**How to Cite**:
Madan, S., Magon, M., & Chandila, S. (2022). Secure encrypted image parsing over server. *International Journal of Health Sciences*, *6*(S3), 10452–10461.
https://doi.org/10.53730/ijhs.v6nS3.9449

# Secure encrypted image parsing over server

**Shefali Madan**
Associate Professor
*Corresponding author email: shefalimadan@gmail.com

**Mahima Magon**
Associate Professor
Email: Mahima.magon@gmail.com

**Suman Chandila**
Assistant Professor
Email: sumanchandila8@gmail.com

***Abstract*---**Security of data is the major concern in today's scenario. Transferring of data from one source point to a destination point is referred as data transfer. Encryption is one of the methods which is widely used for transfer of information over secured communication channel. Through security of various encryption techniques, we can make our data safe from hackers. Confidential data can be secured by various proposed methodologies and algorithms. Survey has been performed taking into consideration various image encryption techniques and algorithms as well as procedures in this paper and reference ideas about various cryptography techniques and discussed about the challenges faced in the image encryption.

***Keywords*---**encryption, decryption, cryptography, hyper-chaotic.

## Introduction

In today's scenario images are all over web. Various social networking sites and many more users use image sharing multimedia among friends. But with this comes a responsibility of securely sharing data between users and encryption is a technique to secure data. Various image encryption techniques are used to convert original image to unreadable image that can't be read by any other user and keep it confidential. To keep our image secure it is important to encrypt image before parsing and decrypt image to end user. Image encryption has been used over various places like multimedia systems, social networking sites, military communication, navy code signals communication etc. Images are basically different coded text. We can use several old techniques to directly encrypt data by using various cryptosystems but certainly there are lags and

flaws with them that create great effects in lowering the efficiency. One could be image size is always greater to text as it is multimedia file. Other problem is that decrypted image musty be equal to original image as it was before encryption applied. Thus, old systems are lags and are less efficient as well as less reliable. Various encryption algorithms are proposed to make it efficient and faster.

In today's world where data is more important than money people requirements are to securely parse their data images to authenticated user. It is a big challenge for security members to safely and on time parse data to authenticated user. Paper has been organized in such a way that it introduces why it is necessary to encrypt images, what are previous reviews of various algorithms used for image encryption and decryption, literature reviews based on various analysis and finally a conclusion.

**Cryptography**

(or cryptology; "hidden, secret"): It is known for the study of various techniques for communicating over the protected networks and when third party is present (called adversaries). In general, it is the technique where we construct and analyze the protocol to overcome influence of adversary relating to various aspects including the data integrity, its confidentiality and its authenticity.

**Plain Text**

It is the original data text that contains information as it is.

**Cipher text**

It is the coded or protected non- understandable form of original text called cipher or encrypted form that is formed when some algorithm is applied.

**Encryption**

It is the process of coding original image into unreadable form using some algorithm that can only be accessed by authenticated user that has the key to decrypt the cipher data and obtain original information.

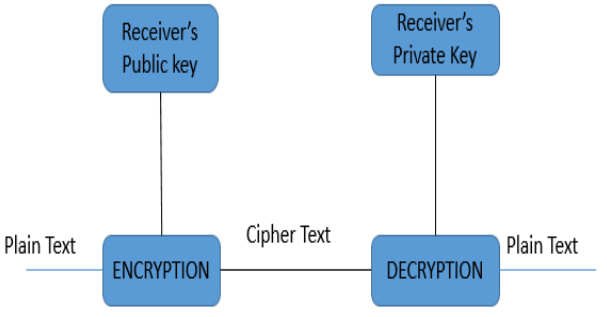


Fig.1. Asymmetric Cryptography Process

Figure 1 “Asymmetric cryptography” is a technique where both sender & receiver have knowledge of a secret code which is known as key. Information can be send by sender by encryption and thereafter read by receiver using decryption of key mechanism. There is one more asymmetric key cryptography called “public key encryption”. It is known best for encryption & decryption algorithm pair. Cryptography is a technique where a person sends secret messages to other over the transmission phase. Cryptography technique basically works on various algorithms i.e., for encryption as well as decryption of data.

