ISSN 1533-9211

DOI 10.5281/zenodo.7302482

HIGH-SPEED SECURE ARMY COMMUNICATION EMPLOYING RANDOM SHUFFLE CRYPTOGRAPHY IN IMAGE PROCESSING

SHEREEN. S. JUMAA

Al-Farahidi University, College of Technical Engineering, Baghdad, Iraq

ABSTRACT:

As advanced encryption becomes more extensively used in technological products and social messaging apps. The terrorists are using technology to communicate and store information in a secure manner. Legislation to aid law enforcement authorities in dealing with the problem of "going dark" would, on the other hand, never result in a return to the status quo. According to counterterrorism officials, terrorist groups are increasingly using encryption to communicate securely. In today's world, when data is transmitted via the internet, information security has turned a critical component of all topics of human life. Unauthorized access is possible because information is transmitted through a network. Image encryption is one method for safeguarding prints sent over the internet. The current study aimed to add to the general body of knowledge in the field of cryptography implantations and by developing an algorithm for image encryption by using random shuffle the pixel values. Finally, the algorithm allows for the fast and secure encryption and decryption of images based on pixel location. The algorithm was created using MATLAB.

1) INTRODUCTION:

Information security has grown to be a significant concern in the modern day because our lives are dependent on technology and the interchange of information [1]. This data can be presented in a diversity of ways, including text, photos, video, and audio [2]. Additionally, photographs specifically have a wide range of uses in a variety of sensitive contexts, including, among others, medical, military, and personal data [3]. For this reason, researchers are working to safeguard the security of photos when they are sent across multiple communication channels and to stop any potential hacker attempts. Three separate techniques encryption, steganography and watermarking can be used to secure data. One of the first widely used techniques for information security was encryption [4]. Ancient Egyptians, Babylonians, and Romans all used encryption; it was used for military purposes for the first time by the Romans. Because of the larger data sizes sent by images, traditional encryption was unable to achieve its goal, necessitating a significant amount of time and computational resources. Nowadays, methods that are quicker and more effective are in demand. In fact, the encryption was already in place. It includes swap or change. In both situations, encryption is required. The same secret key is used for both encryption and decryption [5].

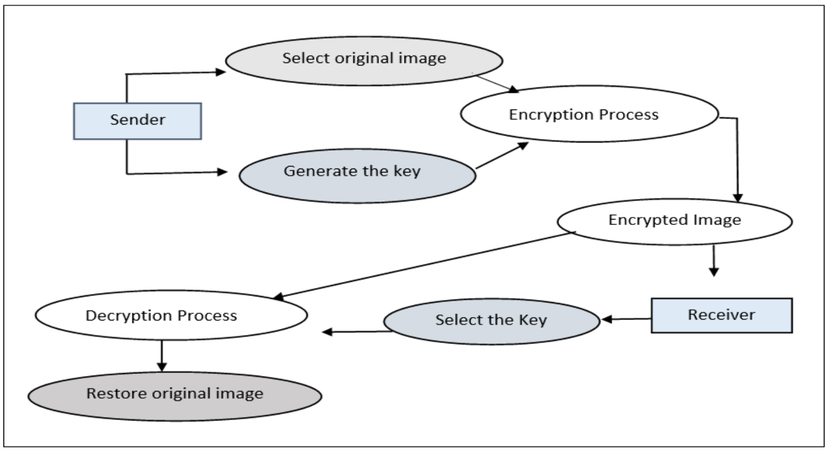
2) REVIEWS ON RELATED WORK

An advanced method for effective RGB pixel shuffling for image encryption was extinguish by Navita Agarwal. Before obtaining the cipher image, the values of the input image are retrieved using this procedure. There is no need to increase the pixel size or change the bit values with this technique. Numbers are moved from their original locations, rearranged, combined with RGB values, and distributed across the image. To generate the encrypted image, the RGB values are then exchanged. To create an encrypted image, the numerical values of an image are adjusted, shifted, and then exchanged with RGB values. The image encryption is depend on the rearrangement and shuffling of RGB pixels. The bit values of the photographs were not changed in this way. Also, there is no pixel dislocation during the encryption and decryption processes. Their values have not changed in the image. To make the cipher image, numerical values from the input image were shifted about and rearranged using RGB values. RGB pixel values are swapped with their native pixel positions within the image limits. The values of pixels in the image have not changed. To create the cryptograph image, numerical values from the input image were shifted about and reordered using RGB values. RGB pixel values are modified in accordance with their native pixel positions within the image borders. Finally, the image is shifted by RGB values and RGB pixel values are modified. There are some methods that use photographs as the key [6]. Kamboji demonstrated a new technique for extracting edge information from color images with fixed threshold values. A single image serves as the key for both encryption and decoding in RGB image encryption. These procedures make use of encryption and decryption algorithms [7].

