A Functional Review Of Image Encryption Techniques

Amnesh Goel, Dr. Rakesh Bhujade

Abstract: The prime concern of this digital era is the security [1]. As the development is making progress in various technical facilities across the world, security has risen up as the main concern. Technical development of tools and digital features are going hand in hand with the security concerns. In the era, the people residing in urban areas are more tend to technology, mobile, internet, and other commonly available facilities and these facilities also opening doors of theft and hack in individual privacy. Usage of images has grown multifold in recent years, and in the research domain, advancements are happening in making the images more secure. In this paper, we will take a look at various technical options available to make the images secure over transportation and at rest.

Index Terms: Image Encryption, Digital Image, Encryption Key etc.

1. INTRODUCTION

At first, we will touch base few basic concepts related to the images like what is an image encryption, why we need the image encryption [2] procedures, how we do the image encryption, types of encryption etc. In the laymen terms an image encryption is the process of building a plain image in such a form that it is not readable by the human eye, also at the same time, it doesn't lose its original content. So, basically, it can be understood as the process of hiding the original information of the plain image within that image using certain processes. The process by which an image is encrypted should be well known to the receiver also, otherwise how they will convert the encrypted image into the plain image. So, image encryption helps to maintain the confidentiality of information; it ensures that image information cannot be read by anyone and it also ensures that original information cannot be tempered during transit or at rest.

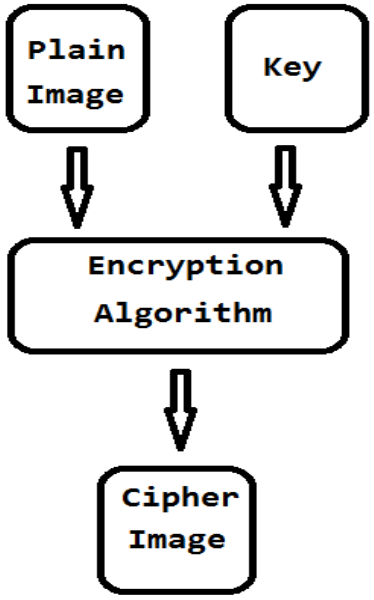

Fig 1: *Image encryption process*

Now the point is, why we need the image encryption procedures. The overall usage of the image has increased multifold in this technical era and people are using n number of mobile applications in their smartphones to not only click the good quality images but also to share it with their friends and for the official purposes. Image encryption or image security is required not only while the image is in transport towards receiver but also when it is at rest in mobile storage. If the image is not secured during storage then obviously other neighboring applications can read and process those unencrypted images which may create problems for the mobile owner. On the other hand, the images should be secure while in transport towards receiver because an intruder can hack in the network to see what is flowing and can read the messages. So, we need the strong image encryption algorithms which should be capable of making images secure at rest and during transit. To encrypt an image, we always think of a unique procedure which is harder to guess and difficult to get the original image back without following the decryption procedure. And, a strong image encryption algorithm is powered by the "key" formation. If the encryption key is not

- *Amnesh Goel is currently pursuing PhD (Computer Science and Engineering) From Mandsaur University, India, PH-08237519134. E-mail: amneshgoel7@gmail.com*
- *Dr. Rakesh Bhujade, Mandsaur University, India*

strong enough then it becomes easier to break the image encryption algorithm. In the symmetric image encryption algorithms, the key should be the same for both sender and the receiver. However, in the case of asymmetric image encryption algorithms, the sender and receivers use the different keys i.e. public and private keys. Key length and its formation procedure have a huge impact on how image encryption algorithm is going to work. The key length and algorithm strength are inversely proportional to each other. If the image encryption algorithm is built using a very short size key then it takes less time to execute and it becomes easy to break the algorithm, and on the other hand, if algorithm is having a large key space then obviously it will take a good amount of time to break the algorithm and more time to finish the execution. It is very important in image encryption domain to check the key sensitivity. Key should be very sensitive such that if there is any minor change in the key then it should not work and the intruder shouldn't get the plain image back. A good image encryption algorithm should run certain analysis on the decrypted image to validate the encryption process such as histogram analysis, correlation analysis etc.

