Artificial Intelligence & Robotics Development Journal
Volume 2, Issue 3, pp 187-200, July 2022, https://doi.org/10.52098/airdj.202255
ISSN: 2788-9696 Received: 6/7/2022 Revised: 12/7/2022 Accepted: 14/7/2022

Terminologies and Techniques based Image Encryption: A Survey

Rogash Younis Masiha[1,*]
[1] Researcher, Department of Statistics, Duhok, Iraq
* Corresponding author: Rogash Younis Masiha[1], rogash.babiri@gmail.com

Abstract

In this day and age of social media and smartphones, when practically all smartphone users are clicking and publishing their pictures on social media, it is of the utmost significance that the images that are transferred remain secure. Image encryption algorithms are an important part of the multimedia application landscape, playing an important part in both the security and authenticity of images. The purpose of this work is to provide an in-depth analysis of a variety of image encryption methods. In comparison to grayscale images, colored images are more affordable technologically, thus more people use them. Additionally, colored images have more information packed into them, so they are more useful. In this paper, a state-of-the-art survey of various techniques developed by various researchers in the field of image encryption is presented, and a detailed comparison of various available techniques and algorithms in the field of image encryption is carried out. Both of these aspects are addressed in the context of this particular paper.

Keywords: cryptography; Image Encryption; Image Decryption; Chaotic cryptography.

1. Introduction

The past decade has increased interest in smartphones, the Internet, and multimedia technologies. Music, film, and video are frequently utilized on the phone to transmit information about the more comprehensive network, i.e., texting. As a result of the increasing use of images and video (Diro et at., 2020), a secure network is now necessary. The information included in a photograph can be changed or tampered with by anyone who has access to the photograph (Ali & Ali, 2020). In order to include and advance network infrastructure, increased image security is required. Image security was protected by digital imaging encryption, which was the subject of research.

Cryptography in cyber security means converting data from a readable format to a format encrypted by an algorithm using a specific key. The encrypted data can only be read or processed after decrypted (Huang & Ye, 2018; Yousif & Saini, 2020). The more complex the encryption key, the more secure the encryption, as third parties are less likely to be able to decrypt it through algorithms that apply a set of random numbers in order to guess the correct combination. Encryption is one of the building blocks of data security to ensure that information is not stolen or read by someone who wants to use it for malicious purposes (Saini, & Yousif, 2021).

Individual users and large companies widely use data security encryption to protect user-information transmitted between the browser and the server. This information may include anything from payment data to personal information. A data encryption program, also known as an encryption algorithm or just cipher, is used to develop a cipher scheme that can theoretically only be hacked with massive computing power in the Internet of Things transitions (Alblushi & Yousif, 2021).

Before transmission across open networks, cryptography renders the original data meaningless. In order to safeguard the photographs, the most effective strategy is to use image encryption methods. As the name suggests, steganography is the practice of hiding information in cover material such as digital image enhancement, audio signals, or movies (Haji et al., 2020; Hasoon et al., 2011). As a result, steganography conceals data so that no one other than the intended recipient can decipher its contents. Although no information is hidden from view when using cryptography (Sivakumar & Venkatesan, 2015), the information's value is obfuscated. By embedding unique identification signals known as watermarks into the digital information, you can identify and authenticate your content utilizing digital watermarking techniques. The watermark will be removed from the watermarked image at the receiver end in order to validate the digital contents. Audio, image, video, and text are all examples of digital content (Hassan

et al., 2021). A watermark can be removed to validate ownership claims whenever watermarked photos are discovered to be unlawfully reused (Li & Kim, 2013). Figure 1 depicts the many types of Image Encryption.

