

Colour Image Encryption - A Wavelet Transformation Associated with Artificial Neural Network Approach

Prateep Upadhyay
DST-CIMS Banaras Hindu University
Varanasi Uttar Pradesh India 221005

S.K. Upadhyay, PhD
Department of mathematical sciences IIT(B.H.U.)
DST-CIMS Banaras Hindu University
Varanasi Uttar Pradesh India 221005

ABSTRACT

Image encoding decoding concept is studied by using the techniques of wavelet transformation, artificial neural network(ANN)and threshold value. The aforesaid techniques are useful in encoding and decoding. This process gives more ensured, a three leveled security to the images in three different terms. First is wavelet transformation. Second is encoding decoding keys along with weights of ANN and third is the threshold value for the decoding process. The decoding process does not start until the correct threshold value is entered.

Keywords

ANN, Threshold value, Keys, Weights

1. INTRODUCTION

This paper intends to develop a high security technique for encryption and decryption of images. Wavelet transformation along with a neural network can play the leading role in the encryption of an image. Another neural network and inverse wavelet transformation have been used for the decryption of image. The cardinal aspect of this paper is that a three layered mechanism has been used for the encryption and decryption of an image. First, wavelet transformation has been used by which the security of the image is enhanced in a way that if a person is ignorant about the kind of information used, decryption of the image becomes impossible for the person. Second, the better way for the security of the image, a neural network associated with security keys has been used for the encryption under which without knowing the weights or strengths of interconnection or the keys, the decryption of the image becomes next to impossible. Similarly decryption of the image holds the above rule as well. Third and the most vital part is that the decryption process used under the technique of neural network is completely dependent upon a certain threshold value i.e. the process of decryption will never start until and unless the correct threshold value is input. An image is a single picture which is representative of something from real world. This may be of a person, mass, forest, animal; anything of an outdoor object or a micro photograph of an electronic component or the findings of medical investigations. However the security of the images, thus received, is of prime concern of this era. Global communication technologies and a complete coverage of internet provide numerous modes for worldwide transfer of images. As the use of the digital techniques is continuously in de-

mand for transmitting and storing images, the fundamental need of image protection, confidentiality, integrity, authenticity and non repudiation have become inevitably essential. In this paper theory of [5] has been used. A better and a more secured method of image encryption and decryption is given. For doing this, absolutely no loss of information to the images is ensured in this paper that is the decoded image is perfectly same in every respect as that of the original image.

2. ORGANIZATION OF THE PAPER

The whole paper is organized as follows- section 3, section 4 and section 5 give the brief descriptions about wavelet transformation, artificial neural networks and images respectively. In section 4, the importance of threshold value has been discussed. In section 6 using the theory of wavelet transformation and neural networks, the encoded image has been obtained. In section 7 suitable algorithm has been given about the entire encoding and decoding process. In section 8 and section 9 conclusion and future scope have been given. In the section 3 from [1], [6] and [7] the definition of 2D wavelet transformation of a function $f(x, y)$ has been recalled. Finally, in the section 10 and in its subsections, demonstration and verification of the procedure on some colour images have been given.

3. WAVELET TRANSFORMATION

From [1, 6, 7], the wavelet transformation of a signal $f(x, y)$ with respect to wavelet $\psi_{a,b}(x, y)$ in two dimensions is defined by $W(a_x, a_y, b_x, b_y) = \int_{\mathbf{R}} \int_{\mathbf{R}} \Psi_{a,b}^*(x, y) f(x, y) dx dy$ Where * denotes the complex conjugate. We generate a doubly indexed family of wavelets from ψ by dilating and translating.

$$\psi_{a,b}(x, y) = \frac{1}{\sqrt{|a_x||a_y|}} \psi\left(\frac{x-b_x}{a_x}, \frac{y-b_y}{a_y}\right)$$

where $a, b \in \mathbf{R}^2, a \neq 0$. (We use both negative and positive a at this point).

Inverse wavelet transform is given by

$$f(x, y) = \frac{1}{C_\psi} \int_{\mathbf{R}} \int_{\mathbf{R}} \int_{\mathbf{R}} \int_{\mathbf{R}} \frac{W(a_x, a_y, b_x, b_y) \Psi_{a,b}(x, y)}{a_x^2 a_y^2} da_x da_y db_x db_y$$

where $C_\psi = \int_{\mathbf{R}} \int_{\mathbf{R}} \frac{|\hat{\psi}(x, y)|}{|x||y|} dx dy$ and $\hat{\psi}$ denotes the Fourier transformation of ψ .