1. LITERATURE REVIEW

Here is the review of certain image encryption algorithms that were proposed lately. In this paper, Muhammad Asim and Varun Jeoti [3] proposed a new image encryption algorithm which took fewer computations than AES (Advance Encryption Standard). The new algorithm, Chaotic Encryption Scheme (CES) is based on the 2D cat map and S-box. For this encryption scheme, the authors used a 16 characters secret key. Each character in the secret key denotes the 8-bit block of the secret key which leads to a total key of 128 bits. To start with proposed algorithm, authors created blocks of 128 bits from the plain image (a 4x4 matrix) like AES. Further, these blocks were scrambled and then random values are extracted from these blocks. S-box is used and masking is applied before and after applying the S-box values. Authors presented the Histogram analysis which shows that cipher image content is completely random. Histogram analysis is shown for different images with the key of "abcdefghijklmnop". Authors also presented the "Key sensitivity analysis" where they changed the key value during decryption. "Differential image analysis" is also performed to show that when two images are encrypted using the same key then they do not result in the same output. This encryption method is based on the Henon chaotic maps and proposed by Xin Zhang and Weibin Chen [4]. This encryption algorithm follows a two-step encryption scheme in which the original image is fused with a key image in the first step, and the fusion image is used to encrypt with Henon chaotic maps. The one thing which should be talked about is, this encryption methodology has a dependency on the key image because to complete the first step of fusion, key image size should be same as the plain image size, and otherwise, fusion cannot be completed. To support their encryption algorithm, authors performed the histogram analysis where they claim that the histogram of fusion image and cipher image are different and the histogram of cipher image is uniformly distributed as compared to the plain image. Authors claim that their encryption scheme is better and strong against the brute force attack because they use the key-image and the initial values of Henon chaotic map as their secret key combination. In this paper, ZHANG Yun-peng, ZHAI Zheng-jun, LIU Wei, NIE Xuan, CAO Shui-ping, DAI Wei-di [5] proposed a new image encryption algorithm which is based on the chaotic sequence. Generally, the Chaos-based image encryption techniques result with some deficiencies like limited accuracy problem. To overcome this problem, the authors proposed to use Improved DES along with the logistics chaos sequence number. To improve the DES efficiency, DES is performed 16 rounds of iteration as compared to its traditional 4 rounds of iteration. These 16 rounds improve the quality of the encryption process. However, more rounds also increase the computation overhead. After the encryption process, authors performed the Histogram analysis which shows the uniform distribution of pixels in the cipher image as compared to the plain image. Authors also performed the correlation between the adjacent pixels to see if pixels in the cipher image is correlated or not. A low value of correlation coefficient indicates that pixels in the cipher image are not correlated. In this encryption algorithm, Feng Pan, ChuanCai Wang, XiaoNan Chen [6] used Discrete Wavelet Transform (DWT) and the image is divided into smaller blocks. In the beginning, a subband of DWT coefficient is analyzed. These DWT coefficients are used to compute the complexity of each block of the image. Each block is then encrypted using corresponding intensity according to different complexity. DWT is basically a new theory which is widely used in signal processing space and in this case, DWT is used to decompose the image into different space and to find the frequency of sub-image. This process helps to get the image energy in different aspects like low-frequency LL, energy in horizontal LH, vertical HL, and diagonal HH. This process aims to get detail information about the image. Authors study says that low-frequency energy space is used to scramble the image but sometimes high-frequency space is also used as per the need. After finding out the detail information about the image, chaotic image encryption method was used to shuffle the pixels at row and column level. Authors took one sample image and divided it into the blocks of 32x32. Authors presented the relationship between the variance of the high-frequency coefficient and the image complexity. Authors did not perform any kind of statistical analysis to support their results. In this paper, Manjunath Prasad, K.L.Sudha [7] proposed to use the encryption algorithm which is based on the pixel shuffling within the image and employ the Henon Map and Lorentz. Authors suggested to first pull out the R, G and B component of an image into a separate 1D array. Then these 3 1D arrays are used to encrypt using the Henon Map. Authors repeated the same procedure with the Lorentz Map technique. After applying the Henon or Lorentz map, authors sorted the arrays and stored the index values. Authors presented the results by using two different images. In this paper, authors did not discuss the size of the key and how it used at the encryption end or at the decryption end. Authors performed the Correlation analysis to show that pixels in the cipher image (R, G, and B separately) are not correlated with each other. Same Correlation is calculated for cipher image obtained by Lorentz map technique also. Key sensitivity analysis is also performed on the results and it was found that, if the key has very minor changes then it is not possible to get the

