based on a Novel One-Dimensional Chaotic System," in *IEEE Access*, vol. 8, pp. 174463-174479, 2020, doi: 10.1109/ACCESS.2020.3024869.

[8] S. Ibrahim and A. Alharbi, "Efficient Image Encryption Scheme Using Henon Map, Dynamic S-Boxes and Elliptic Curve Cryptography," in *IEEE Access*, vol. 8, pp. 194289-194302, 2020, doi: 10.1109/ACCESS.2020.3032403.

[9] Y. Li, D. Tang and R. Ye, "A Novel Color Image Encryption Scheme based on Hybrid Chaotic Maps," 2019 14th IEEE Conference on Industrial Electronics and Applications (*ICIEA*), Xi'an, China, 2019, pp. 1431-1436, doi: 10.1109/ICIEA.2019.8833652.

[10] X. Wang and S. Chen, "Chaotic Image Encryption Algorithm Based on Dynamic Spiral Scrambling Transform and Deoxyribonucleic Acid Encoding Operation," in *IEEE Access*, vol. 8, pp. 160897-160914, 2020, doi: 10.1109/ACCESS.2020.3020835.

[11] A. Al-Khedhairi, A. Elsonbaty, A. A. Elsadany and E. A. A. Hagras, "Hybrid Cryptosystem Based on Pseudo Chaos of Novel Fractional Order Map and Elliptic Curves," in *IEEE Access*, vol. 8, pp. 57733-57748, 2020, doi: 10.1109/ACCESS.2020.2982567.

[12] Q. Liu and L. Liu, "Color Image Encryption Algorithm Based on DNA Coding and Double Chaos System," in *IEEE Access*, vol. 8, pp. 83596-83610, 2020, doi: 10.1109/ACCESS.2020.2991420.

[13] F. Yang, J. Mou, Y. Cao and R. Chu, "An image encryption algorithm based on BP neural network and hyperchaotic system," in China Communications, vol. 17, no. 5, pp. 21-28, May 2020, doi: 10.23919/JCC.2020.05.003.

[14] H. Hu, Y. Cao, J. Xu, C. Ma and H. Yan, "An Image Compression and Encryption Algorithm Based on the Fractional-Order Simplest Chaotic Circuit," in *IEEE Access*, vol. 9, pp. 22141-22155, 2021, doi: 10.1109/ACCESS.2021.3054842.

[15] G. Shengtao, W. Tao, W. Shida, Z. Xuncai and N. Ying, "A Novel Image Encryption Algorithm Based on Chaotic Sequences and Cross-Diffusion of Bits," in *IEEE Photonics Journal*, vol. 13, no. 1, pp. 1-15, Feb. 2021, Art no. 3900215, doi: 10.1109/JPHOT.2020.3044222.

[16] S. T. Kamal, K. M. Hosny, T. M. Elgindy, M. M. Darwish and M. M. Fouda, "A New Image Encryption Algorithm for Grey and Color Medical Images," in *IEEE Access*, doi: 10.1109/ACCESS.2021.3063237.

[17] A. G. Mohamed, N. O. Korany and S. E. El-Khamy, "New DNA Coded Fuzzy Based (DNAFZ) S-Boxes: Application to Robust Image Encryption Using Hyper Chaotic Maps," in *IEEE Access*, vol. 9, pp. 14284-14305, 2021, doi: 10.1109/ACCESS.2021.3052161.

[18] H. Liu, X. Wang, and A. Kadir, ‘‘Image encryption using DNA complementary rule and chaotic maps,’’ Applied Soft Computing, vol. 12, no. 5, pp. 1457–1466, May 2012.

[19] M. G. Avasare and V. V. Kelkar, "Image encryption using chaos theory," 2015 International Conference on Communication, Information & Computing Technology (ICCICT), Mumbai, India, 2015, pp. 1-6, doi: 10.1109/ICCICT.2015.7045687.

[20] Prasenjit Kumar Das, Mr. Pradeep Kumar and Manubolu Sreenivasulu, “Image Cryptography: A Survey towards its Growth,” Advance in Electronic and Electric Engineering, India, ISSN 2231-1297, Volume 4, Number 2 (2014), pp. 179-184.

[21] Gajendra Singh Chandel, Vinod Sharma, Uday Pratap Singh, “Different Image Encryption Techniques-Survey and Overview,” International Journal of Advanced Research in Computer Science and Software Engineering, ISSN: 2277 128X, Volume 6, Issue 8, August 2016, pp. 264-268.

[22] Mukul, Sajjan Singh, Nishi, 2013, The Origins of Digital Image Processing & Application areas in Digital Image Processing Medical Images, INTERNATIONAL JOURNAL OF ENGINEERING RESEARCH & TECHNOLOGY (IJERT) NCEAM – 2013, ISSN (Online): 2278-0181, (Volume 1 – Issue 02), pp. 48-52.

Shashikant S. Radke received the B.E. degree in Computer Science and Engineering from the Government College of Engineering, Amravati of Amravati University, Amravati, Maharashtra, India in 2003 and the M.Tech. degree in Computer Engineering from VJTI, Mumbai of University of Mumbai, Mumbai, Maharashtra, India in 2010. He is currently pursuing the Ph.D. degree from MPSTME, Mumbai of SVKM's NMIMS University, Mumbai, Maharashtra, India. His research interests include Security and image processing and image cryptosystem.

Dr. Dhirendra Mishra received the B.E. degree in Computer Engineering from RAIT, Mumbai, Maharashtra, India in 2002, M.E. in Computer Engineering from TSEC, Mumbai, Maharashtra, India in 2008 and Ph.D. in Computer Engineering from NMIMS, Mumbai, Maharashtra, India in 2012. He is currently working as Professor in department of Computer Engineering with MPSTME, NMIMS University, Mumbai, Maharashtra, India. His research interests include Image Processing - Image Database, Pattern matching, Image/Data Mining, Biometrics, Storage Technologies, Data Analytics.