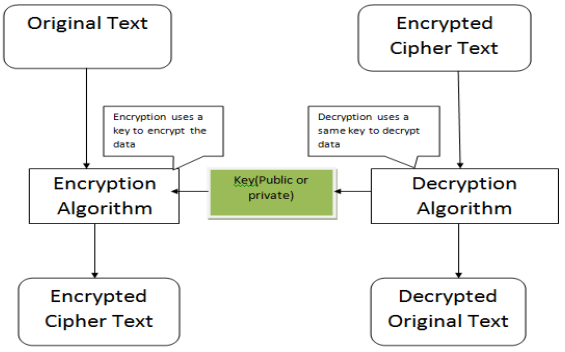


Fig. 2. Symmetric Key Encryption

Figure 2 Describes the process of **“symmetric encryption”** in which a single key is used for both encryption as well as decryption. These days when a person is transferring sensitive information which gets accumulated in our computers and got leaks over the web networks, we need to safeguard and also ensure the security of information. Extras include, when transmitting information, it is very essential to safeguard our images from illegal access. A weakness gets introduced into the cryptosystem when there is carelessness handling of “plaintext” which lets an attacker gain access the cryptograph. “Plaintext” whether in electronic or paper format is vulnerable to some attack. Physical Security is the security of the information and all storage devices from the attack which is physical i.e., someone physically enter building offices to acquire storage mediums, papers, documents, computers etc. Any type of document material which has to be destroyed and if it is not discarded securely, it will impose a risk. By reverse-engineering even small evidence of documents and any erased media will be reconstructed with knowledge.

**Previous Algorithm and Methods**

“DES (Data Encryption Standard)”: “NIST (National Institute of Standards and Technology)” recommended its first secure encryption standardization. IBM proposed an algorithm which they call them “Lucifer” and it was based on this algorithm. Standardization was done in 1974”TropSoft”. After that many methods and various attacks were recorded that became enlightened to weakness and flaws of “DES” that made them and unprotected cipher code. “3DES”: “DES” has an enhancement and as a result, the “3DES (Triple DES) Encryption Standard” came into play which is a standardized of the encryption method is same to “Original

DES" but can be applied 3 times to secure the level. But compared to previous, it works much slower.

"AES (Advanced Encryption Standard)": NIST introduced new standards. This replaced DES algorithm. Rijndael algorithm was considered as best encryption practices. In brute force attack large amount of data is stored and hit and trial character combinations are used to breach data. Both block codes consists of AES and DES. Figure 3 shows the highest performance of AES in comparison to other algorithms. "Blowfish": "Bruce Schneier" provided algorithm which is widely utilized in public domain secure encryption algorithm. "Bruce Schneier" was a leader and world's leading cryptologists who specializes in security of counterpane systems. Introduction of "Blowfish Algorithm" which is having a variable length key. Hardware applications that can be optimized as well as widely used in software application. The key consist of 64 bit block which has less secure key problem.

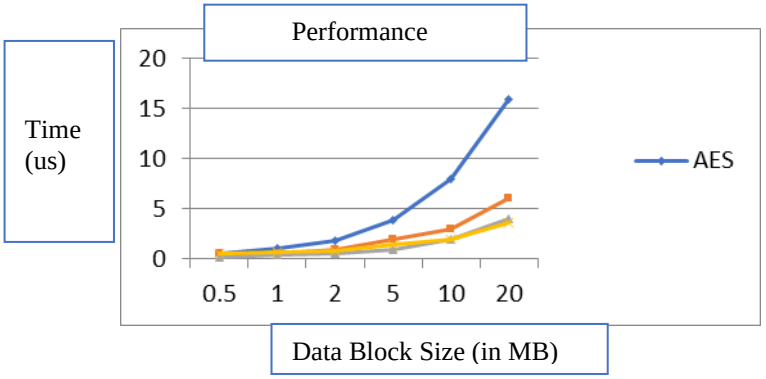


Fig.3 Graphical Performance of Algorithm

Figure 3 compares the performance of algorithms in accordance to the time and size captured by them to calculate the no of pixel value.