plain image back. In this paper, ROHITH S, K N HARI BHAT, A NANDINI SHARMA [8] proposed an image encryption scheme which is based on the Logistic map technique. This image encryption algorithm basically depends on the grayscale component of the image and doesn't deal with the color image. If we extract the grayscale image from a color image then obviously we will lose the image content. Hence, this is not used for color images. In the first step of encryption, the whole image pixels are converted into a 1D array of pixels and each pixel value which ranges between 0-255 is converted into its binary equivalent of 8 bit. These image pixels are XOR with a key to get the encrypted pixel. This XOR operation is then performed on all the pixels in the image to get the cipher image. Authors then performed the Histogram analysis, Mean Square Error analysis, Entropy Analysis, and Correlation Analysis to support their results. And from these analyses, the authors claim to have a secure image encryption algorithm. However, still authors could employ image encryption algorithm on the color images as these days, uses of grayscale images are very minimal. In this paper, Jean De Dieu Nkapkop, Joseph Yves Effa, Monica Borda, Laurent Bitjoka, Alidou Mohamadou [9] proposed an image encryption scheme in which they used the Chaotic Logistic Map but the sequence of this map they used in the descending order. In this paper, all the pixels are not diffused using the same keystream, only the first pixel is diffused with the main key stream and for the subsequent pixels, key stream + previous pixel values are used to diffused the following pixel. Authors performed the Confusion step in which pixels are scrambled over the entire image without changing their values and authors claim that using this step, the image becomes unrecognizable. And, in the diffusion step, different chaotic algorithms are employed like key Tent map and Logistic map. Authors performed the Histogram analysis on the cipher image and found that the pixels in the cipher image have approximately a uniform distribution. Authors calculated the entropy for the cipher image and they found that entropy value is 7.9996 which is very close to ideal entropy value of 8. Authors proposed to use a 256-bit keyspace for this algorithm. Correlation analysis is performed on the adjacent pixels of the cipher image and it was found that adjacent pixels are not correlated in the cipher image. Authors performed the Key sensitivity analysis in which the authors changed the original key and decrypted the cipher image. During this analysis, they saw that they did not get the plain image back even if there is a slight change in the Key. This image encryption system is powered with use of spatial domain watermark images and proposed by Ali Al-Haj, Hiba Abdel-Nabi [10]. This spatial domain watermark image is embedded in the plain image using the Histogram Shifting RDH method. This will generate the partial encrypted image. Pixel permutation is done on this encrypted image. Now, authors used another spatial domain watermark image to encrypt this encrypted image using RDH Histogram shifting method. Authors then combined two images i.e. watermarked image and the encrypted watermarked image of 8-bit planes to generate 16-bit planes. In this paper, authors did not discuss the details of the pixel permutation step. Also, the key details are not discussed in this paper. Authors did not present any result in this paper, however, they presented the Peak Signal to Noise Ratio Analysis on the plain image and the cipher image. The overall presentation of this paper is weak and the content is not well written.

1. CONCLUSION

In this paper, we discussed various image encryption algorithms that were proposed lately. These algorithms have different implementations but aim to make image encryption stronger. However, as we discussed in the introduction section, the very important aspect of image encryption algorithm is its key and we have included the key aspect of these papers here.

REFERENCES

[1] HTTPS://EN.WIKIPEDIA.ORG/WIKI/SECURITY.
[2] https://en.wikipedia.org/wiki/Encryption.
[3] Muhammad Asim, Varun Jeoti, "On Image Encryption: Comparison between AES and a Novel Chaotic Encryption Scheme" IEEE - ICSCN 2007, MIT Campus, Anna University, Chennai, India. Feb. 22-24, 2007. pp.65-69.
[4] Xin Zhang and Weibin Chen, "A New Chaotic Algorithm for Image Encryption" 2008 IEEE International Conference on Audio, Language and Image Processing.
[5] ZHANG Yun-peng, ZHAI Zheng-jun, LIU Wei, NIE Xuan, CAO Shui-ping, DAI Wei-di, "Digital Image Encryption Algorithm Based on Chaos and Improved DES" Proceedings of the 2009 IEEE International Conference on Systems, Man, and Cybernetics San Antonio, TX, USA - October 2009.
[6] Feng Pan, ChuanCai Wang, XiaoNan Chen, "An Image Encryption Scheme Based on Image Complexity" 2010 IEEE International Conference on Information Theory and Information Security.
[7] Manjunath Prasad, K.L.Sudha, "Chaos Image Encryption using Pixel shuffling", D.C. Wyld, et al. (Eds): CCSEA 2011, CS & IT 02, pp. 169–179, 2011.
[8] ROHITH S, K N HARI BHAT, A NANDINI SHARMA, "Image Encryption and Decryption using Chaotic Key Sequence Generated by Sequence of Logistic Map and Sequence of States of Linear Feedback Shift" 2014 International Conference on Advances in Electronics Computers and Communications.
[9] Jean De Dieu Nkapkop, Joseph Yves Effa, Monica Borda, Laurent Bitjoka, Alidou Mohamadou, "A Secure and Fast Chaotic Encryption Algorithm Using the True Accuracy of the Computer" Informatica 40 (2016) 437–445.
[10] Ali Al-Haj, Hiba Abdel-Nabi, "Digital Image Security Based on Data Hiding and Cryptography" 2017 IEEE 3rd International Conference on Information Management 978-1-5090-6306-2/17 © 2017.