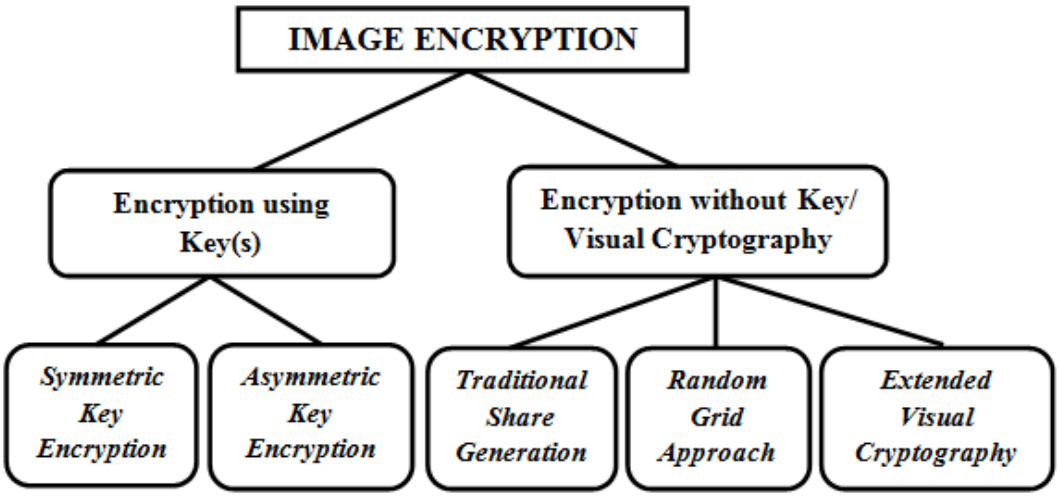

Figure 1: Image Encryption techniques

A single key is kept in place for both encryption and decryption in private key cryptography. If nothing else works, this means that if all else fails, the accompanying person will be given an emulation of the key, and the key will be struck by being transferred across a protected channel. Moreover, because they cannot be destroyed, then the machines accept them. In this approach, they are ready and able to encrypt large-scale data sets. Because of their vast convenience, the scrambling and decryption calculations are crucial to the overall adjusted encryption. The encryption check is required because the plaintext is more extensive than expected. Encryption's tally is being added together. The encryption check if the estimation is utilized to continue dealings with the information stranger plaintext quietly. Mysterious key cannot be differentiated from the encryption figure or plaintext, yet it is an accomplice of the encryption's information-gathering wellsprings (Sridevi, M., 2014).

This paper's primary contribution is comprehensive work that has reviewed previous material and examined image encryption methods. In addition, it examined and contrasted other optical image encryption methods, the vast majority of which were disregarded in previously published review publications. In addition, by looking over the most current articles, this paper has identified several problems with the image encryption methods that have recently been published. The numerous methods of picture encryption currently in use can be grouped according to various principles, including chaos, DNA, compressive sensing, and optical.

2. Encryption Background

Figure 2 depicts the general structure of picture encryption methods. Ciphering is the process of encrypting and decrypting images, and plain images need to be encrypted before they may be decrypted (Alia et al., 2020). P and C represent the plain and ciphered images, respectively.

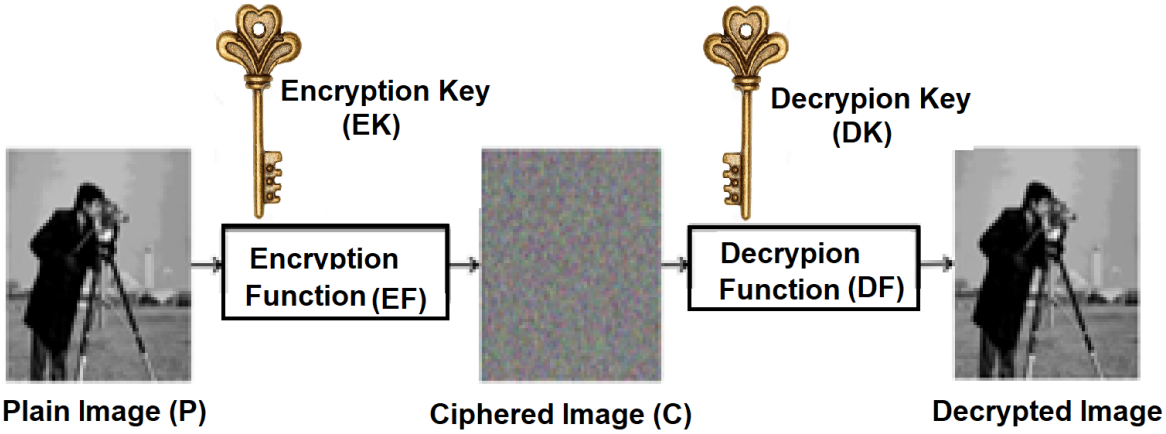

Figure 2: Generic framework of image encryption techniques

Data confidentiality and non-repudiation are just a few benefits of cryptography. Cryptography is widely employed today because of its many benefits in terms of security (Khanapur & Patro, 2015; Sridevi, M., 2014). Here is a list of some cryptography's main objectives

- **Confidentiality:** The computer stores sensitive information that should only be accessed by those with the proper credentials.
- **Authentication:** Any information that is received by a system must first undergo a check to determine the identity of the sender and determine if the information is coming from a legitimate source or a person using a false identity.
- **Integrity:** It is only permissible for the authorized party to make changes to the information that has been transmitted. Nobody in the middle, both the sender and the receiver, is authorized to make any changes to the communication.
- **Non-Repudiation:** This ensures that neither the person who sent the message nor the person who received it can reject the transmission of the message.
- **Access Control:** The information can only be accessed by those who have been granted permission.

