

A New Algorithm to Encryption and Compression Image Data File

Riyad Mubarak Abdullah

Department of Computer Science / College of Education
University of Mosul

Received
11 / 06 / 2009

Accepted
09 / 09 / 2009

RSA

bmp

ABSTRACT

In this research algorithm to encryption and image compression data file was developed. This algorithm is a result of merge between RSA algorithm for encryption and Morlet Wavelet which is used for image data file compression. We applied this algorithm to a group of images which is randomly choused and bmp type with different in size and content, this algorithm gives good results for keeping the security of the information because the data file encrypted at the beginning and then compressed as a result it will be difficult to recognize the file content for unauthorized person.

Keywords: RSA Method, Morlet Wavelet

1.1 Introduction

Encryption is a method for keeping the security of the information (constant and moving) by using programs that have the ability to change and translate this information to symbols will be difficult to understand by unauthorized persons.

This kind of programs witness markedly development after that the US authorities allow to the corporations to sell the technology and make it available to the public, after it was restricted for many years and authorized for military purposes only. The US Government took this decision to support the security side of the electronic trade. Noting that the US Government till early times has restrictions to export the technology outside the US, especially the technology that have encryption more than 56 bit [1].

Each individual or company or commercials have privacy and important information that no one should know them, also we can't give up the service available like the internet and email or electronic shopping. In other words encryption is the process of changing text so that it is no longer easy to read [1].

So the encryption goals are:

1. Confidentiality is a service used to keep the content of information from all but those authorized to have it.
2. Data integrity is a service which addresses the unauthorized alteration of data.
3. Authentication is a service related to identification.
4. Non-repudiation is a service which prevents an entity from denying previous commitments or actions [2].

1.2 Private key Encryption

Private key encryption is the standard form. Both parties share an encryption key, and the encryption key is also the one used to decrypt the message. The difficulty is sharing the key before you start encrypting the message - how do you safely transmit it?

Many private key encryption methods use public key encryption to transmit the private key for each data transfer session [1].

1.2.1 Public Key Encryption

Public key encryption uses two keys - one to encrypt, and one to decrypt. The sender asks the receiver for the encryption key, encrypts the message, and sends the encrypted message to the receiver. Only the receiver can then decrypt the message even the sender cannot read the encrypted message [1].

1.2.2 Limitations of Encryption

Cryptanalysis, or the process of attempting to read the encrypted message without the key, is very much easier with modern computers than it has ever been before. Modern computers are fast enough to allow for 'brute force' methods of cryptanalysis - or using every possible key in turn until the 'plain text' version of the message is found.

The longer the key, the longer it takes to use the 'brute force' method of cryptanalysis, but it also makes the process of encrypting and decrypting the message slower. Key length is very important to the security of the encryption method - but the 'safe' key length changes every time CPU (Central Processing Unit) manufacturers bring out a new processor.

Encryption system which is used public keys is called the RSA (Ron Rivest, Adi Shamir, dan Len Adleman) system, although it is much better and more secure from the DES (*Data Encryption Standard*) system but it is slower, because that the encryption and decryption process should be done nearly at the same time, anyway RSA system is not difficult to be infiltrated. Which is possible to be infiltrate incase there is the necessary time and money, see Figure (1).

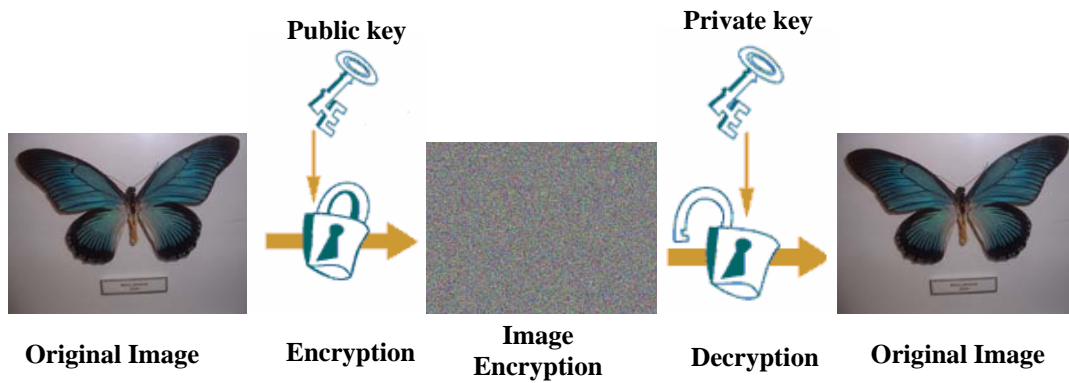


Figure (1): Encryption and decryption [1].

