International Journal of Scientific Research in Engineering and Management (IJSREM)
Volume: 07 Issue: 05 | May - 2023 SJIF 2023: 8.176 ISSN: 2582-3930

Review of Image Encryption Techniques

Sanidhya Agarwal | Aksh Nayak

Department of Computer and communication engineering, Manipal University, Jaipur, Bagru, Jaipur, Rajasthan,303007

Abstract: *Today, one of the most important topics of study is security. The image can be transmitted securely using a widely used technique called encryption. Any picture encryption technique aims to create a high-quality hidden image in order to conceal information. This study reviews the protocols and frameworks of various image encryption systems that offer security and privacy.*

Keywords: *Chaos, Arnold Transform, XOR Algorithm.*

I. Introduction

Information is transformed using an algorithm in the process of encryption so that unauthorised users cannot read it. Image encryption is the process of encoding an image using an encryption method. Our lives are not complete without images. It has been common practice to capture events on camera. Digital photos are very confidential and secure because to image scrambling, which also offers aesthetic benefits and protection from unauthorised alterations and copying. It is a potent digital picture security technology with several uses across diverse sectors.. In order to diagnose aberrant symptoms, we employ MRI and CT scan images. Patients who want a second opinion frequently struggle to protect their privacy and transmit their CT or MRI pictures securely. However, the development of technology and image encryption methods has made sending and receiving photos simpler. However, a public medium like the internet could not always be secure for transmission. Military and medical photos may need to be kept discreet and away from prying eyes. Consequently, a secure image sharing technique is required in order to guarantee secure image transfer. To accomplish this, cryptography is essential. There are numerous techniques for image encryption because it is becoming more and more common and necessary. like Sun J. A chaotic image encryption algorithm combining 2D chaotic system and random XOR diffusion. Physica `Scripta. 2021 Jul 1;96(10):105208, Min, Li, Liang Ting, and He Yu-jie. "Arnold transform based image scrambling method." *3rd International*

Conference on Multimedia Technology (ICMT-13). Atlantis Press, 2013, Arnold transform [6-10] by Y. L. Yang, N. Cai; B. Li and J. W. Xu.

Our goal in writing this succinct evaluation is to give readers an accessible summary of the information in the aforementioned papers so they can decide which technique best suits their needs. We briefly discuss each technique.

II. Arnold's Encryption Algorithm [1][3][4][5]

The process involves applying two linear transformations iteratively to the image pixels to randomly shuffle them. The following is a list of the steps in Arnold's The following is a list of the steps in Arnold's image-scrambling process. Arnold, who first put up the idea in 1983. After rearranging the columns and rows, the Arnold transform is applied. The two images are not very comparable to one another. Arnold's approach to image obscuring provides a number of benefits. It offers a high level of security against unauthorised access and is quick and easy to implement. However, it is not a particularly effective encryption technique and is easily reversible if the settings used for the scrambling are known. As a result, it is frequently applied as a pre-processing stage in more complex encryption systems. Arnold's cat map, a mathematical model that captures the chaotic motion of a cat chasing its tail, served as the basis for this programme. Both grayscale and colour photos can be scrambled using the quick and easy procedure. Arnold's method of picture scrambling is quick and simple to use and provides a high level of protection against unauthorized access. Grayscale and colour photographs may be easily scrambled using it. However, because it is simple to reverse once the parameters for the scrambling are known, it is not a particularly good encryption technique. As a result, it is widely used as a pre-processing stage in encryption systems with greater complexity.

III.XOR Based Scrambling Algorithm [2]

By conducting a bitwise exclusive OR (XOR) operation between each pixel and a random key, XOR image scrambling is a straightforward technique for obscuring the individual pixels of a picture. The XOR image scrambling technique is a straightforward and quick way to jumble up the pixels in an image. However, if the random key is known, it is easily reversible and not very robust. In order to strengthen the security of the image, it is frequently employed as a fundamental technique in conjunction with other encryption techniques. The XOR image scrambling technique is a straightforward and quick way to jumble up the pixels in an image. However, if the random key is known, it is easily reversible and not very robust. In order to strengthen the security of the image, it is frequently employed as a fundamental technique in conjunction with other encryption techniques. This method is suitable for real-time applications like video streaming

since it is quick and easy to use. However, the strength of the key generation method has a significant impact on the security of the XOR-Based Scrambling method, and an attacker can quickly guess or crack a weak key. The security of the XOR-based scrambling technique heavily depends on the robustness of the key generation technique. The picture becomes subject to assaults if a weak key is employed since an attacker may easily guess or crack the key. To maintain the secrecy and integrity of the scrambled picture, it is crucial to utilise a robust and secure key creation process.

