IOSR Journal of Computer Engineering (IOSR-JCE)
e-ISSN: 2278-0661, p- ISSN: 2278-8727Volume 16, Issue 3, Ver. III (May-Jun. 2014), PP 108-111
www.iosrjournals.org

Analysis and Implementation of Selective Image Encryption Technique Using Matlab

[1]Upendra Bisht, [2]Shubhashish Goswami
[1]M.Tech (CSE) student, DBIT, Dehradun
[2]Asst. Prof., HOD IT/CS Dept. DBIT, Dehradun

Abstract: *Encryption plays a very significant role in secure transmission of digital images from one place to another. There are a number of encryption algorithms available which perform the task of encryption. However some algorithms are fully layered which perform the encryption of the whole content of the images. But sometimes there is a requirement of partial image encryption so that there is reduced execution time and hence increases in performance. This type of partial image encryption can be achieved through Selective image encryption technique. This paper aims to propose an analysis and implementation of Selective image encryption technique using Matlab.*

Keywords: *encryption, partial image encryption, selective image encryption, matlab*

I. Introduction

An image may be defined as a two-dimensional function(x, y) where x and y are spatial coordinates and the amplitude of 'f' at any pair of coordinates(x, y) is called the intensity or gray level of the image at that point. When x, y and the intensity values of f are all finite, discrete quantities, we call the image a digital image. Digital image processing refers to processing digital images by means of a digital computer. A Digital image is composed of a finite number of elements each of which has a particular location and value. These elements are called picture elements, pels and pixels.

In today's fast moving world where millions of images are transmitted in seconds all over the world, the security of images is a burning issue. Encryption is a solution to the security concern of transmitted images. The security of image can be achieved by various types of encryption schemes. Different chaos based and non-chaos based algorithms have been proposed. Among this the chaotic based methods are considered to be more promising. The chaotic image encryption can be developed by using properties of chaos including deterministic dynamics and unpredictable behaviour. There are three kinds of encryption techniques namely substitution, transposition or permutation and techniques that include both transposition and substitution. Substitution schemes change the pixel values while permutation schemes just shuffle the pixel values based on the algorithm. In some cases both the methods are combined to improve security.

In selective encryption some content of the image is encrypted. It reduces the execution time because it encrypts only a part of the image. Consequently, selective encryption is sometimes called partial encryption. This algorithm provides security to the image and in the same time, some part of the image is visible. Nidhi et.al , proposed a selective encryption technique in wavelet domain for conditional access systems. This encryption is applied only to a subset of multimedia data stream rather than the multimedia data in its entirety to save the computational time and computational resources, thus controlling the transparency of the multimedia data at the time of encryption. Gaurav Bhatnagar , presented a simple selective encryption technique based on Saw-Tooth space filling curve, pixels of interest, non-linear chaotic map and singular value decomposition. The core idea of this algorithm is to scramble the pixel positions by the means of Saw-Tooth space filling curve followed by the selection of significant pixels using pixels of interest method. Then the diffusion process is done on the significant pixels using a secret image key obtained from non-linear chaotic map and singular value decomposition. Priyanka Agrawal and Manisha Rajpoot explained a concept where important part of the image that can efficiently achieve by conceptually selecting the part of the image which is further used in its normal mode of operation for encryption. Once encryption is done, the encrypted data is sent along with remaining original part of the message, ensuring its secured transmission and distribution over public networks.

The proposed paper aims to provide a selective encryption technique for easy and fast partial encryption of images using matlab. This paper has been divided into five sections. First section contains Introduction, second section contains description of Selective Image Encryption technique, third section contains proposed Selective image encryption technique using matlab, fourth section contains Results and Discussion and fifth section contains conclusion.

II. Selective Image Encryption Technique

The general selective encryption mechanism works as follows. The image is first compressed (if needed). Afterwards the algorithm only encrypts part of the bit stream with a well-proven ciphering technique; incidentally a message (a watermark) can be added during this process. To guarantee a full compatibility with any decoder, the bit stream should only be altered at places where it does not compromise the compliance to the original format. This principle is sometimes referred to as format compliance. WEN et al. [] have recently described a general framework for format-compliant encryption. In their simulations, they focus on MPEG-4 video error resilient mode with data partitioning and discuss which fields can be encrypted. They also pointed out that the encryption of a variable length code (VLC) code word may not result in another valid code word.

With the decryption key, the receiver decrypts the bit stream, and decompresses the image. In principle, there should be no difference between a decoded image and an image that has been encrypted and decrypted. However there might be a slight though invisible difference if a watermark message has been inserted in the image. This process of selective encryption technique is depicted in figure 2.

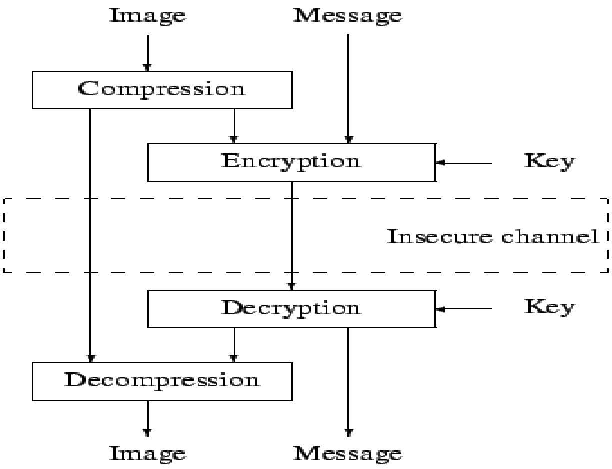
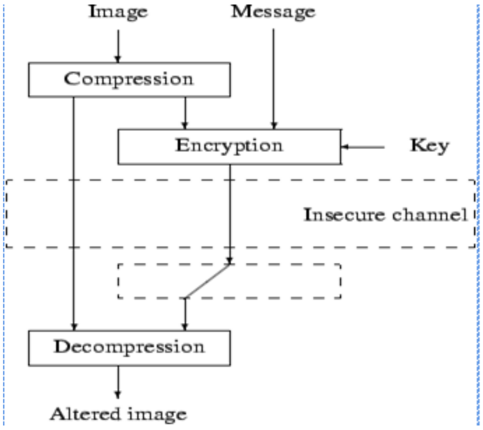


Figure 2: Selective image encryption mechanism.

