International Journal of Science and Research (IJSR)
ISSN (Online): 2319-7064
Impact Factor (2012): 3.358

Image Cryptography Based Upon Scrambling and Random Integer

Gurpreet Singh[1], Lovleen Kaur[2]

[1]BFCET Deon (Bathinda), Punjab, India
[2]BFCET Deon (Bathinda), Punjab, India

Abstract: ***In this research work chaotic system is implemented for encryption of images. That is confusion and diffusion is implemented in all multi levels of cryptography. Cryptography means to change the sense i.e. decoding from one form to another. In first level pixels are scrambled row wise by a step of two and in second level pixels are shifted column wise by a step of two. All rows and columns are not shifted as it would generate same image upside down. The third level implements confusion as in this pixels are arranged in increasing level of their intensities. The fourth level implements diffusion as at this level random integer function is used to generate new intensity values for the pixels. In the same way these can be decrypted by following these steps to get the original form.***

Keywords: Encryption, Decryption, cryptography, correlation coefficient

1. Introduction

In the modern era, information security is becoming more important in data storage and transmission. Images are widely used in several processes. Therefore, the protection of image data from unauthorized access is important. Image encryption plays a significant role in the field of information hiding. Hiding is giving the reasons for encryption. Image hiding or encrypting methods and algorithms range from simple spatial domain methods to more complicated and reliable frequency domain ones. It is argued that the encryption algorithms, which have been originally developed for text data, are not suitable for securing many real-time Multimedia applications because of large data sizes. Software implementations of ciphers are usually too slow to process image and video data in commercial systems. Hardware implementations, on the other hand, add more cost to service providers and consumer electronics device manufacturers. A major recent trend is to minimize the computational requirements for secure multimedia distribution by "selective encryption" where only parts of the data are encrypted. There are two levels of security for digital image encryption: low level and high-level security encryption. In low-level security encryption, the encrypted image has degraded visual quality compared to that of the original one, but the content of the image is still visible and understandable to the viewers. In the high-level security case, the content is completely scrambled and the image just looks like random noise. In this case, the image is not understandable to the viewers at all. Selective encryption aims at avoiding the encryption of all bits of a digital image and yet ensuring a secure encryption. The key point is to encrypt only a small part of the bit stream to obtain a fast method. Network security and image encryption has become important and high profile issues. Most traditional or modern cryptosystems have been designed to protect textual data. An original important and confidential plaintext is converted into cipher text that is apparently random nonsense. Once the cipher text has been produced, it is saved in storage or transmitted over the network. Upon reception, the cipher text can be transformed back into the original plaintext by using a decryption algorithm.

However, images are different from text. Although we may use the traditional cryptosystems (such as RSA and DES-like cryptosystems) to encrypt images directly, it is not a good idea for two reasons. One is that the image size is much greater than that of text, so the traditional cryptosystems need much time to directly encrypt the image data. The other problem is that the decrypted text must be equal to the original text. However, this requirement is not necessary for image.

2. Encryption Process

We use multi level cryptography. Cryptography is the art and science of writing in secret codes. A general cryptographic system includes two processes further in it to work:

a) Encryption
b) Decryption

In encryption we encrypt the image to make it to unreadable form for secure transmission and information hiding and in Decryption we restore back the image to its original form. A number of techniques are available for encryption, what we are using is multi level encryption and decryption by shifting the rows and columns.

3. Implementation of Proposed Algorithm

Let's have a look upon proposed algorithm in detail from which we can clarification that how the proposed technique works.

Step 1.Read the color image I m*n, where m and n is the height and width of image respectively
Step 2.Scramble the image by shifting half of the rows column wise by a step of two at first level of encryption.
Step 3.scramble the image by shifting half of the columns, row wise by a step of two at second level of encryption.
Step 4.Convert the image to one dimensional array sort the pixels in increasing order of intensity at third level of encryption.

Step 5.Replace pixel's intensity value by adding one to the values generated by the random integer function at fourth level of encryption. Decryption process is the inverse of encryption process.

Correlation Coefficient is also known as Pearson's correlation coefficient r. It is widely used in statistical analysis, pattern recognition and image processing. Other applications include comparing two images for the purposes of image registration, object recognition and disparity measurement.

