International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 04 Issue: 10 | Oct -2017 www.irjet.net p-ISSN: 2395-0072

# Color Image Encryption for Secure Transfer over Internet: A survey

**Farzana Kabir [1], Jasmeet Kaur[2]**

[1] *M.Tech (CSE), AP Goyal Shimla University, Shimla, Himachal Pradesh, India*
[2] *Associate Professor, AP Goyal Shimla University, Shimla, Himachal Pradesh, India*

---

**Abstract -** *With the tremendous and rapid growth of information interchange through internet transmission, information security has become a major issue to deal with. As because images are being used more in business and industrial process, military and medical and also in scientific researches, it has become the important factor to protect the confidential image data from unwanted access or intruders. Because of development of technology, the hacking techniques, and attacks are also becoming more and more intelligent. As a result, traditional approaches of image encryption are failing to be a good competitor with the attackers. Image encryption has been a wide area of research field. The protection of image data is more important because it contains maximum features of a person or thing. Image encryption is employed to protect an image from unauthorized access and increase image security over internet. Nowadays Internet is used for transmitting and storing huge amount of information. Since the internet has many loopholes and several scopes of hacking or being attacked by intruders. So, our personal and private image need to be protected during transmission over internet. Researches have done satisfactory numbers of researches and developed lots of image encryption algorithms till now. In this paper, we illustrated a brief survey of some significant works regarding image encryption techniques in different domains and our main perspective will be to come up with a better solution to make images more secure in the future.*

***Key Words***: Image, Encryption, Security, Internet, Transmission

## 1. INTRODUCTION

Image is one of the multimedia data that is different from simple text data in many ways. It can be defined as graphical or pictorial representation of any information. Image inordinately assist communication over internet in this phase of multimedia evolution. The evolution of multimedia technology in our modern generation has made digital images to play a more significant and unique role than the other data such as traditional texts, number. That's why images demand serious protection of users' privacy for all applications and during transmission [6]. While transmitting a private or confidential image over an insecure transmission channel over internet, it is necessary to ensure the security and privacy and preserve the confidentiality of the image. Encryption is the process of encoding messages & information in such a way that only authorized persons can be able to access it. An authorized person can read the message with the key provided by the sender. Any unauthorized intruder cannot access the encrypted data because he or she does not have the required key, without which it is not possible to read the confidential information [2]. Encryption is the process of disguising a message [3]. In encryption, the content of confidential data is protected and a key is required to decrypt the information properly. The original message is called the Plaintext and the encrypted message is called the ciphertext [3]. It can be employed to various types of data like text, image, audio etc. [4] Image encryption is one of the techniques that grips restraint of image. Image encryption provides a prominent strategy to secure the image over internet [1]. Encryption of image is possible with the traditional data encryption algorithms such as DES, RSA etc. But they are not totally efficient for image data. [4] Digital image contents needs to be secured from various types of attacks such as interruption, interception, modification, and fabrication etc. [5]. The image size is usually more than text. For which, the traditional encryption algorithms need more time to directly encrypt the image data. While applying large, complicated and difficult performance and security analysis, the encryption technique becomes more time-consuming. [9] Most of the existing image security systems are not up to date enough to fight against the latest possible attacks. While transferring images over the internet, image security becomes the major security concern for military, security agencies, social or mobile applications. But existing image encryption mechanisms fail to provide better image security and sometimes proved to be breakable or hackable. The security of a recently published image encryption scheme based on a compound chaotic sequence was studied. It was proved before that with only three images, the scheme can be broken. The attack takes less than one minute on MATLAB running on Mac OS to completely break the image encryption algorithm. [10]

