JETIR.ORG ISSN: 2349-5162 | ESTD Year : 2014 | Monthly Issue
JOURNAL OF EMERGING TECHNOLOGIES AND INNOVATIVE RESEARCH (JETIR)
An International Scholarly Open Access, Peer-reviewed, Refereed Journal

FAST IMAGE ENCRYCPTION BASED ON RANDOM IMAGE KEY

[1]**K.V.Acharyulu,**[2]**Vyda Gireesha,**[3]**M.A.M.B.Raju,**[4]**M.Pravallika,**[5]**G.Ruby Benedict**
[1]**AssistantProfessor,** Dept of ECE, Godavari Institute of Engineering and Technology(A),Rajahmundry,AP
[2,3,4,5]**Students,** Dept of ECE, Godavari Institute of Engineering and Technology (A),Rajahmundry,AP

Abstract-Over the last decade, researchers in the field of information security have focused extensively on the topic of picture encryption, leading to the introduction of several image encryption algorithms, and the Internet's central role in the dissemination of vast quantities of multimedia. The picture is one kind of this multimedia content. The sender searches for an encryption scheme to conceal picture data before sending it across the network in secrecy. The purpose of this work is to devise a color picture encryption method that generates a random image key and requires a minimal amount of time to encrypt and decode images. In this case, the XOR technique is utilized to spread the encrypted picture farther, resulting in a more secure transmission.

Keywords:

Image Segmentation,Encryption,Decryption,**Wavelet,DWT**

1. INTRODUCTION

We said in the introduction that people are primarily visual beings, meaning that they use their eyes to interpret their environment. We use our eyes not just to locate and classify items, but also to scan for differences and get a "feel" for an environment with only a few seconds of looking around. Humans have developed highly refined visual capabilities, including the ability to instantly recognise faces, distinguish between different colours, and process a vast amount of visual information in a short amount of time. But the world is always changing, so if you stare at one object for too long, it will likely transform in some way. Even a large, substantial structure like a building or a mountain will take on a different appearance at different times of day, with different amounts of sunlight (clear vs cloudy), and with different numbers of shadows falling over it. Here, we focus on isolated pictures, or "snapshots," as they are sometimes known. Although image processing is adaptable enough to handle changing environments, we will not be focusing on this aspect. For our purposes, an image is any single photographic representation of anything. Whether it's a snapshot of an individual, a group of people or animals, or the natural world; a close-up of an electrical component; or the results of medical imaging, images come in many shapes and sizes. The picture will not be a random blur even if it is not recognised at first glance. An efficient way of encrypting digital images, random image keys are generated from the image's data and used as the encryption key. After the key has been generated in a secure cryptographic manner, it is used to encrypt the image. This method provides higher levels of security than conventional encoding methods by guaranteeing that the image cannot be decoded without the key. Discrete Discrete wavelet transforms (DWTs) include all wavelet transforms that make use of discrete sampling of wavelets and find use in both numerical analysis and functional analysis. Because it captures both frequency and spatial information, this wavelet transform is superior than Fourier transforms (location in time).

2. PROPOSED SYSTEM

To both encrypt and decode color images, a quick technique is presented here. The proposed technique works for images of any resolution. Symmetric picture encryption necessitates a shared key between the transmitter and the receiver. In this work, we propose a novel technique for generating an image key from the same picture or from another image of the sender's choosing. The method relies heavily on XOR logic. The primary concept is to sever the image in such a way that the subjects are no longer easily recognisable, particularly if the picture has been chopped both horizontally and vertically into smaller and smaller pieces. In this work, we implement this concept by generating an image key by rotating the source picture in three different axes. After randomly splicing and jumbling the four photos, the XOR logic is used to produce the image key. The following algorithm serves as an example of the aforementioned algorithm.

Image Key Generating Algorithm Steps:

1. load a coloured photo into the system.
2. rotate the colour picture 90 degrees in each of three directions (left, right and down).
3. Following the first two steps, we randomly permute each picture by cutting and pasting it into the next image.
4. Using XOR logic, step 4 yields the main key.
5. Analyzing the three main channels as the fundamental key in a study (R, G and B).
6. rotate R through 90 degrees (left to right, up to down and right to left)
7. rotate R and flip it so that it points in three different directions (left to right, up to down and right to left)
8. Use XOR to derive a new R from any of the matrices obtained in stages 6 and 7.
9. Obtaining a new G and a new B requires a repeat of steps 6-8. 9.
10. Create a new picture by piecing together the red, green, and blue components.
11. Use XOR to combine the new picture from step 9 with the original image from step 1.
12. Three-channel analysis of the picture analysed in Step 11 (R, G and B).
13. Use XOR on the RGB values to create the image's key.
14. End.