3) METHODOLOGY

Nowadays, images are commonly used to transmit information. As a result, before allocating an image to anyone, it must be encrypted. The input image is encrypted using the randomly shuffle integers technique, which splits the image into random equal pieces, which are then shuffled. That implies that the key image is utilized to encrypt the original image. Anyone with the same key image can decrypt a picture. The reverse encryption technique of decrypting a photograph. This method is ideal for encrypting 3D and color pictures. Fig. 1 shows the architecture system and how is send image and encrypted its. Fig.2 shows the image flowchart for shuffle pixel displacement encryption and in Fig.3 shows flowchart for shuffle pixel displacement decryption.

Figure 1: The architecture system



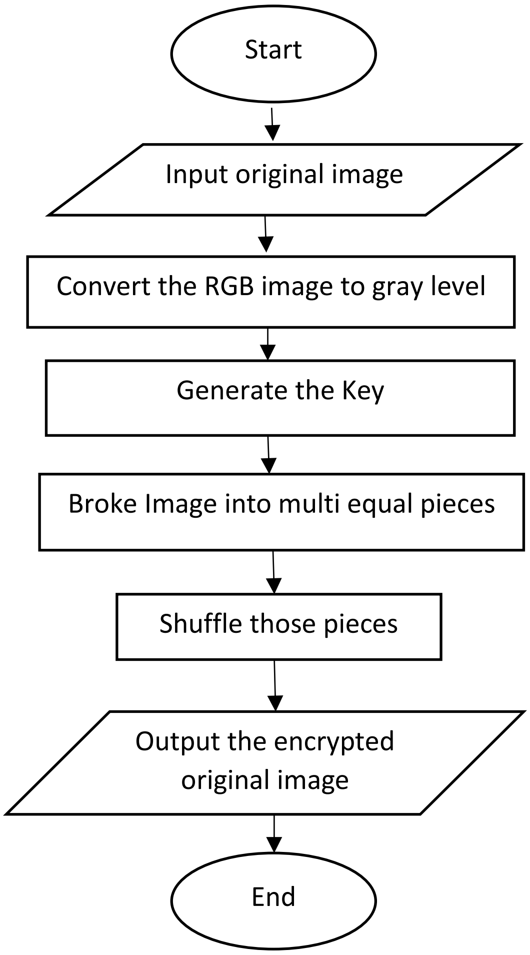

Start
Input original image
Convert the RGB image to gray level
Generate the Key
Broke Image into multi equal pieces
Shuffle those pieces
Output the encrypted original image
End