**Literature Review**

**Image Encryption Using Advanced Hill Cipher Algorithm**

"Vibhudrendra Acharya, Saroj Kumar Panigrahi, Sharat Kumar Patra, and Ganapathi Panda" [10] have introduces an advanced developed Hill (Advihil) ciphere enumeration that uses an invisible key framework.They proposed "AdvHill" (advance ciphere) figure calculation utilizing the bygone one. What's more, it is plainly observed which unique Hill Cipher cannot do its working appropriately as it didn't encode the pictures appropriately if the picture comprises of huge territory safeguarded with similar dark shades. In any case, their calculation works for any pictures with various dark scale just as shading pictures.

**Digital Image Encryption Algorithm Based Composition of Two Chaotic Logistic Maps**

“Ismail Amr Ismail, Mohammed Amin, and Hossam Diab” [13] introduced tumult “based stream figure”, forming 2 confused strategic mapping and also outer secret (hidden) key for hiding the image. This “mystery key” of pieces of 104 and 2 clamorous calculated maps had been used to segregate the scrambled image and the plain image. Furthermore, the “mystery key” is modified subsequent to encoding every pixel of normal original plain image that makes the scrambled image progressiveness robust. “Criticism instrument” that enlarges heartiness of the introduced framework is present at that point.

**Image Encryption Using Affine Transform and XOR Operation**

"Amitav Nag, Jyoti Prakash Singh, Surbani Khan, Saswati Ghosh, Sushant Biswas, D. Sarkar and Partha Pratim Sarkar" [15] came up with the idea of a new algorithm that would overhaul image pixels using the affine transformations. This algorithm is divided into two two-step encryption and decryption algorithms. In the first step, in the encryption of resultant image take place using operations like XOR then using affine transformations, the redistribution of various pixels take place to different places with “4-bit keys”. The new image i.e. transformed was then distributed into two pixels x two pixels blocks and every block was secured utilizing the “XOR operation” with “48-bit keys”. This result provides necessary conclusion that relation of pixel values was noticeably reduced after the transformation.

**Permutation based Image Encryption Technique**

"Seshapallivindrakanti and PS Adani" [16] proposed a newly made working algo based on pixel shuffling numbering an incentive for maintenance of image quality. This encryption is classified into three processes. Phase 1 was encryption of image. Phase 2 is the major implementation and generating phase. Phase 3 is the knowing/identifying process. It provides privacy to the colour image and reduces computation.

**Image Encryption Based on the General Approach for Multiple Chaotic Systems**

"Qais H. Alsafsah and Ouda A. Arfoa" [17] introduced a newly made algo for combining the “Lorenz chaotic system and the Rosler chaotic system”. By means of experimentation analysis, both showed demerits of this encryption algorithm of image that were highly ambiguous with greater speed, abundance of space for key and security of high level.

**Image Encryption Using Differential Evolution Approach in Frequency Domain**

"Ibrahim S. I. Abuba and Meel A. S. Hasan" [18] introduced newly vigorous methodology for “image encryption” that manipulates phase and magnitude by utilising “Differential development” (DD) and “Development Evolution (DE)”

approaches. To elaborate and show new image encryption algorithm security, they performed principal various analysis i.e. “space analysis, statistical analysis, and principal sensitivity analysis”.