When one party has to send confidential messages to another party across a communication connection, the method of cryptography is utilized to accomplish this task. The primary categories of cryptography are asymmetric and symmetric. When using a form of cryptography known as symmetric-key cryptography, both the sender and the receiver are aware of the same secret code, which is referred to as the key. The sender of the message uses the key to encrypt the message, and the recipient uses the same key to decrypt the message (Sridevi, M., 2014). In symmetric cryptography, the key plays a highly significant role because the security of the system is directly dependent on the characteristics of the key, such as its length and other parameters. The encryption and decryption algorithm pair use asymmetric key cryptography to protect sensitive information. When using public-key cryptography, keys only function when they are paired with their corresponding public and private counterparts.

The concept of public-key cryptography is to encrypt a picture on the sender's end by making use of the public key of the receiver, and then to pass that encrypted image on to the receiver. The receiver, on the other hand, made use of its private key to decrypt the encrypted image and convert it into a plain image. The operation of the public key cryptosystem as illustrated in Figure 2, which may be found here. The method assures that the cipher image is generated using the public key of the owner of the paired private key; nevertheless, on the receiver side, the private key of that specific paired key is used to decode the data without compromising the system's security. The fact that the public key can be used by anybody to encrypt data, while the private key is kept secret and only known to the owner of the paired key, is what provides security (Zhang & Tang, 2018).

Image encryption is essentially the act of making the image that is entered into the process unrecognizable so that a person who does not have authorized access cannot find the original image. The image that has to be encrypted is depicted in Figure 3, along with the image that was delivered after encryption.

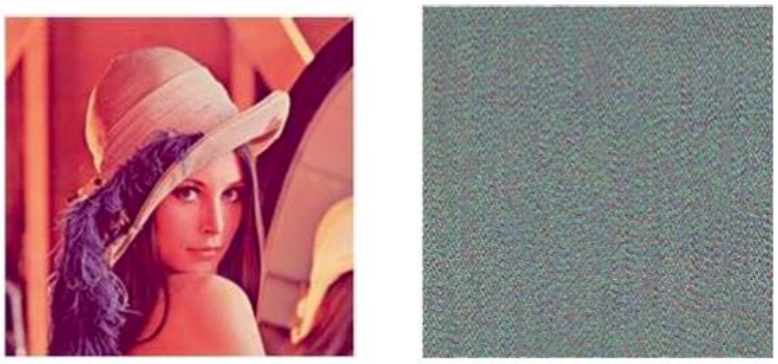

Figure 3: Original Image and Encrypted Image

3. Image Encryption Evaluation Matrices

The picture encryption method must first be evaluated, as this is an essential step before determining whether or not it is successful. By experimenting with these parameters, the many qualities of an image encryption technique can be investigated.

3.1. Differential Analysis

In order to conduct an analysis of the differential attacks, several measures, including the Pixel Change Rate (NPCR) and the Unified Average Changing Intensity (UACI), are utilized. The differential attack is a method for determining how sensitive an encryption technique is to even minute shifts in the plain picture that it is protecting. Attackers frequently introduce a barely perceptible alteration to the original image. Encrypt both the original and the updated image using the same key that you have kept hidden. After that, make an effort to determine the connection between the encrypted versions of the original photographs and the modified versions (Joshet al, 2017). The grayscale level weights of ciphered images C1 and C2 are marked as C1(i,j) and C2(i,j) for row (i) and column (j). The NPCR is calculated as in equation 1 (Abusham E.,2021).

$$NPCR = \frac{\sum_{i,j} D(i,j)}{M \times N} \times 100\% \tag{1}$$

The width and height are M and N of two random images and D (i, j) is represented in equation (2).

$$D(i,j) = f(x) = \begin{cases} 1, & if\ C_1(i,j) \neq C_2(i,j) \\ 0, & otherwise \end{cases} \tag{2}$$

In equation (3), the UACI computes the intensity average for the difference in color feature between the two cipher images, C1(i, j) and C2(i, j).

$$UACI = \frac{1}{M \times N}\left[\sum_{i,j} \frac{C_1(i,j) - C_2(i,j)}{255}\right] \times 100\% \tag{3}$$

3.2. Evaluation Ratings

Statistical analysis of an encrypted image is another method that can be used to break encryption schemes. Histogram Analysis (HA) and Correlation Coefficient (CC) are two methods that are utilized to confirm the robustness of an encryption scheme against statistical attacks (Kumar et al.,2017). These methods are applied to an encrypted

image's neighboring pixels for analysis. When two cipher images are compared, the Correlation Coefficient (CC) is used to find similarities (Al-Hatmi, & Yousif, 2017). It is calculated as in equation 4.

$$CC = \frac{\sum_i \sum_j W_{ij} W'_{ij}}{h \times w} \tag{4}$$

where W_{ij} and W'_{ij} are the weights of two cipher images, the height of the cipher image is h, and w is its width.