Figure 2 : The flowchart for shuffle pixel displacement encryption

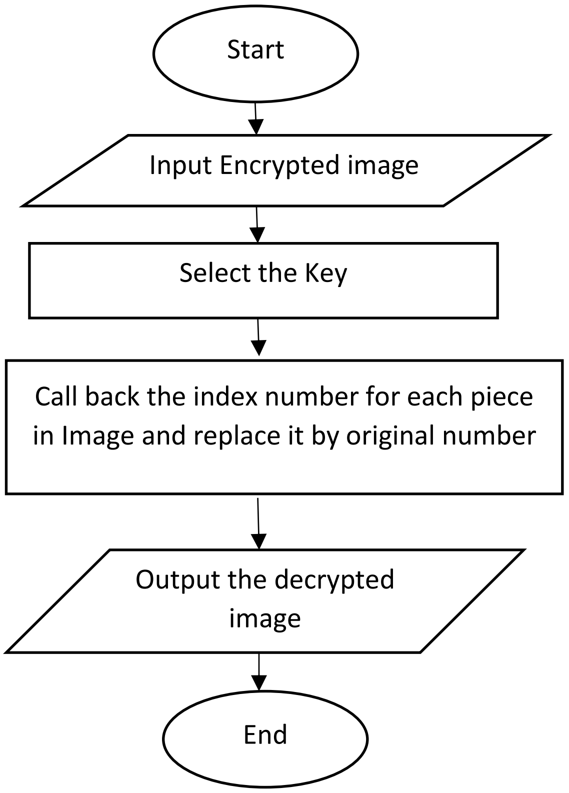
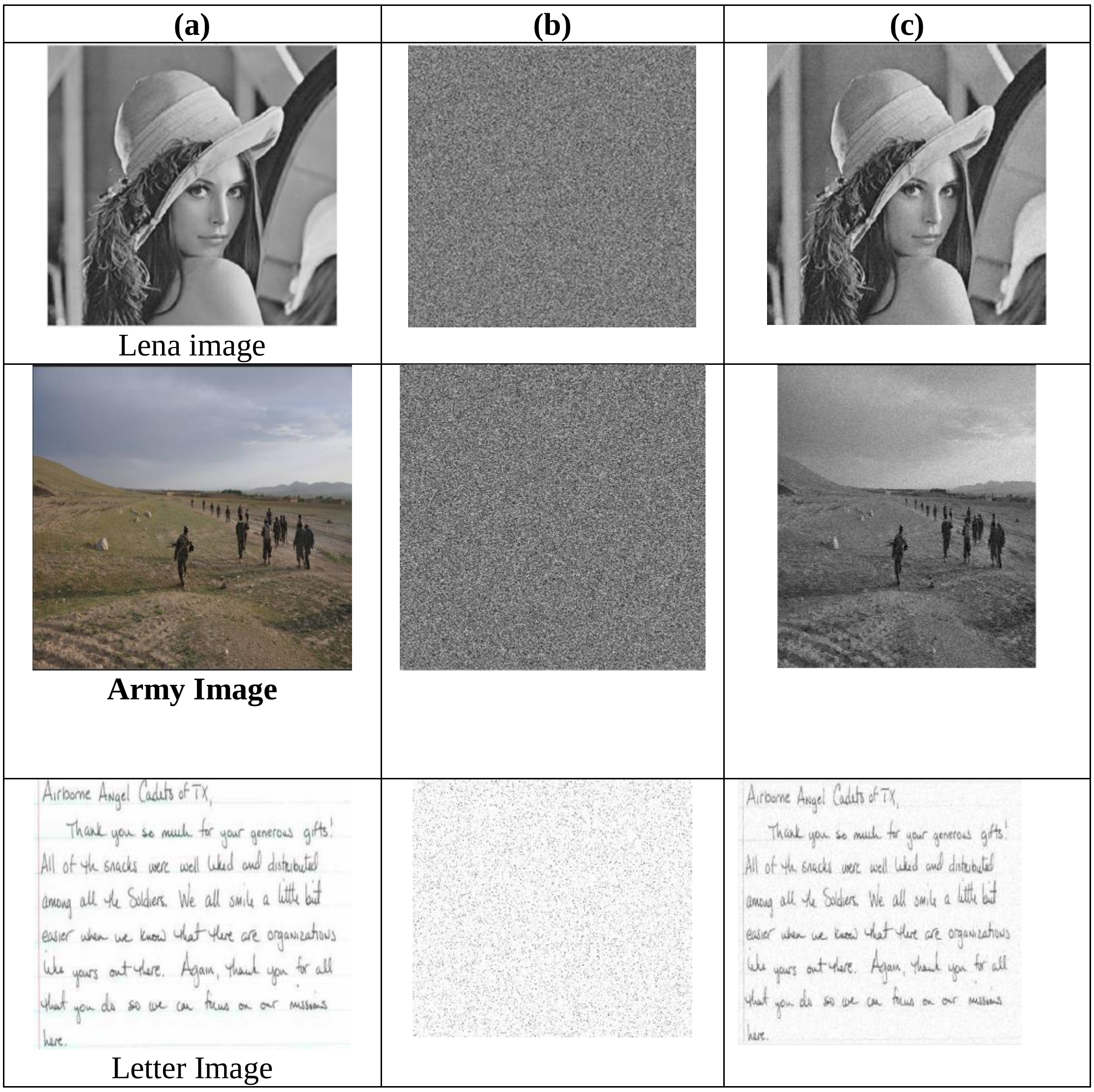