**Chaotic Image Encryption Algorithm Based on Circulant Operation**

This is encryption system is based on “time-delay Lorenz system”. Circulant matrix is used to represent novel chaotic image encryption. The permutation of pixels is placed according to the 1st and 2nd components in diagonal and antidiagonal respectively, using the sequence generated by the Lorenz system. From time-delay Lorenz system a pseudo-random permutation is made by making use of all the given components. Plain image parameters decide the modular operation to be followed for the block’s diffusion. To stop the attack from hacker various experimental analysis is carried out that shows larger key space properties. Attacks like brute force attack, gray values to be distributed in encrypted image and the dependence of sensitive information. Hence, it can be considered an effective method for faster image encryption.

**Optical color image encryption without information disclosure using phase-truncated Fresnel transform and a random amplitude mask**

New color image encryption using a phase-truncated Fresnel transform and random amplitude mask (RAM) is proposed in this [24], without the possibility of revelation of details. In the first step image is divided into three categories (red, green and blue). The possibility of leakage of data as compared to other methods is reduced by adding “RAM system”.

**Image Security using Chaos and EZW Compression**

“T. Venkatasinath Gupta, Chau. Naveen, V. R. Satpute and A. S. Gandhi” made a new emphatic method of image security as well as image compression by utilising both chaos and EZW. Chaos image is used for the security of data, but it contains some drawbacks, which is improvised by implementing together with EZW. It is observed that differentiation of EGW with “chaos” using levels gives 2 levels security of image. Major advantages that can be broadly classified as 2 i.e. secured images as well as less in size i.e. compressed form. In the paper, “Table II” demonstrates that reduction ratios are significantly higher with good “PSNR values”. Conclusion involves a mileage, i.e. security and compressed form is best suited for various apps that include both the deciding factors and these parameters that are of great importance.

**Image Encryption Scheme Based on a Peter De Jong Chaotic Map and a RC4 Stream Cipher**

This effective method is proposed by Peter De Jong and mainly based on chaotic map and RC4 stream cipher and the initial keys will generated by RC4 Stream generator[25]. This stream produces rotation of pixel value randomly and utilized for diffusion operations. This method follow the three stages “permutation”, “number of pixel value” and “diffusion”.

**Hyper-chaotic Colour Image Encryption Algorithm and Security Analysis**

"Chenghai Li", "Fangzheng Zhao", "Chen Liu", "Lei" and "JieZhang" came up with idea which is based on '4D hyper-chaotic system' and "transformation-scrambling-Diffusion" and was algorithm for new colour image encryption. It works on "scrambling-diffusion" methodology. The algorithm shows good statistical characteristics as per the chaotic sequence generated by the 4D-chaotic system, the scrambling and diffusion are completed. The encryption and decryption process were easy. Its design mechanism works in a way, that some encryption keys depend upon the plain text which indirectly increasing the sensitivity towards it and thus reduces the chances of attack. This algorithm has better security as well as strong anti-damaging ability. Therefore, in the field of image encryption, this algorithm plays a vital role.

**Medical Color Images Encryption Using Chaotic Systems**

"Seyed Shahabeddin Moafimadani, Yucheng chen, chunming tang" proposed the algorithm which mainly focuses on the part to increase the process of permutation and adaptive diffusion and implemented using MATLAB software that measures the image quality on the basis of correlation coefficients and number of pixel rate change and intensity.

**Methods of generalized Vigenére-type table in Virtual Planet Domain**

In this technique proposed set of rules is primarily based on a new method using a generalized Vigenére-kind table over a symmetric cluster of order n within the virtual planet domain (VPD). The primary aim of this work is to conquer on the limitations of DNA totally based on the coding, those are noted in this article. Using NIST statistical VPD has been examined and in this proposed scheme the encrypted image is first converted into the VPD domains and then interfacing will be done using proposed methods[21].