3.3. Information Entropy (IE)

It determines the average amount of information contained in each bit of an image. It includes all of the information that might be gleaned from the photograph in question. Each pixel has a separate value. Because of this, the entropy of an encrypted image denotes that every pixel possesses the same probability and follows a uniform distribution (Kumar et al.,2017). The entropy function, H(m) of a message can be calculated as in the equation 5:

$$H(m) = \sum_{i=0}^{2^N - 1} p(m_i) \times \log_2 \frac{1}{p(m_i)} \tag{5}$$

3.4. Execution Time (ET)

The amount of time necessary to carry out a specific method of picture encryption is what is meant by the term "execution time" (ET). It is the total amount of time required to compile and run the program. The ET should be kept to a minimum in order to facilitate the practical implementation of picture encryption. The standard units of measurement for it are seconds, milliseconds, or minutes (Kumar et al.,2017).

4. Literature Survey

Image encryption is a procedure that involves changing the values of the pixels in an image in such a way that it alters the intensity of that particular pixel. Changing the value of a pixel in a secret image causes the amount of information contained in the image to change as well. In the next subsections, we will talk about the literature review that pertains to a few different methods.

In the study by Kandele (Kandele & Tiwari, 2013), explored a novel method of encryption that does not require a predetermined key. The input string is broken up into multiple smaller parts, and each of those parts is encrypted using a different encryption technique. On the whole, three different techniques were used to encrypt the fragmented string based on its orientation. This was done in order to ensure that the data was secure. The key is derived from the two keys that are determined in separate ways to provide a higher level of protection. The most notable aspect of this

algorithm is that it modifies a portion of the string by converting its base, and then it distorts another portion of the string by rearranging its locations and performing an increasing number of repeats. Both of these processes occur simultaneously. The process of encryption takes time. The encryption process takes time.

A brand-new image encryption technique is presented in this publication (Kushwah & Shibu, 2013), which you can see here. It is already common knowledge that the algorithm's level of security is directly proportional to the length of the key. This implies that a longer key length will always be able to support good security features. The algorithm that was proposed used a key length of 128 bits, which provided an excessive amount of security for the algorithm that was proposed. Accessing the original key or performing a cryptographic analysis of the suggested key is required 2128 times in order to crack the key, which is an endeavor that is nearly hard for any hacker. Because the proposed algorithm does not use these kinds of mathematical formulas, there is no possibility that it will produce a floating-point error. Floating-point errors are impossible to produce. Calculations were made to determine both the correlation coefficient and the entropy values associated with the suggested algorithm.

Mohammed (Mohammad et al., 2017) explores several related image encryptions using classic and modern techniques. The results show that the chaotic encryption technique based on hyper-chaotic is the most efficient. In the paper (Ye et al., 2016) proposed a method for the efficient and safe encryption of images that makes use of the SHA-3 hash function in conjunction with double two-dimensional Arnold chaotic maps. This system makes use of the traditional encryption architecture, which consists of permutation in addition to diffusion. In order to save time during the permutation step and eliminate the time-consuming sorting procedure for the pixel location index, a unique wave-line-based confusion that features four random directions of shuffling has been developed. The key stream that is produced by the Arnold map is utilized for the respective vertical and horizontal circular confusions. In these confusions, the initial conditions are modified by the SHA-3 hash values of the chaotic matrix and a new vector that is constructed from the plain picture. In light of this fact, in contrast to certain other encryption strategies currently in use, the suggested technique is immune to the known-plaintext attack. In addition, the blocking technique is built using the outputs of the hash values in the previous block permuted picture. These outputs are then utilized to update again the initial conditions for the Arnold map. This occurs during the diffusion stage. During each cycle, the currently active block will have an effect on the following block, which provides a level of defense against the chosen-plaintext attack.

The study be Wang (Wang et al., 2017) proposed the idea of an adaptive optical encryption structure that may be used in a variety of lighting up situations and can accommodate disproportionate encoding. The information picture is encoded by the utilization of two self-assured shrouds that are positioned in a veering circular wave field at the information plane and the conjugate plane respectively. When compared to the partners who use planar brightening and symmetric keys, one of the most significant differences is that it is possible to change the locations of the optical components that are connected for encryption on a consistent basis. This results in unscrambling keys that are different from the encryption keys, as well as variable size displays of encoded and decoded images. Our proposal is strengthened by a concise and detailed numerical portrayal as well as an estimation of the results obtained from several data transmissions of the structure.