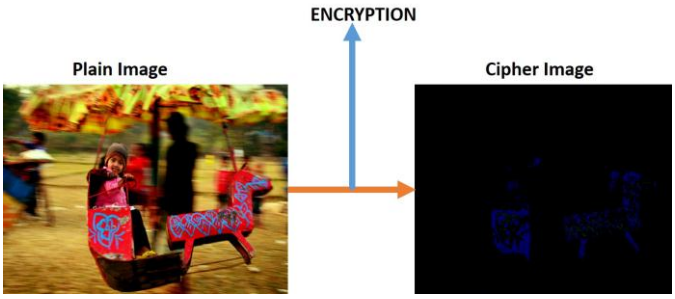


Fig 1: Image Encryption Technique

## 2. Image Encryption Issues:

Image is different from normal text data with respect to some unique characteristics of image data. Therefore, Image encryption techniques need some more additional features to be added to it that will make it different from other encryption techniques in order to make it more suitable for image encryption. A high degree of redundancy is discovered in image data and which needs fast processing. Some method provides large security but the speed becomes slow. On the other hand, some method provides great speed but not that much efficient. [4] Because of some inherent and unique features of image, classical encryption algorithms such as RSA, DES etc. are not efficient for image encryption. Especially high volume image data is a major challenge for traditional encryption algorithms. Due to bigger data volume and real-time processing requirement, algorithms that are appropriate for textual data may not be accurate for image. Each kind of data has its own features. Therefore, different techniques should be applied to make the confidential image secure from unauthorized access [6]. Since image data is far more complex and part of image is redundant, encryptions based on one-dimensional data is not much effective for image encryption. [7] The problem of image encryption is beyond the capability of established and usually used algorithms. This is primarily because of the constraints determined by the data structure and the application requirements for image, such as format compliance, complexity, real-time performance, compression efficiency, the security level and perceptibility. To address these constraints, significant attempts have been made to develop robust and advanced encryption schemes for the image data. [8]

## 2. Literature survey:

In the year of 2017, Wenting Yuan, Xuelin Yang, Wei Guo, and Weisheng Hu proposed a double-domain image encryption using hyper chaos. This paper discovered an image encryption strategy during transmission that works in both frequency domain and spatial-domain using digital hyper chaos. In the proposed encryption technique, the image was encrypted in both frequency and spatial-domain. They used XOR operation in this technique. It consists two major part: frequency domain encryption and spatial-domain encryption. This multi-level chaotic encryption was experimented and statistically verified. They focused on entropy, correlation. In their histogram, double-domain encryption had the maximum entropy value and minimum absolute value of correlation. The experimental result showed that the combination of frequency and spatial-domain encryptions increase the level of security in image encryption. But in future, the speed of transmission needs to be increased more to make it more efficient. [7]

Chengqing Li and Dongdong Lin did cryptanalyzing an image scrambling encryption algorithm of pixel bits in 2017. In this paper, they reevaluated the ISEA (Iterative Seed-Extension Algorithm) algorithm in order to find the real reasons for the attacks. It scrambles the binary representation of the gray level image by using a pseudo-random number sequence which is generated by a digital chaotic map. It uses horizontal and vertical permutation operation in this strategy. They analyzed the efficiency of ISEA with respect to some possible security attacks such as- Cipher text-Only attack, Known-Plaintext attacks, Chosen-Plaintext Attack etc. The correlation in between the multimedia data was supposed to be used to support those specific attacks. This encryption technique was able to enhance braking performance. Secret scrambling operations alone are unable to provide enough high security in order to fight against known- and chosen-plaintext attacks. Their cryptanalysis made some significant contributions to protecting multimedia data. [11]

Long Bao, Shuang Yi and Yicong Zhou introduced a (k,n)-sharing matrix S (k,n) and its generation algorithm in their paper titled "Combination of sharing matrix and image encryption for lossless (k; n)-secret image sharing" in 2016. They used mathematical analysis in order to show the potential of their approach for secret image sharing. Further, they proposed a lossless private image sharing mechanism by combining sharing matrix with image encryption. This scheme is named as SMIE-SIS. SMIE-SIS encrypts the plain image by substitution. They implemented many simulation operations with binary, grayscale and color images by using SMIE-SIS with sharing matrices to determine the robustness of this method. Their proposed method was able to achieve lossless secret image sharing for various types of images. SMIE-SIS was proved to have excellent performance considering distortion analysis, pixel expansion and computation cost. It has high level of security to deal with the brute-force attack, differential attack and it has the ability to detect the fake share by using a verification function. On the other hand, the computational cost is much higher which needs to be reduced in future. [12]