When the decrypting key is unknown, the receiver will still be able to decompress the image, but this image will significantly differ from the original. This scenario is depicted in Figure 3.



III. Proposed Selective Image Encryption Technique using matlab

This paper describes the selective image encryption technique using matlab. The steps involved in this encryption technique are depicted in figure.4

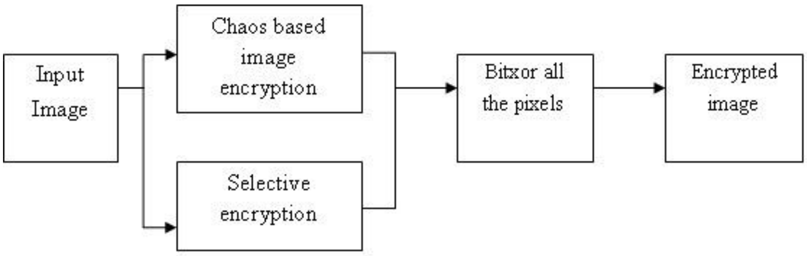


Figure 4 Proposed Selective Image Encryption technique

Algorithm of proposed selective image encryption technique using matlab is as follows:
Step1: Input any coloured image (which contains R, G, B pattern)
Step 2: R, G, B pattern will be in the form of matrix. Save this matrix in a variable.
Step 3: In this algorithm the technique of confusion and diffusion is used which means that each pixel of the input image is replaced by another value. The value will be generated by random number generator ex. Henon function, Lorentz function etc
Step 4: After generating the random numbers, those random numbers will be XORed with the original image pixels.
Step 5: The output will be an encrypted image.

IV. Results and Discussion

Input image, Encrypted image and Final image are shown in the figure 5. These images have been the input and output of executing the proposed selective image encryption technique in matlab.

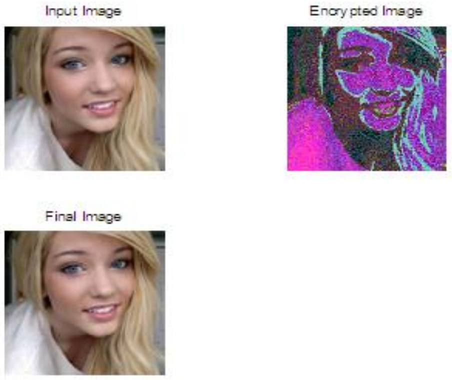


Figure 5. Input and Output of executing proposed selective image encryption technique in matlab Histograms of respective images being used in the proposed selective encryption technique are shown in Figure 6.

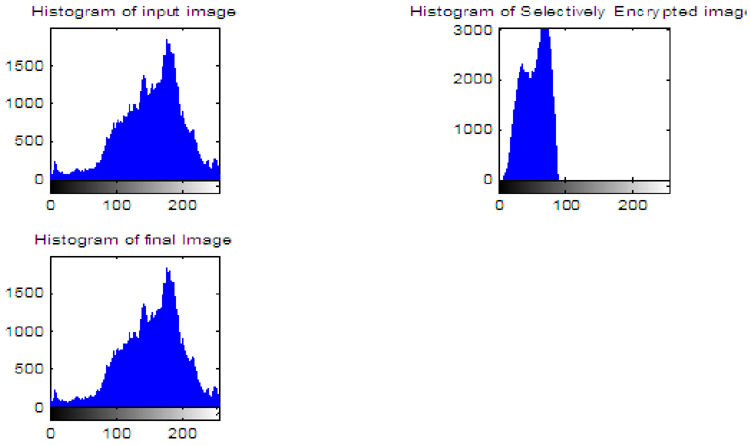


Figure 6.Histograms of respective images

As we can see from the input image and encrypted image of figure 5, the proposed selective image encryption algorithm has been successful in encrypting the image and the final image is similar to the input image proving that the algorithm has also been successful in decrypting it correctly.

V. Conclusion

In this paper we have presented an analysis and implementation of selective image encryption algorithm using matlab. The technique proposed in this paper is easy to understand and can easily be implemented through matlab. This technique can be very useful in various fields of life where partial encryption is required.

References

[1]. Nidhi S Kulkarni, Balasubramanian Raman, and Indra Gupta, "Selective encryption of multimedia images", NSC 2008, December 17-19, 2008.

[2]. Gaurav Bhatnagar , Q.M. Jonathan Wu, Selective image encryption based on pixels of interest and singular value decomposition, Digital Signal Processing 22 (2012) 648–663.

[3]. Priyanka Agrawal and Manisha Rajpoot A Fast and Secure Selective Encryption Scheme using Grid Division Method, IJCA vol.51 no.4,pp 29-33, Aug -2012.

[4]. Panduranga H T et al. / International Journal of Engineering and Technology (IJET) "Selective Image encryption for medical and satellite images".

[5]. Marc Van Droogenbroeck and Raphaël Benedett "Techniques for a selective encryption of uncompressed and compressed images".

[6]. Rafael_C._Gonzalez,_Richard_E._Woods,_Steven_L._E "Digital image processing".