A technique to the encryption of images that makes use of a 2D sine map and a Chebyshev map was developed by (Chen et al., 2020). It came up with an antidegradation universal strategy for chaotic maps, which enhances performance even on devices with a poor level of precision. The concept of image encryption based on a spatiotemporal chaotic map and DNA encoding was proposed by Xuejing (Xuejing & Zihui, 2020). After first converting a simple image into three DNA matrices according to a random encoding rule, the final DNA product is then combined with the original matrix to produce a modern matrix. After that, the ascent matrix will perform several permutations on it to produce the cipher image. In order to encrypt the images, Wang (Wang et al., 2020) used linked map lattices, also known as CML, in conjunction with the DNA method. Ismail (Ismail et al., 2020) conducted research on a brand-new lossless picture encryption system that was founded on fractional-order and double-humped logistic maps. A technique for the encryption of images that is based on quantum coding and a hyperchaos system was developed by Luo (Luo et al., 2020). An approach to picture encryption was proposed by Lu (Lu et al., 2020) and is based on a chaotic map and an S-box. This methodology was utilized in the creation of the discrete compound chaotic map. Additionally, a logistic-sine system is used in the building of the S-box.

A study conducted by Arab (Arab et al., 2019) made the suggestion of developing an android application that would convert the text into an image. RGB substitution and the AES encryption algorithm are the foundations of this system. Using this approach, the secret key is deftly transmitted along with the figure message in a single transmission. With the expectation that this technique will be enough for resolving the key trade issue that frequently arises in encryption models. The encrypting and decrypting processes both use a mixed database, one on the sender's side and one on the recipient's side, so that the material can be transformed into a different picture. A new pixel has been added

to this picture, and it has been programmed to store an estimation of the combinational number that was used to change the content of the image. The AES key that was utilized in the calculation is converted into its corresponding RGB resultant value. At long last, the value that was achieved and the image that was produced are traded for the objective. The decoding process is carried out by connecting the switch steps on the beneficiary side. When put into action, the proposed framework will result in a significantly more grounded transmission of the material.

For the purpose of image encryption, (Arab et al., 2019) used a combination of the chaotic map with an advanced encryption technique (AES). They did the picture encryption using a modified version of the AES algorithm, and they created the key for the block cipher encryption using an Arnold cat map. In modified AES, the round keys were created with a chaos system in each round of encryption. This made the algorithm resistant to differential assaults, which was one of the goals of the modification.

A method for grayscale photos was proposed by Dawahdeh (Dawahdeh et al., 2018) which involved the use of the Hill cipher algorithm for time-efficient computations and the application of elliptic curve cryptography in order to compensate for the methodology's relatively poor level of security. The creation of random numbers does not make use of any chaotic maps in this instance. The method of elliptic curve cryptology is capable of working with smaller key spaces. In this case, it is not necessary to find the inverse of the matrix; rather, the same matrix is utilized in the encryption process. It is safe and can withstand a wide variety of assaults. Kandar (Kandar et al., 2019) presented a method for processing grayscale images in which the cyclic group would be responsible for generating the random sequences. The methodology is predicated on the use of cyclic groupings. In this case, first, the positions of the pixels are shuffled about, and then the bits that make up those pixels are shuffled around. After that, bits are moved in accordance with the transformation array, and iterative pixel additions for diffusion follow after that.

5. Results and Discussion

These are the problems that have arisen as a result of reading the relevant literature. Greater key size security is required in order to ensure that it is not readily broken. Even more importantly, there is a requirement for conventional hybridization of the cryptographic system. In addition, several kinds of diffusion matrices can be applied in the form of text as well as visual representations. As a result, in order to integrate steganography with cryptography in a way that provides a greater level of security, there is a requirement for encryption as well as decryption of the information.

As seen in Figure 4, the number of published research papers in 2021 has achieved the maximum number with 8310 articles, which indicates more interest in image encryption. On the other hand, in 2012, published about 1460

articles.