**Joint encryption and compression of 3D images based on tensor compressive sensing with non-autonomous 3D chaotic system**

For the three-dimensional (3D) data sequences like video , medical image etc. various techniques are used in simultaneous compression as well as encryption of images[22]. For the compression ratio this may be enough for compression ratio and decryption accuracy but cannot have both at the same time. As images are taken care of individually so their co-existence or relation is not to be considered. This is the major concern. Instead of different 2D images as sequence "Tensor Compressive Sensing (TCS)" is used to solve this problem to compress and encrypt image of 3D as specifically "Tensor". For the security of image, we further proceed by a non-autonomous system namely "Lorenz System" is made to have a control over the TCS 3 matrices of separate measurements. This method maintains a balance between decryption security and compression ratio. The basic structure of 3D image sequences is preserved.

**Secure surveillance framework for IoT systems using probabilistic image encryption**

Firstly, to extract essential information various informative frames are extracted by using “video summarization method” through visual sensors. An unauthorized event when sensed from various keyframes, it automatically sends an alert message to the authority[23]. Extracted keyframes decides the final conclusion as any upgradation made in transmission through cracker can result in losses of data. To solve this problem a proposal made of a lightweight and faster probabilistic algorithm for securing keyframes before any transmissions. Taking into considerations of the processing and memory consumptions that are required of devices that are constrained which makes efficient IOT systems.

**Conclusion**

In the fastest growing world of hackers where everything is insecure and not ensure for security, so the image and data security is the main issue and it is very important. This paper adduces the surveyed different technologies related to image security. In this paper, various image encryption algorithms and methods are stated which meets the industry’s safety standards. An interested reciter may read the papers in references that are similar to their own objective of the research. We have not elaborated the specifics of each of the methods for the sake of brevity and distribution of appropriate information. Although various methods for image encryption come into view but still have plenty of scope to discover so that the hackers can’t hack them for their own usage. However, it is not feasible to propose a fully safe method due to increasing number of hackers and one more reason that is growing very fast in today’s world which is artificial intelligence because AI machines have the ability to think and make decisions more rapidly as compared to humans and implement it independently. So it is necessary to make the changes in the transmission technique periodically.

**References**

1. Wang Ying, Zheng DeLing, Ju Lei, et al., ―The Spatial-Domain Encryption of Digital Images Based on High-Dimension Chaotic System‖, Proceeding of 2004 IEEE Conference on Cybernetics and Intelligent Systems, Singapore, pp. 1172-1176, December. 2004
2. M.-R. Zhang, G.-C. Shao and K.-C. Yi, ― T-matrix and its applications in image processing‖, IEEE Electronics Letters 9th December 2004 Vol. 40 No. 25
3. Shaojiang Deng, Linhua Zhang, and Di Xiao, ―Image Encryption Scheme Based on Chaotic Neural System‖, J. Wang, X. Liao, and Z. Yi (Eds.): ISNN 2005, LNCS 3497, pp. 868-872, 2005.
4. Huang-Pei Xiao Guo-Ji Zhang ―An Image Encryption Scheme Based on Chaotic Systems‖, IEEE Proceedings of the Fifth International Conference on Machine Learning and Cybernetics, Dalian, 13-16 August 2006.
5. GuoshengGu, Guoqiang Han ―An Enhanced Chaos Based Image Encryption Algorithm‖, IEEE Proceedings of the First International Conference on Innovative Computing, Information and Control (ICICIC'06) in 2006.