Once a color image is loaded, the system will generate a symmetric random image key that may be used for image encryption. Figure 1 depicts the process through which the Haar wavelet transform is used to extract characteristics from each channel of the origin image, yielding four components: low-low, high-low, low-high, and high-low. Scrambling entails multiplying the complements of the last three components by (-1), which flips the sign of the elements, and then using shifting to achieve more disorientation and confusion. Inverse Wavelet Transform is used to achieve the distorted image in this case. Scrambling the picture and applying XOR logic to the resulting image key will result in an encrypted image. Last but not least, assemble the three-channel input into a single coherent whole in order to get the secret image.

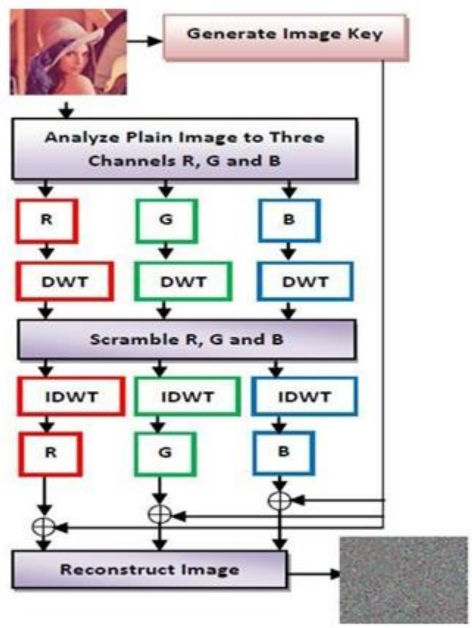

Fig1: Proposed Encryption Algorithm

To better understand the suggested encryption technique, its phases are laid forth below:

1. Simply input a basic color picture
2. make a password using the image's simple colors as the key.
3. separate the color picture into its red, green, and blue components.
4. use the Wavelet Transform to extract RGB features.
5. mix up the letters R, G, and B.
6. Create a new picture using Inverse Wavelet Transform.
7. Use XOR encryption using a secret key for all channels.
8. Using the RGB channels together, make the cypher color picture in step 8.

9. Keep the encrypted picture.
10. End.

The picture may be decrypted using the same symmetric key seen in fig2 thanks to a special reverse method.

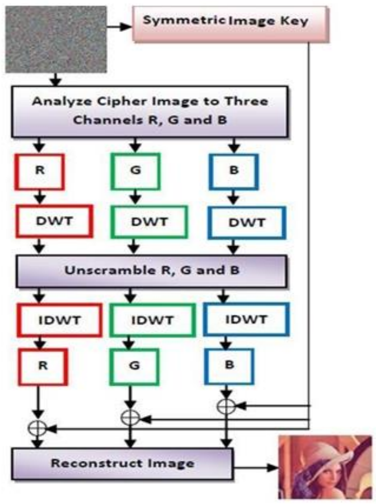

Fig2: Proposed Decryption Algorithm

The suggested decryption algorithm's stages are shown in the following example:

1. load a simple color picture.
2. separate the color picture into its R, G, and B components.
3. using Wavelet Transform to draw out RGB features.
4. Decode each R, G, and B.
5. Apply the Inverse Wavelet Transform to get a different picture.
6. use XOR decryption to unlock each channel with the secret key.
7. reclaim the original, uncomplicated color picture by fusing the R, G, and B channels.
8. Show the first photograph that was taken.
9. End.

3. RESULTS

MATLAB R2013a on a Windows PC is used to develop the proposed encryption technique. The suggested technique takes as input pictures of size 256 by 256 pixels in colour. Multiple checks are considered below. Histograms, for instance, should be taken into account in order to get insight.

The histogram is a metric from the realm of statistics that may be used to the distribution of visual data. It is a way to represent a colour picture by allocating a certain amount of pixels to each value. In order to prevent an attacker from decrypting the original picture, it is important to ensure that the values of all of the pixels in the encrypted version are the same, as seen in the Figure. The same picture is divided into its individual red, blue, and green components.