In 2017, Huiqing Huang and Shouzhi Yang introduced a novel method for encrypting color image using the logistic map and double random-phase encoding. They used a logistic map to diffuse the color image. Then the R, G, B components of the color image were scrambled by replacement of the color matrices using logistic map. They converted the three scrambled image into one encrypted image by utilizing double random phase encoding. Some numerical simulations were performed to examine the proposed encryption algorithm for one image. It was proved that the encrypted image was totally different. It does not disclose any information about the original image. It was observed that the proposed color image encryption algorithm was secure enough to fight with resisting brute-force attack. It has the largest key space. With some testing, it was shown that this method can decrypt the original image even if the image is destroyed or damaged somehow. That

means this algorithm has robustness. This encryption scheme can also resist the differential attack. For encrypting the original color image, they used XOR operation, fully phase encoding and pixel scrambling techniques. It can prevent the loss of data. But the key space is large so the key generation will be a complex one and time-consuming. [13]

In 2016, A multiple-image encryption method that is based on a modified logistic map algorithm, compressive ghost imaging, and coordinate sampling is proposed. [14] In this method, first the random phase-only mask was generated with the modified logistic map. By using the 2D discrete cosine transformation, multiple secret images were spared. These images were scrambled by different random sequences. Then the scrambled images were combined into one image with the use of coordinate sampling matrices. This image was put on the object plane of the Compressive ghost imaging system. The cipher image was obtained from the buck detection algorithm and transmitted to the receiver. To check the feasibility of the proposed scheme, computer simulations were carried out. The main outcome of this above approach was to be able of encrypting multiple images at the same time which is a unique feature of the system. The combination of compressive ghost imaging and modified logistic map algorithm can compress and decrease the data volume of the cryptosystem as well as it can increase significantly the efficiency of data transmission.

Hongjun, Abdurahman Kadir and Xiaobo Sun (2017) proposed another chaos based color image encryption method. The highlight of this scheme is to apply randomly sampled noise signal for serving as the initial value of the chaotic system. They got one time initial value from the 256-bit hash value of noise. In this approach, they only performed exclusive or (XOR) operation. This operation was applied to diffuse the pixels of the image. Some specific measures were taken to speed up the encryption technique. To measure the reliability and efficiency of the approach, they performed some statistical tests in terms of complexity and security. The proposed method uses 256-bit external key H. This key is the common hash value that is calculated by SHA-256 algorithm. The input of this scheme was a plain color image with a size of W × H. It was with randomly sampled noise signal N. The output is the cipher color image with the same size W x H. This method used some time saving operations to improve the speed of encryption. It effectively determined iterative times according to image size, faster integer operation, the exact amplification factor of state variables, matrix calculation, and pre allocated memory. The experimental results proved the effectiveness of the proposed color image encryption scheme. This intensity of the algorithm can easily be increased by replacing SHA-256 with other hash functions with more bits such as SHA-384 SHA-512 etc. [15]

The summarization of the above methods are shown in the following table:

| Name | Method | Outcomes | Limitations |
|---|---|---|---|
| A Double-Domain Image Encryption Using Hyper Chaos | • Hyper digital chaos<br>• XOR operation | • Highest Entropy<br>• High Security<br>• Efficiency | • Need to increase transmission speed. |
| Cryptanalyzing an Image Scrambling Encryption Algorithm of Pixel Bits | • ISEA algorithm<br>• Vertical and Horizontal permutation. | • Fight against specific attacks.<br>• Enhance performance | |
| Combination of sharing matrix and image encryption for lossless (k; n)-secret image sharing | • Secret image sharing scheme (SMIE-SIS).<br>• Chaotic-based encryption. | • Excellent overall performance.<br>• Ability to resist several common attacks. | • Computational cost is much higher. |
| Color image encryption based on logistic mapping and double random-phase encoding | • Logistic mapping.<br>• Double random-phase encoding.<br>• XOR operation<br>• Diffusion | • Large key space.<br>• Robust<br>• Prevent data loss. | • Key generation is complex<br>• Time consuming. |
| Multiple-Image Encryption Based on Compressive Ghost Imaging and Coordinate Sampling. | • Modified logistic map algorithm.<br>• Compressive ghost imaging<br>• Coordinate sampling<br>• Discrete cosine transformation (DCT) operation | • Multiple images encryption and decryption.<br>• Efficient.<br>• Decrease data volume. | • Feasibility needs to be improved. |
| Chaos-based fast color image encryption scheme with true random number keys from environmental noise. | • Exclusive OR<br>• Chaotic color image encryption. | • Running speed is effectively improved.<br>• Effective<br>• Fast | • Encryption intensity needs to be improved. |

## 3. CONCLUSIONS

In the above survey, some of the major color image encryption techniques were analyzed to understand the methods used and the outcome they achieved. We also tried to find out some future works and challenges that needs to be given more attention. Some of the approaches focused only on some specific kind of attacks and some of them worked in general. Most of the techniques tried to enhance the efficiency of the encryption technique for color image. In future, more importance should be given to the transmission speed of the encrypted image. On the other hand we should also focus on the fact that, the encryption technique should protect against all the possible attacks rather than concentrating on specific type of attack.