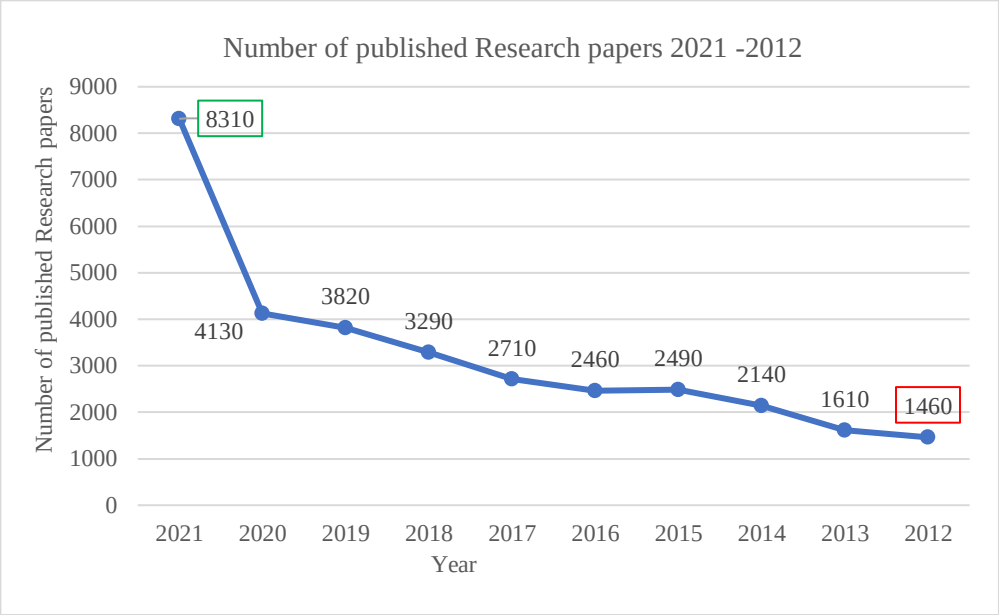

Figure 4: Number of published Research papers 2021 -2012

Figure 5 shows that the number of published review papers in 2021 has reached the maximum with 298 articles, demonstrating more attraction to reviewing the image encryption methods. However, in 2012, about 19 review articles were published.

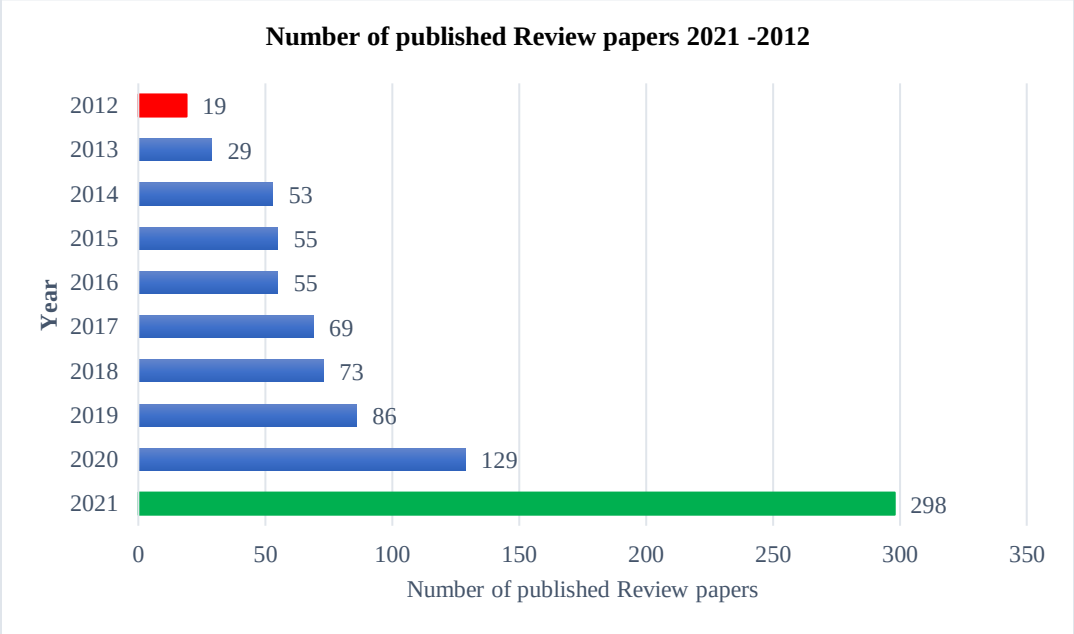

Figure 5: Number of published Review papers 2021 -2012

In Figure 6, the most implemented techniques for image encryption are Chaos methods, which achieved the highest rate with 41%, and XOR operations, which achieved the lowest rate with 3%.