V. Arnold and Logistic [5]

According to Jinshan Wang, Xiaodong Wang, and Changjiang Zhang's technique, the watermark should be included into the image's low-frequency components in order to produce a resilient watermark. The provided image is first transformed using the Arnold transform. Then, for scrambling, logistic maps are employed. A discrete wavelet transform decomposes the initial image. The Arnold transform is used to combine the watermarked picture. The final watermarked picture is created by embedding this one into the discrete stationary wavelet domain's low-frequency components. As a result of the high visual quality of the final rebuilt picture, this approach is both effectively invisible and resilient to noise, rotation, and compression. The watermark is virtually undetectable according to the suggested approach, which also provides good visual quality in the rebuilt picture, making it challenging to find. The watermark can maintain its integrity even after an image has been altered since it is resistant to popular image editing techniques including noise, rotation, and compression. Arnold and logistic maps work together to give a safe and effective technique to insert watermarks in digital photos, making it helpful for a variety of applications including copyright protection and image authentication.

VI. Fractional Fourier Transform [6][7]

For the purpose of calculating the Fourier transform of functions, specific formulae have been developed. A Fourier transform converts one function, say f(x), into another, let's call it F(x). Both the Fourier transform and the fractional Fourier transform are used widely. The approach put forth by Juan Vilardy, Jorge Calderon, Lorenzo Mattos, and Cesar Torres proposes to encrypt images using the fractional Fourier transform. In this technique, masks and the fractional Fourier transform are used to effectively phase-encrypt the picture. The necessary masks are generated at random, and analogue rather than digital images are used for encryption. The opposite of the encryption process is the decryption procedure. This procedure computes quickly. Real-time applications are made possible by the rapid decryption process, which is the opposite of encryption. However, the unpredictability of the mask creation process and the potency of the encryption key

determine how secure the encryption technique is. This method offers resistance against a variety of assaults, such as statistical, differential, and brute-force assaults. However, in order to ensure adequate encryption, the analogue parts of the system must be precisely calibrated and enormous volumes of random data must be generated and stored.

VII. Conclusion

We have covered a few contemporary methods for image encryption in this paper that adhere to the highest security requirements. The papers in the references that the reader finds interesting and that are relevant to their own study goals can be read. Even though there are already several image encryption methods, more may be created so that hackers cannot access the pictures for bad purposes. Presenting a perfectly secure system, however, is impractical due to the prevalence of unauthorized picture decoding tools and the availability of ambitious unauthorized hackers. As a result, image encryption is a dynamic process that necessitates frequent modifications to the transmission technique.

IX. References

[1]. V.M. Manikandan, V. Masilamani. “An Efficient Visually Meaningful Image Encryption Using Arnold Transform”, TechSym Conference Pages: 266 – 271, IEEE, 2016.

[2] A chaotic image encryption algorithm combining 2D chaotic system and random XOR diffusion.

[3] Min, Li, Liang Ting, and He Yu-jie. "Arnold transform based image scrambling method." *3rd International Conference on Multimedia Technology (ICMT-13)*

[4] *Arnold's Cat Map for Image Encryption" by K. B. Khanchandani and P. W. Raote (2011)*

[5] Image Encryption Using Arnold Cat Map and Logistic Map" by J. S. Khehra, A. K. Tiwari, and S. K. Singh (2019)

[6]. Juan M. Vilardy, Jorge E. Calderon, Cesar O. Torres, Lorenzo. Mattos, “Digital Images Phase Encryption using Fractional Fourier Transform” CERMA conference, Pages: 15–18, 2006.

[7]. H Yoshimura, R Iwai,” New encryption method of 2D image by use of the fractional Fourier transform”, IEEE Conference on Signal Processing, Pages: 2182 – 2184, 2008.