The correlation coefficient is defined as:

$$r_{xy} = \frac{\text{cov}(x, y)}{\sqrt{D(x)}\ \sqrt{D(y)}}$$

Where x and y are grey scale values of two adjacent pixels in the image. In numerical computations following formulas are used:

$$E(x) = \frac{1}{N}\sum_{i=1}^{N} x_i$$

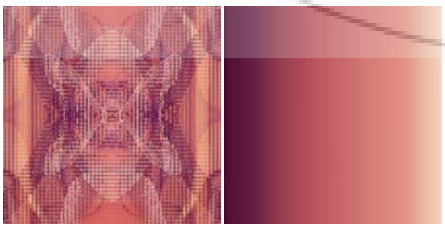
$$D(x) = \frac{1}{N}\sum_{i=1}^{N}(x_i - E(x))^2 \quad \text{Con}(x,y) = \frac{1}{N}\sum(x_i - E(x))(y_i - E(y))$$

The correlation coefficient has the value r=1, if the two images are absolutely identical r=0 if they are completely uncorrelated and r=-1 if they are completely anti-correlated.

4. Results and Analysis

In this paper experimental analysis of the proposed algorithm as been done with a color image and MATLAB 7 is used to realize the algorithm. Simulation results are shown as Figure.

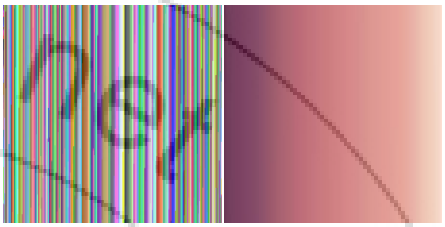
(a) (b)



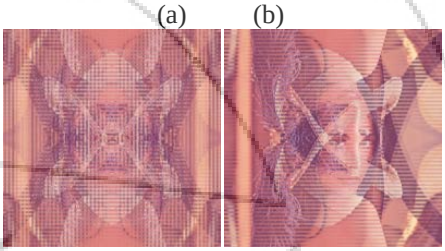
(c) (d)

(e)

Figure 1: Encryption images: (a) Original image (b) Scrambled image at level1 (c) Scrambled image at level 2 (d) Scrambled image at level 3 (e) Multi level encrypted image



(a) (b)



(c) (d)

(e)

Figure 2: Decryption images: (a) Encrypted image (b) Decrypted image at level2 (c) Decrypted image at level 3 (d) Decrypted image at level 4 (e) Original image

Histogram analysis: To prevent the leakage of information to an opponent, it is also advantageous if the cipher image bears little or no statistical similarity to the plain image. An image histogram illustrates how pixels in an image are distributed by graphing the number of pixels at each color intensity level. We have calculated and analyzed the histograms of the several encrypted images as well as its original images that have widely different content. The histogram of the cipher image as shown in same fig, significantly different from that of the original image, and bears no statistical resemblance to the plain image.

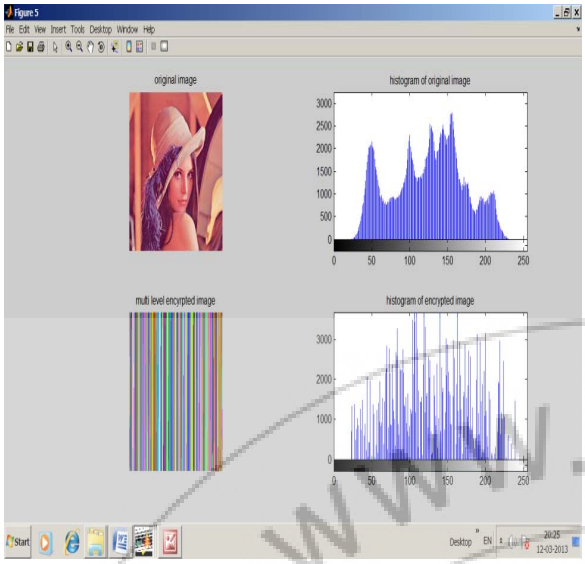


Figure 3: Different Histogram for original and encrypted image

5. Conclusion

In this paper it is proposed that multi level image cryptography to securely encrypt the images for the purpose of storing images and transmitting them over the Internet. There are two major advantages associated with this system. The first advantage is that it makes the encrypted image with a constant increasing intensity. The second advantage is that it does not impose any restriction on the decoding of the specific image signal because with every new image signal it produces a new hash accordingly. Our system would be systematically evaluated, and it shows a high level of security with excellent image quality.

6. Future Work

In future we can extend this method by making it more fast by reducing the random integer generation time. Moreover we can introduce diagonal interchanging to enhance more secure cryptography. Compression of the keys can be done to reduce overhead.