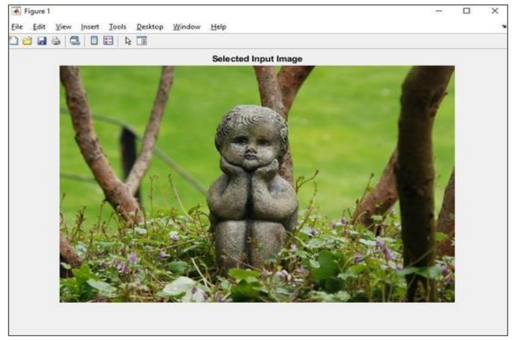

Fig3: Selected Input image

Fig4: R, G and B Channel extraction of input image

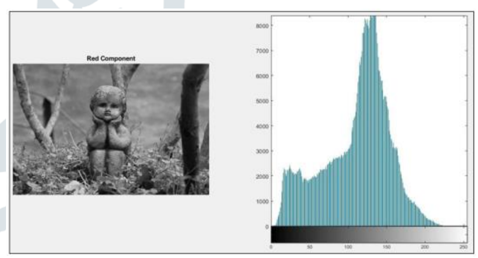

Fig5: Red component of an image with its Histogram

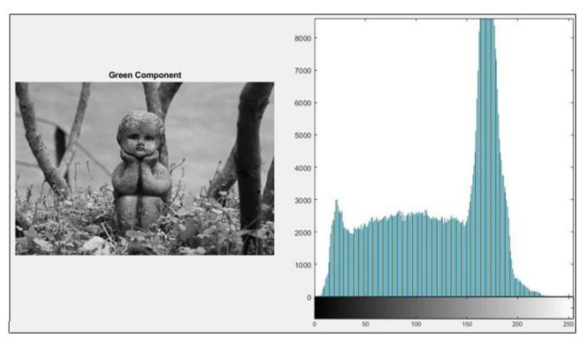

Fig6: Green component of an image with its Histogram

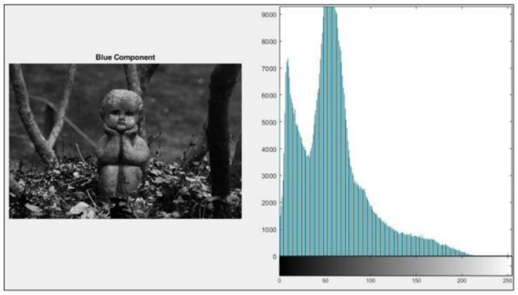

Fig7: Blue component of an image with its Histogram

Fig8: Wavelet based decomposed image

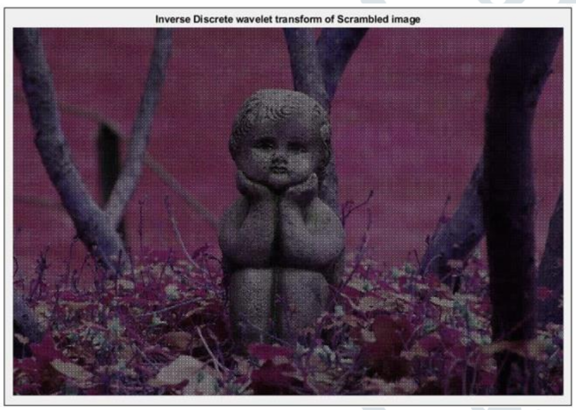

Fig9: Inverse Discrete Wavelet transform of Scrambled image

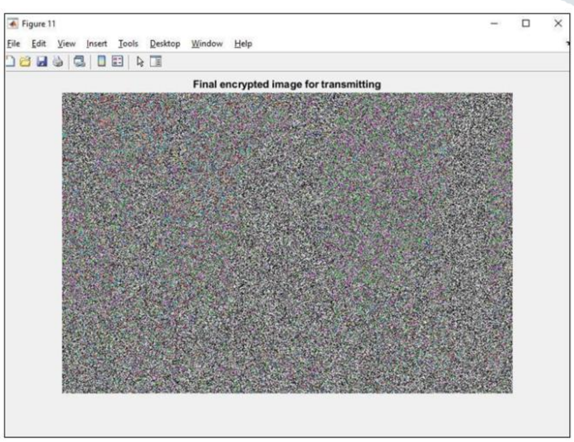

Fig10: Final encrypted image for transmitting over the channel

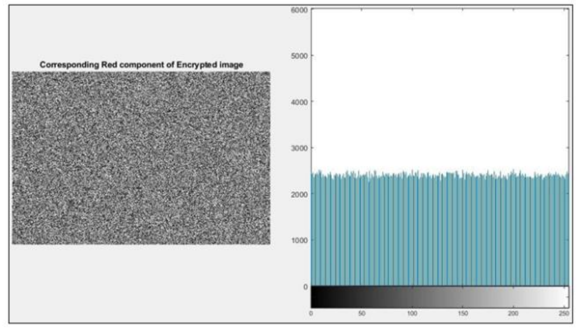

Fig11: Histogram for the red channel of encrypted image

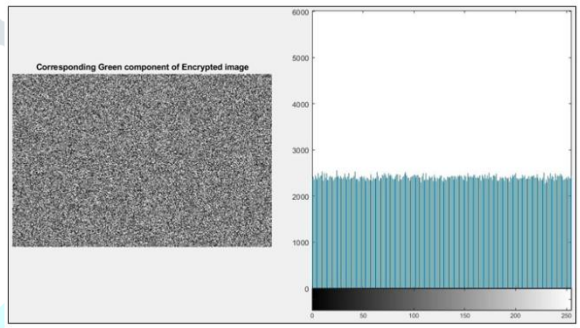

Fig12: Histogram for the green channel of encrypted image

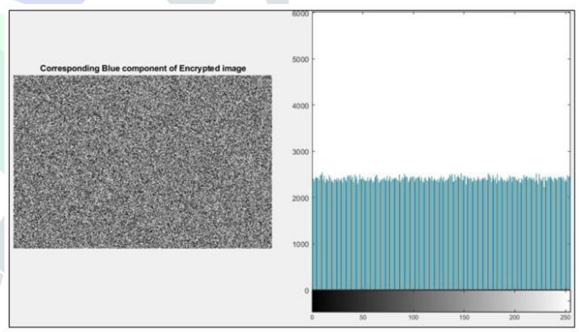

Fig13: Histogram for the blue channel of encrypted image

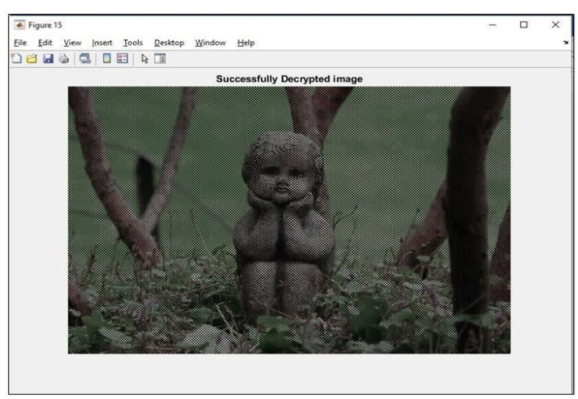

Fig14: Final Decrypted image using proposed algorithm

4. CONCLUSION AND FUTURE SCOPE

The importance of information security in data storage and transmission is growing at the present time. The usage of images is widespread across many industries. That's why it's crucial to safeguard picture information from abuse. When it comes to secret communication or data storage, image encryption is crucial.

We propose and develop a fast image key-based color picture encryption and decryption technique. The picture used to produce the image key does not need to be the same size as the original color image. Both the sender and the receiver have access to the same image key, and because this image key shares the qualities of a hash function, an attacker cannot recover the original picture from it. When applied to a number of statistical tests, the suggested method produces satisfactory results and is able to encrypt data.

At long last, just a selected region of a picture has to be encrypted in order to be secure. Additionally, it yields respectable performance when used as a block cypher rather than a stream cypher. In addition, compression of the simple picture using an image key may be produced to save data transmission costs.

REFERENCES

[1] Changgui Shi, Sheng-Yih Wang, Bharat K. Bhargava 1999: "MPEG Video Encryption in Real-time Using Secret Key Cryptography". PDPTA: pp2822-2828.

[2] Wu Y., Noonan J., and Agaian S. 2011: "NPCR and UACI randomness tests for image encryption", Journal of Selected Areas in Telecommunications (JSAT), pp. 31–38.