6. M. Zeghid, M. Machhout, L. Khriji, A. Baganne,R. Tourki, A Modified AES Based Algorithm for Image Encryption World Academy of Science, Engineering and Technology 27 2007.
7. Mohammad Ali BaniYounes and AmanJantanImageEncryption Using Block-Based Transformation Algorithm IAENG International Journal of Computer Science, 35, 2008.
8. Saroj Kumar Panigrahy, Bibhudendra Acharya and Debasish Jen, Image Encryption Using Self-Invertible Key Matrix of Hill Cipher Algorithm 1st t International Conference on Advances in Computing, Chikhli, India, 21-22 February 2008
9. Mohammad Ali BaniYounes and AmanJantan, An Image Encryption Approach Using a Combination of Permutation Technique Followed by Encryption, IJCSNS International Journal of Computer Science and Network Security, VOL.8, April 2008.
10. Vibhudendra Acharya, Saroj Kumar Panigrahy, Sarat Kumar Patra, and Ganapati Panda, Image Encryption Using Advanced Hill Cipher Algorithm, International Journal of Recent Trends in Engineering, Vol. 1, No. 1, May 2009
11. Zhang Yun-peng, Liu Wei, Cao Shui-ping, Zhai Zheng-jun, Nie Xuan, Dai Wei-di, Digital image encryption algorithm based on chaos and improved DES, IEEE International Conference on Systems, Man and Cybernetics, 2009.
12. Seyed Mohammad Seyedzade, Reza EbrahimiAtani and SattarMirzakuchaki, A Novel Image Encryption Algorithm Based on Hash Function 6th Iranian Conference on Machine Vision and Image Processing, 2010.
13. Ismail Amr Ismail, Mohammed Amin, HossamDiab A Digital Image Encryption Algorithm Based a Composition of Two Chaotic Logistic Maps, International Journal of Network Security, Vol.11, No.1, PP.1 -10, July 2010.
14. Kamali, S.H., Shakerian, R., Hedayati, M., Rahmani, M., A new modified version of Advance Encryption Standard based algorithm for image encryption,Electronics and Information Engineering (ICEIE), 2010 International Conference.
15. Amitava Nag, Jyoti Prakash Singh, Srabani Khan, Saswati Ghosh, Sushanta Biswas, D. Sarkar ParthaPratim Sarkar, Image Encryption Using Affine Transform and XOR Operation, International Conference on Signal Processing, Communication, Computing and Networking Technologies (ICSCCN 2011).
16. SeshaPallaviIndrakanti, P.S.Avadhani, Permutation based Image Encryption Technique, International Journal of Computer Applications (0975 – 8887) Volume 28– No.8, 2011.
17. Qais H. Alsafasfeh, Aouda A. Arfoa, Image Encryption Based on the General Approach for Multiple Chaotic Systems Journal of Signal and Information Processing, 2011.
18. Ibrahim S I Abuhaiba, Maaly A S Hassan, Image Encryption Using Differential Evolution Approach Inn Frequency Domain
19. Seyed Hossein Kamali, Reza Shakerian “A New Modified Version of Advanced Encryption Standard Based Algorithm for Image Encryption”, IEEE Electronics and Information Engineering International Conference (ICEIE 2010). 1-3 Aug. 2010, V1-141 - V1-145.

20. [20] Shannon CE., "Communication theory of secrecy system," Bell SystTech J 1949; 28: 656-715.

.

21. Manish Kumar, R.N. Mohapatra, Sajal Agarwal, G. Satish, S.N. Raw, “A New RGB Image Encryption using generalized Vigneretype table over symmetric group associated with virtual planet domain”, Multimedia Tools and Applications, Volume 78, Pages: 10227 – 10263, 2019 (Springer)
22. Wang Q, Wei M, Chen X, Miao Z (2018) Joint encryption and compression of 3D images based on tensor compressive sensing with non-autonomous 3D chaotic system.
23. Muhammad K, Hamza R, Ahmad J, Lloret J, Wang HHG, Baik SW (2018) Secure surveillance framework for IoT systems using probabilistic image encryption. IEEE Trans Ind Inform 14(8):3679–3689.
24. Wang Y, Quan C, Tay C (2015) Optical color image encryption without information disclosure using phase-truncated Fresnel transform and a random amplitude mask. Opt Commun 344:147–155.
25. Gururaj Hanchinamani, Linganagouda Kulkarni, an efficient image Encryption Scheme Based on a Peter De Jong Chaotic Map and a RC4 Stream.