References

[1] Ravishankar, K. C. and Venkateshmurthy, M. G., "Region Based Selective Image Encryption", ieee, pp.1-6, 2006.
[2] Zhang, Y. P., Zhai, Z. J., Liu, W. X., "Digital Image Encryption Algorithm Based on Chaos and Improved DES", ieee international conference on systems, man and cybernetics, pp.474-479, 2009.
[3] Lin Q. H., Yin, F. L., and Zheng, Y. R., "Secure Image Communication Using Blind Source Separation", ieee 6th cas symp.on emerging technologies, pp.261-264, 2004.
[4] Paul, A. J., Mythili, P. and Jacob, K. P., "Matrix Based Cryptographic Procedure for Efficient Image Encryption", ieee, pp.173-177, 2011.
[5] Xiang, F., and Cong, G. X., "An Image Encryption Algorithm Based on Scrambling and Substitution Using Hybrid Chaotic Systems", ieee seventh international conference on computational intelligence and security, pp.882-885, 2011.
[6] Menon, N. A., Gilani, S. A. M., and Ali, A., "Watermarking of Chest CT Scan Medical Images for Content Authentication", ieee, 2009.
[7] Yu, H., Zhu, Z., and Chen, G., "An Efficient Encryption Algorithm Based on Image Reconstruction", ieee international workshop on chaos-fractals theories and applications, pp.200-204, 2009.
[8] http://www.apprendre-en-ligne.net/crypto/bibliotheque/PDF/Kwang.pdf
[9] http://www.mathworks.in/help/techdoc/matlab_prog/f2-43934.html
[10] Nien, H. H., Huang, W. T., Hung, C. M., Chen, S. C., Wu, S. Y., Huang, C. K., and Hsu, Y. H., "Hybrid Image Encryption Using Multi-Chaos-System", ieee, icics, 2009.
[11] Kuang, L. Q., Zhang, Y., and Han, X., "A Medical Image Authentication System Based on Reversible Digital Watermarking", ieee, 2009.
[12] Kamali, S. H., Shakerian, R., Hedayati, M., and Rahmani, M., "A New Modified Version of Advanced Encryption Standard Based Algorithm for Image Encryption", ieee iceie, vol.1, pp.vi-141-vi-145, 2010.
[13] Wang, R. Z., and Hsu, S. F., "Tagged Visual Cryptography", ieee signal processing letters, vol.18, no.11, 2011.
[14] Wu ,D.W., and Tsai, W. H., "Data Hiding in Images Via Multiple Based Number Conversion and Lossy Compression", ieee transactions on consumer electronics, vol. 44, no. 4, 1998.
[15] Dutta, A., Sen, A. K., Das, S., Agarwal, S., and Nath, A., "New Data Hiding Algorithm in MATLAB Using Encrypted Secret Message", ieee international conference on communication systems and network technologies, pp.-262-267, 2011.
[16] Loukhaoukha, K., Chouinard, J. Y. and Berdai, A., "A Secure Image Encryption Algorithm Based on Rubik's Cube Principle", journal of electrical and computer engineering, vol. 2012, article id 173931, pp – 13, 2012.
[17] Schyndel, R. G., Tiekel, A. Z.and Svalbe, I .D., "Key Independent Watermark Detection", ieee, pp.580-585, 1999.
[18] Xiaolin, X., and Jiali, F., "Research and Implementation of Image Encryption Algorithm Based on Zigzag Transformation and Inner Product Polarization Vector", ieee international conference on granular computing, pp.556-561, 2010.
[19] Cheng, H., and Li, X., "Partial Encryption of Compressed Images and Videos", ieee transactions on signal processing, vol. 48, no. 8, 2000.
[20] Kang, I., Arce, G. R., and Lee, H. K., "Color Extended Visual Cryptography Using Error Diffusion", ieee transactions on image processing, vol. 20, no. 1, 2011.
[21] Tseng, Y. C. and Pan, H. K., "Data Hiding in 2-D Color Images", ieee transactions on computers, vol. 51, no. 7, 2002.
[22] Liu, F. and Wu, C. W., "Embedded Extended Visual Cryptography Schemes", ieee transactions on information forensics and security, vol. 6, no. 2, 2011.

Author Profile

Gurpreet Singh was born in Punjab, India in 1989. He has done his B-Tech. from P.T.U. Jalandhar. Presently, he is pursuing M-Tech. from PTU Jalandhar. His main Research interests are in image processing.