[3] Pratibha S. Ghode, SEM IV. and Tech M. 2014 "A Keyless approach to Lossless Image Encryption", International Journal of Advanced Research in Computer Science and Software Engineering, Vol. 4, No. 5, pp 1459-1467.

[4] Khanzadi H., Eshghi M. and Borujeni S. E. 2013 "Image Encryption Using Random Bit Sequence Based on Chaotic Maps", Arabian Journal for Science and Engineering AJSE,Vol.39, No. 2, pp1039–1047

[5] Mirzaei O., Yaghoobi M. and Irani H. (2012) "A New Image Encryption Method: Parallel Sub-Image Encryption with Hyper Chaos", Nonlinear Dynamics, Vol. 67, No. 1, pp557-566.

[6] Wei X., Guo L., Zhang Q., Zhang J., and Lian S. 2012 "A novel color image encryption algorithm based on DNA sequence operation and hyper-chaotic system", The Journal of Systems and Software, Vol. 85, No. 2, pp290-299.

[7] Panduranga H. T. and Naveen kumar S. K. 2011 "Hybrid Approach to Transmit a Secrete Image", 2nd National Conference on Emerging Trends and Applications in Computer Science IEEE.

[8] Ibrahim S. I. Abuhaiba and Maaly A. S. Hassan 2011 "Image Encryption Using Differential Evolution Approach In Frequency Domain", Signal & Image Processing An International Journal SIPIJ Vol. 2, No. 1.

[9] Wang X., Zhao J. and Liu H. 2012 "A new image encryption algorithm based on chaos", Elsevier.Vol.285 No.5, pp562–566.

[10] Seyedzade S. M., Atani R. E., and Mirzakuchaki S. 2010 "A Novel Image Encryption Algorithm Based on Hash Function", In 6th Iranian Conference on Machine Vision and Image Processing IEEE.

[11] Min L. and Lu H. 2010 "Design and analysis of a novel chaotic image encryption", 2nd International Conference on Computer Modelling and Simulation, Publication IEEE, pp517-520.

[12] Pall A. K., Biswas G. P. and Mukhopadhyay S. 2010 "Designing of High-Speed Image Cryptosystem Using VQ Generated Codebook and Index Table", International Conference on Recent Trends in Information, Telecommunication and Computing IEEE, pp39-43.

[13] Pang C. 2009 "An Image Encryption Algorithm Based on Discrete Wavelet Transform and Two Dimension Cat Mapping", Proceedings of the International Conference on Networks Security, Wireless Communications and Trusted Computing IEEE, Vol. 2, pp711-714.

[14] Acharya B., Patra S. K., and Panda G. 2008 "Image Encryption by Novel Cryptosystem Using Matrix Transformation", 1st International Conference on Emerging Trends in Engineering and Technology IEEE, pp77-81.

[15] Al-Khassaweneh M. and Aviyent S. 2008 "Image Encryption Scheme Based on Using Least Square Approximation Techniques", International Conference Electro Information Technology IEEE, pp108-111.

[16] Gupta M. et al. 2012 "A New Approach for Information Security using Asymmetric Encryption and Watermarking Technique" International Journal of Computer Applications (IJCA) Vol.57 No.14.

[17] Francia A., Yang M. and Trifas M. 2009 "Applied image processing to multimedia information security", Int. Conf. Image Analysis and Signal Processing IEEE, pp286 - 291

[18] Mursi M. et al. 2014 "Combination of Hybrid Chaotic Encryption and LDPC for Secure Transmission of Images over Wireless Networks", International Journal of Image, Graphics and Signal Processing, pp8-16.

[19] Toufik, B. and Mokhtar N. 2012 "The Wavelet Transform for Image Processing Applications. In: Advances in Wavelet Theory and Their Applications in Engineering, Physics and Technology", Chapter 17, InTech, USA, pp395-422.

[20] Sivakumar T. and Venkatesan R. 2014 "A Novel Approach for Image Encryption Using Dynamic Scan Pattern" International Journal of Computer Science IAENG, Vol. 41, No. 2, pp91-101.

[21] Thakur N, Devi S. 2011 "A new method for color image quality assessment" International Journal Computer Application. Vol. 15, No.2, pp10–17.