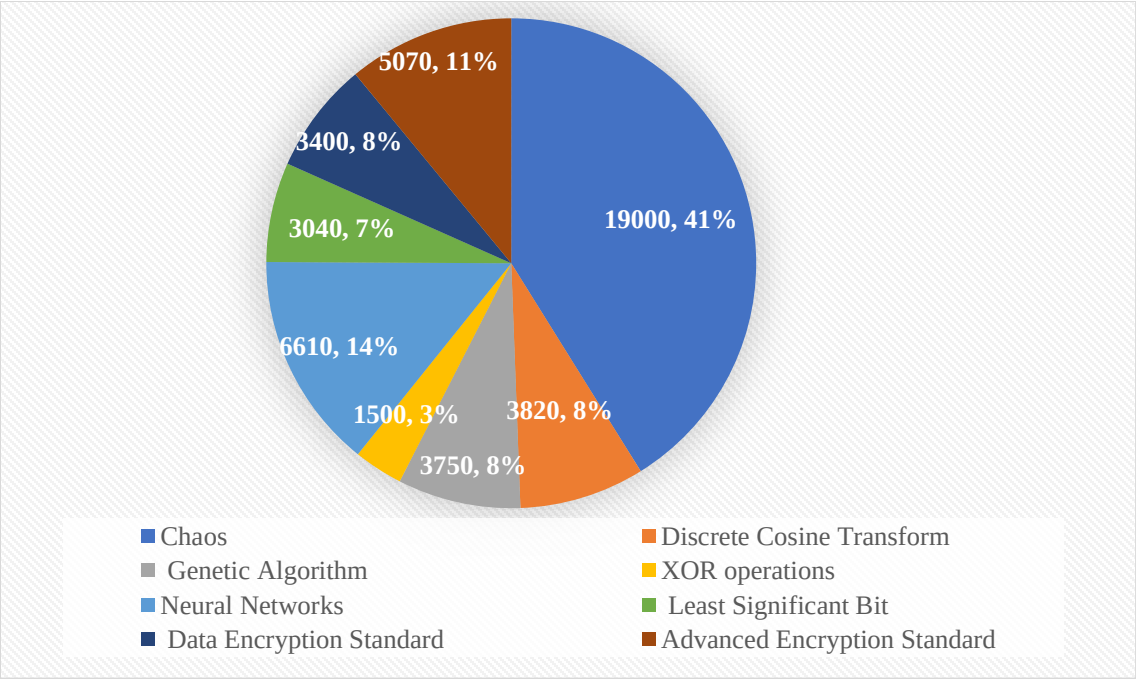

Figure 6: Method used for Image Encryption

These techniques that are used for image encryption mainly include the following:

- Chaos
- Discrete Cosine Transform
- Genetic Algorithm
- XOR operations
- Neural Networks
- Least Significant Bit
- Data Encryption Standard
- Advanced Encryption Standard

6. Conclusion

Maintaining absolute secrecy is one of the essential requirements for adequate information security. Researchers have found that the chaos-based approach is more suitable for digital image encryption due to some intrinsic properties

of digital images. Many algorithms have been designed to encrypt digital images, and researchers have found that this approach is the most effective. In this research, a detailed review of the various image encryption methods that are currently in use was presented. It was found that the techniques to picture encryption required a high level of confusion, did not correlate with the images that were used as input, had less computational complexity, and offered a high level of resistance to the cryptanalysis process.

The most implemented techniques for image encryption are Chaos methods, which achieved the highest rate with 41%, and XOR operations, which achieved the lowest rate with 3%. Based on the number of articles published, 2021 demonstrated a greater interest in reviewing image encryption methods.

In the future, there will be a requirement for such encryption methods that produce fewer mistakes in terms of mean square error.

Acknowledgment

The research leading to these results has received no Research Grant Funding.

Conflicts of Interest

The authors declare no conflict of interest.

References

[1]. Abusham, E. A. (2021). Image Processing Technique for the Detection of Alberseem Leaves Diseases Based on Soft Computing. Artificial Intelligence & Robotics Development Journal, 103-115.
[2]. Alblushi, A., & Yousif, M. J. (2021). Internet of Things: Layers, possible attacks, secure communications, challenges. Applied computing Journal, 103-118.
[3]. Al-Hatmi, M. O., & Yousif, J. H. (2017). A review of Image Enhancement Systems and a case study of Salt &pepper noise removing. International Journal of Computation and Applied Sciences (IJOCAAS), 2(3), 171-176.
[4]. Ali, T. S., & Ali, R. (2020). A novel medical image signcryption scheme using TLTS and Henon chaotic map. IEEE Access, 8, 71974-71992.
[5]. Alia, A. S., Al-Tamimib, M. S. H., & Ahmed, A. (2020). Secure Image Steganography Through Multilevel Security. Image, 11(1).
[6]. 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.
[7]. Chen, C., Sun, K., & He, S. (2020). An improved image encryption algorithm with finite computing precision. Signal Processing, 168, 107340.
[8]. [Dawahdeh, Z. E., Yaakob, S. N., & bin Othman, R. R. (2018). A new image encryption technique combining Elliptic Curve Cryptosystem with Hill Cipher. Journal of King Saud University-Computer and Information Sciences, 30(3), 349-355.
[9]. Diro, A., Reda, H., Chilamkurti, N., Mahmood, A., Zaman, N., & Nam, Y. (2020). Lightweight authenticated-encryption scheme for Internet of Things based on publish-subscribe communication. IEEE Access, 8, 60539-60551.
[10]. Haji, M. S., Rahim, M. S. M., Ahmed, F. Y., & Sulong, G. B. (2020). A Survey on Digital Image Steganography and Steganalysis. Journal of Computational and Theoretical Nanoscience, 17(7), 3256-3263.
[11]. Hasoon, F. N., Yousif, J. H., Hasson, N. N., & Ramli, A. R. (2011). Image enhancement using nonlinear filtering based neural network. Journal of Computing, 3(5), 171-176.
[12].[Hassan, O. M. S., Abdulazeez, A. M., Mohammed, A. I., Salih, S. O., Alih, S. H., Ahmed, F. Y., & Zeebaree, D. Q. (2021, November). An Efficient Robust Color Watermarking Algorithm Based on DWT, DCT, BFO and Implementation. In 2021 IEEE 11th International Conference on System Engineering and Technology (ICSET) (pp. 90-95). IEEE.