Start
Input Encrypted image
Select the Key
Call back the index number for each piece in Image and replace it by original number
Output the decrypted image
End

Figure 3 : The flowchart for shuffle pixel displacement decryption

4) EXPERIMENTAL RESULTS

The visual results of suggested method can be brief in Fig. 4 on a few sample images from many database which were tested. The image cryptography process depends on two separate stages. The first stage is encryption, and the second stage is decryption, which is the opposite of encryption. Mathematically, it is recognized that minor modifications during encryption procedures result in significant changes to the original data. As a result, a precise method is required to prevent or decrease alterations in the original data during encryption and decryption operations. The coefficient correlations PSNR and MSE define an image's statistical measures. [8]. Two calculation metrics were used to estimate the proposed method: the Peak Signal to Noise Ratio (PSNR) and the time required for the encryption and decryption stages. PSNR is a well-known metric for assessing the quality of a restored image. The better the image quality, the higher the PSNR score. It is the difference between the image and its reference counterpart in terms of maximum intensity to mean square error. The equ.1 gives it. For the purposes of this study, we calculated PSNR at the decryption stage using a reference image taken from a database. Table 1 shows three sample images [9].

$$\mathbf{PSNR} = \mathbf{10log_{10}} \frac{\mathbf{MaxI^2}}{\mathbf{Mean\ square\ error}} \qquad \mathbf{(1)}$$



Airborne Angel Cadets of TX,
Thank you so much for your generous gifts! All of the snacks were well liked and distributed among all the Soldiers. We all smile a little bit easier when we know that there are organizations like yours out there. Again, thank you for all that you do so we can focus on our missions here.

Figure 4: The visual results for images (a) original Image, (b) encrypted Image, (c) decrypted Image

DOI 10.5281/zenodo.7302482

Table 1: PSNR results and average computational time per step

Image	PSNR	Time of encryption stage(Sec)	Time of decryption stage(Sec)
Lena Image	53.21	34.444175	34.444175
Army Image	52.03	31.815637	31.815637
Letter Image	48.24	12.991811	12.991811

5) CONCLUSION

This research provided a novel approach of communicating in a harsh environment by employing protected photos. The greatest benefit of this technology is its low computing complexity that makes it ideal for usage in high-level applications such as military applications. It is organized into phases that are not only efficient but also simple to implement. The provided approach was analyzed using multiple databases. It is a very simple technique for encrypting color images with the RGB components (RED, GREEN, and BLUE) and scrambling by simply performing some transpose operations on the image with component displacement. This method encrypts and decrypts with a single key. This method is suitable for encrypting photos of various sizes and types that are used for a variety of purposes.

References

1) Sh.Somaraj and M.A.Husain, "A Novel Image Encryption Technique using RGB pixel displacement for Color Images," in IEEE 6th International Conference on Advanced Computing, 2016.

2) A.Elghandour, A. Salah and A. Karawia, "A new cryptographic algorithm via a two-dimensional chaotic map," Ain Shams Engineering Journal, p. 11, 2021.

3) S. Tiankai , W.Xingyuan ,J.Daihong, L.Da, D. Bin and Li. Dan, "A Robust Authentication Algorithm for Medical Images Based on Fractal Brownian Model and Visual Cryptography," Hindawi, p. 11, 2020.

4) I. Yasser ,F.Khalifa, M. Mohamed, and A.Samrah, "A New Image Encryption Scheme Based on Hybrid Chaotic Maps," Hindawi, p. 23, 2020.

5) T.Olzak, The role of cryptography in information security, 2012.

6) Somaraj S and Hussain MA, "Securing medical images by Image Securing medical images by," Intenational Journal of Computer Applications, Vols. 104(3):30-4., 2014.

7) Sh. Somaraj and M.Hussian, "Image Encryption using Edge Map and Key Image," Journal of Science and Technology, vol. 10(4), 2017.

8) M. K. Ramadhan and A. AL-Rammah, "Image Cryptography with Least Squares Approximations," Journal of Computer Science, vol. 15 (11): 1659.1668, p. 10, 2019.

9) K. A.Zidan and Sh.S.Jumaa, "An Efficient Enhancement Method for Finger Vein Images Using Double," International Journal of Advanced Science and Technology, vol. 29, pp. 996-1006, 2020.