4. ARTIFICIAL NEURAL NETWORK

From [8], neural networks aims at mimicking the human abilities to adapt itself towards varying circumstances and the current environment. This is completely dependent on learning from past happenings and to be able to apply this in futurity. For example any diagnosis by a doctor does not depend on a single symptom because of the complexities of the human body for one symptom could lead to many other problems. Generally an experienced doctor's diagnosis is ought to be correct and error free in comparison to someone who has recently completed his medical degree. This is because his past experience guides him to lead to a diagnosis or quite possibly a mistake of his past years might have been embossed in his mind that he would never wish to repeat. Thus we can say the experience has taken the doctor to a superior position in comparison to a fresh degree holder. In the same way how nice it would be if the machines too could have experienced from the past events and basing on them made the decisions. This is basically the role of neural network. A worldwide effort is on to make the machines intelligent like human beings. An artificial neural network has many nodes i.e. processing unit analogs to neurons in the brain. Each node is provided with a node function. This, with a set of local parameters, determines the output of the node with a given input. Local parameters if modified may alter the node function. Therefore artificial neural network is an information processing system. The information is processed by the elements called the neurons. Connection links transmit the signals. The links have associated weights. That is, if x is the input to a neuron and the associated weight of the link is w then the net input given to the neuron is wx . Where wx stands for product of w and x . Output signal can be obtained from the activation function of the neuron i.e. if the activation function is f and the net input to the neuron is wx , then the net output from the neuron will be $f(wx)$. The neural net can either be of single layered or multilayered.

4.1 Feed forward net

From [8], quite possibly feed forward networks may have a single layer of weights where inputs are directly connected to the outputs or there may be multiple layers with intervening sets of hidden units. Hidden units are used by neural networks to create the internal representation of the input patterns.

1.Single layer net: From [8], it is a feed forward net. It contains only one layer of weighted interconnections. The inputs may be connected fully to the output units.

2.Multilayer net : From [8], the multilayer net poses one or even many more layers of nodes in between the input and output units.

4.2 Threshold values in neural networks

From [8], the threshold θ is a value which is used in the calculation of the activation of the given net. i.e. any value other than θ will fail to activate the neural net. Only the threshold value is responsible for the function. A user is free to give the value of threshold according to his/her wish.

5. IMAGES

From [2, 3], an image may be defined as a two dimensional function $f(x, y)$, where x and y are spatial(plane) coordinates and the amplitude of f at any pair of coordinates is called the intensity of

the image at that point. The term gray level is used often to refer the intensity of monochrome images, referred as the Red(R), Green(G) and Blue(B) primary (or component) images. For this reason many of the techniques developed for monochrome images can be extended to colour images by processing the three component images individually. From [2, 3] an image may be continuous with respect to x and y coordinates, and also in amplitude. Converting such an image to digital form requires the coordinates, as well as the amplitude be digitized. Digitizing the coordinate values is called sampling; digitizing the amplitude values is called quantization. Thus x, y , and the amplitude values f are all finite, discrete quantities, we call the image a digital image.

6. METHODOLOGY

Naturally a single layer wavelet transformation always decomposes an image in four different low resolution images. Quite obviously application of inverse wavelet transformation makes the image original one. This paper aims at applying wavelet transformation to the input images. When wavelet transformation is applied, the images are broken down into four different parts of low resolution. Each low resolution part is encrypted using four different keys namely k_1, k_2, k_3 and k_4 representing the values 1000000, 10000000, 100000000 and 1000000000 respectively. At this point this must be kept in mind that the choice of the keys is completely arbitrary. It is the user's choice as to what value he or she wants to choose. Attention is drawn towards the point that in this proposed method it is a general finding that the outcome of encryption technique comes out good if the numeric values of the keys are large. Once the encryption of all the four low resolution parts of the images is done, all these parts are passed through a feed forward network individually. Where they are again encrypted by the weights of interconnection and lastly the encrypted image is formed. In the decoding phase first the encrypted image is passed through a feed forward neural network that operates on a threshold value. The neurons of the neural net won't respond to command unless the required threshold value is achieved (1.6432 in our case). Decoding process can't be started without providing the correct threshold value. Once again this will not be out of the topic to mention that the threshold value is completely discretionary of the user. Once the decoding process is started the original image can be restored by applying inverse wavelet transformation values of the keys $1/k_1, 1/k_2, 1/k_3$ and $1/k_4$.