## REFERENCES

[1] Jeyanthi, N., Thandeeswaran, R. (2017). A Contemplator on Topical Image Encryption Measures. Security Breaches and Threat Prevention in the Internet of Things (chapter 9).

[2] KabirA survey on different image encryption and decryption techniques. Int Journal of Computer Science and Information Technologies. 4. 113-116.

[3] Ahmad, Jawad & Ahmed, Fawad. (2012). Efficiency Analysis and Security Evaluation of Image Encryption Schemes. IJENS. 12. 18-31.

[4] Ramandeep Kaur & Er Sumeet Kaur. (2016). A Survey on Existing Image Encryption Techniques. IJSTE International Journal of Science Technology & Engineering | Volume 2| Issue 12

[5] Ahmad, J., Khan, M.A., Ahmed, F. et al. Neural Comput & Applic (2017). https://doi.org/10.1007/s00521-017-2970-3

[6] JOLFAEI, A., & MIRGHADRI, A. (2010). An Image Encryption Approach Using Chaos and Stream Cipher.

[7] Wenting Yuan, Xuelin Yang, Wei Guo and Weisheng Hu, "A double-domain image encryption using hyper chaos," 2017 19th International Conference on Transparent Optical Networks (ICTON), Girona, 2017, pp. 1-4.

[8] Jolfaei, Alireza & Wu, Xin-Wen & Muthukkumarasamy, Vallipuram. (2015). On the Security of Permutation-Only Image Encryption Schemes. IEEE Transactions on Information Forensics and Security. 11. . 10.1109/TIFS.2015.2489178.

[9] Shanker Yadav, Ravi & Rizwan Beg, Mhd &, Manish & Tripathi, Madhava. (2013). IMAGE ENCRYPTION TECHNIQUES: A CRITICAL COMPARISON. International Journal of Computer Science Engineering and Information Technology Research (IJCSEITR). 3. 67-74.

[10] Sagade A.G, Prof. Pratap Singh. (2013) Image encryption using chaotic sequence and its cryptanalysis. IOSR Journal of Computer Engineering.

[11] C. Li, D. Lin and J. Lü, "Cryptanalyzing an Image-Scrambling Encryption Algorithm of Pixel Bits," in IEEE MultiMedia, vol. 24, no. 3, pp. 64-71, 2017.

[12] L. Bao, S. Yi and Y. Zhou, "Combination of Sharing Matrix and Image Encryption for Lossless $(k,n)$ -Secret Image Sharing," in IEEE Transactions on Image Processing, vol. 26, no. 12, pp. 5618-5631, Dec. 2017.

[13] Huang, Huiqing & Yang, Shouzhi. (2016). Color image encryption based on Logistic mapping and double random phase encoding. IET Image Processing. 11. . 10.1049/iet-ipr.2016.0552.

[14] X. Li et al., "Multiple-Image Encryption Based on Compressive Ghost Imaging and Coordinate Sampling," in IEEE Photonics Journal, vol. 8, no. 4, pp. 1-11, Aug. 2016.

[15] H. Liu, A. Kadir and X. Sun, "Chaos-based fast colour image encryption scheme with true random number keys from environmental noise," in IET Image Processing, vol. 11, no. 5, pp. 324-332, 4 2017.

## BIOGRAPHIES

Farzana Kabir did her Bachelor in Computer Science & Engineering from Chittagong University, Bangladesh. At present she is completing her Masters in Computer Science & Engineering from India. Her current research area is Image Security over Internet. She has published two research papers in International journals.

Jasmeet kaur is currently serving the A P Goyal Shimla University as Associate Professor in the Department of Computer Science & Engineering. She is having more than 8 Years of academic experience in the field of Computer Science. She has published more than 5 research papers in various International & National journals & conferences. She is the member of Board of study of Department of Computer Science & Engineering.