[13]. Huang, X., & Ye, G. (2018). An image encryption algorithm based on irregular wave representation. Multimedia Tools and Applications, 77(2), 2611-2628.
[14]. Ismail, S. M., Said, L. A., Radwan, A. G., Madian, A. H., & Abu-ElYazeed, M. F. (2020). A novel image encryption system merging fractional-order edge detection and generalized chaotic maps. Signal Processing, 167, 107280.
[15]. Joshy, A., Baby, K. A., Padma, S., & Fasila, K. A. (2017, November). Text to image encryption technique using RGB substitution and AES. In 2017 International Conference on Inventive Computing and Informatics (ICICI) (pp. 1133-1136). IEEE.
[16]. Kandele, N., & Tiwari, S. (2013). A New Combined Symmetric Key Cryptography CRDDBT Using–Relative Displacement (RDC) and Dynamic Base Transformation (DBTC). International Journal of Engineering Research & Technology (IJERT), Vol.2 - Issue 10, ISSN, 2278-0181.
[17]. Kandar, S., Chaudhuri, D., Bhattacharjee, A., & Dhara, B. C. (2019). Image encryption using sequence generated by cyclic group. Journal of information security and applications, 44, 117-129.
[18]. Khanapur, N. H., & Patro, A. (2015). Design and Implementation of Enhanced version of MRC6 algorithm for data security. International Journal of Advanced Computer Research, 5(19), 225.
[19]. Kumar, M., Kumar, S., Das, M. K., Singh, S., & Budhiraja, R. (2017, October). Chaotic dynamical systems based image encryption model. In 2017 International conference on information and communication technology convergence (ICTC) (pp. 93-98). IEEE.
[20]. Kushwah, K., & Shibu, S. (2013). New image encryption technique based on combination of block displacement and block cipher technique. International Journal of Computer Science and Information Technologies, 4(1), 61-65.
[21]. Li, X. W., & Kim, S. T. (2013). Optical 3D watermark based digital image watermarking for telemedicine. Optics and Lasers in Engineering, 51(12), 1310-1320.
[22]. Lu, Q., Zhu, C., & Deng, X. (2020). An efficient image encryption scheme based on the LSS chaotic map and single S-box. IEEE Access, 8, 25664-25678.
[23]. Luo, Y., Tang, S., Liu, J., Cao, L., & Qiu, S. (2020). Image encryption scheme by combining the hyper-chaotic system with quantum coding. Optics and Lasers in Engineering, 124, 105836.
[24]. 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.
[25]. Saini, D. K., & Yousif, J. H. (2021). Vulnerability and Attack Detection Techniques: Intrusion Detection System. In Cybersecurity (pp. 17-26). CRC Press.
[26]. Sivakumar, T., & Venkatesan, R. (2015). A novel image encryption using calligraphy based scan method and random number. KSII Transactions on Internet and Information Systems (TIIS), 9(6), 2317-2337.
[27]. Sridevi, M. D. (2014). Modular arithmetic in RSA cryptography. International Journal of Advanced Computer Research, 4(17), 973-8.
[28]. Wang, X., Wang, Y., Zhu, X., & Luo, C. (2020). A novel chaotic algorithm for image encryption utilizing one-time pad based on pixel level and DNA level. Optics and Lasers in Engineering, 125, 105851.
[29]. Wang, X., Zhou, G., Dai, C., & Chen, J. (2017). Optical image encryption with divergent illumination and asymmetric keys. IEEE Photonics Journal, 9(2), 1-8.
[30]. Zhang, Y., & Tang, Y. (2018). A plaintext-related image encryption algorithm based on chaos. Multimedia Tools and Applications, 77(6), 6647-6669.
[31]. Xuejing, K., & Zihui, G. (2020). A new color image encryption scheme based on DNA encoding and spatiotemporal chaotic system. Signal Processing: Image Communication, 80, 115670.
[32]. Ye, G., Zhao, H., & Chai, H. (2016). Chaotic image encryption algorithm using wave-line permutation and block diffusion. Nonlinear Dynamics, 83(4),1-11, 2067-2077.
[33]. Yousif, J. H., & Saini, D. K. (2020). Big Data Analysis on Smart Tools and Techniques. In Cyber Defense Mechanisms (pp. 111-130). CRC Press.