This method is applied to images of sizes 660X458, 740X518, 740X518, 734X402, 364X286, 740X446, 698X486, 464X254 respectively. All the images are coloured images and the images sized 660X458, 740X518, 740X518 are from Windows 7 sample pictures. Rest of the images are the results of random searches of google images. The process is applied to all the images with the same key values (the same values of k_1, k_2, k_3 and k_4). All the original images, encoded images and decoded images are shown in the section of original images, encoded images and decoded images respectively under the section of images. On decoding the images it is found that the image matrix is coming out to be the same as the input image matrix. This clearly indicates that there is absolutely no information loss in this method.

7. ALGORITHM

Step1: Input image.

Step2: Apply wavelet transform.

Step3: Apply the keys and encode the image.

Step4: Pass the encoded image to an artificial neural network and finally get the encoded image.

Step5: To fire the decoding neural network ask the user to enter threshold value.

Step6: Enter the threshold value and check if it is correct.

Step7: If the threshold value is correct goto Step 8 else goto Step10.

Step8: Apply inverse keys to the encoded image.

Step9: Apply inverse wavelet transform to the image got after Step8.

Step10: Stop.

8. CONCLUSION

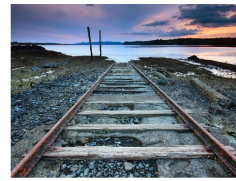
The method proposed in this paper is very useful for image encryption for even if the security keys are known to someone by any means, the weights of the neural network will still remain unknown. In addition to this, the extra level of security is added by introducing threshold value. This threshold value is impenetrable unless the perfect and accurate threshold value is entered. Thus in brief, it can be said that the paper provides three major securities that are almost impossible to break.

9. FUTURE SCOPE

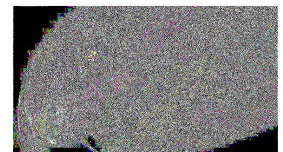
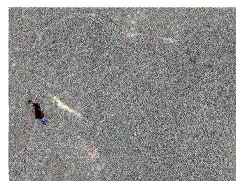
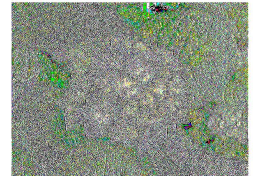
The future works can be based on applying similar techniques of image encoding decoding concepts with other transformations. A comparative study of performance measures can also be done with different types of transformations.

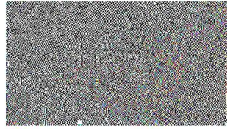
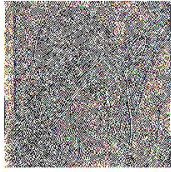
10. IMAGES

10.1 Images before encoding

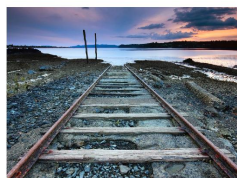


10.2 Encoded images





10.3 Decoded images



11. REFERENCES

- [1] Daubechies .J: Ten Lectures to Wavelets, SIAM, Philadelphia, Pennsylvania, USA,1992.
- [2] Gonzalez C. Rafael, Woods E. Richard, Eddins L. Steven: Digital image processing 3rd edition,Eighth Impression.
- [3] Gonzalez C. Rafael, Woods E. Richard, Eddins L. Steven: Digital image processing using MATLAB 2nd edition,2007.
- [4] Kumar Manish, Mishra D.C., Sharma R.K. :A first approach on an RGB image encryption, Elsevier Optics and Lasers in Engineering 52(2014)27-34,Department of Mathematics,Birla Institute of Technology and Science-Pilani,Hyderabad Campus,Hyderabad500078,AndhraPradesh,India,Department of Mathematics,Indian Institute of Technology,Delhi,HauzKhas110016,NewDelhi,India.
- [5] Lokenath Debnath: Wavelet Transforms and their applications.
- [6] Prasad Akhilesh,Kumar Manish,Roy Choudhury Devdeep: Color image encoding using fractional Fourier transformation associated with wavelet transformation,Elsevier Optics Communications 285 (2012) 1005-1009,Department of Applied Mathematics, Indian School of Mines, Dhanbad-826004, India.
- [7] Pathak R.S.: The Wavelet Transform, Atlantis Press/World Scientific, Amsterdam,Paris, 2009.
- [8] Sivanandam S.N., Sumathi S, Deepa S.N.: Introduction to Neural Networks Using Matlab 6.0 , Tata McGraw Hill Education Private Limited New Delhi,2009.