1.3 Ron Rivest, Adi Shamir, dan Len Adleman (RSA) Encryption Method

A public-key cryptography algorithm which uses prime factorization as the trapdoor one-way function. Define in equation (1):

$$n \equiv pq \quad (1)$$

for p and q primes. Also define a private key d and a public key e as computed in equation (2) and (3):

$$de \equiv 1 \pmod{\phi(n)} \quad (2)$$

$$(e, \phi(n)) = 1 \quad (3)$$

where $\phi(n)$ is the totient function, (a, b) denotes the greatest common divisor (so $(a, b) = 1$ means that a and b are relatively prime), and $a \equiv b \pmod{m}$ is a congruence. Let the message be converted to a number M . The sender then makes n and e public and sends as in formula (4):

$$E = M^e \pmod{n} \quad (4)$$

To decode, the receiver (who knows d) computes

since N is an integer. In order to crack the code, d must be found. But this requires factorization of n since as shown in equation (5) and (6):

$$E^d \equiv (M^e)^d \equiv M^{ed} \equiv M^{N\phi(n)+1} \equiv M \pmod{n} \quad (5)$$

$$\phi(n) = (p-1)(q-1) \quad (6)$$

Both p and q should be picked so that $p \pm 1$ and $q \pm 1$ are divisible by large primes, since otherwise the Pollard $p-1$ factorization method or Williams $p+1$ factorization method potentially factor n easily. It is also desirable to have $\phi(\phi(pq))$ large and divisible by large primes [3].

1.4 Compression

Compression is the process of reducing the size of a file by encoding its data information more efficiently. By doing this, the result is a reduction in the number of bits and bytes used to store the information [4]. Then the image compression means reducing the size of image data files, thus data compression techniques are invented to reduce the data size to be transmitted with minimum loss of image information. The reduced file is called the compressed file which can be used to reconstruct the original image data file which is known as decompressed image [5].

The compression is used just about everywhere. All the images you get on the web are compressed, typically in the JPEG (Joint Photographic Expert Group) or GIF (Graphics Interchange Format) formats, most modems use compression, and several file systems automatically compress files when stored, and the rest of us do it by hand [6], [7].

1.4.1 Compression Ratio

The ratio between original image (uncompressed image) and the compressed image is known as the compressed factor or compression ratio can be calculated from equation (7) [8]:

$$\text{Compression ratio} = \frac{\text{Uncompressed file size}}{\text{Compressed file size}} \quad (7)$$

1.5 Wavelet

Wavelet is mathematical functions that cut up data into different frequency components, and then study each component with a resolution matched to its scale. They have advantages over traditional Fourier methods in analyzing physical situations where the signal contains discontinuities and sharp spikes. Wavelet was developed independently in the fields of mathematics, quantum physics, electrical engineering, and seismic geology. Interchanges between these fields during the last ten years have led to many new wavelet applications such as image compression, turbulence, human vision, radar, and earthquake prediction. This paper introduces wavelet to the interested technical person outside of

the digital signal processing field. We describe the history of wavelet beginning with Fourier, compare wavelet transforms with Fourier transforms, state properties and other special aspects of wavelet, and finish with some interesting applications such as image compression, musical tones, and de-noising noisy data [9].

Wavelet is a mathematical tool for hierarchically decomposing functions. They allow any function to be described in terms of a coarse overall shape, plus details that range from broad to narrow. Figure (2) below illustrate. Wavelet can be applied to a wide variety of objects used in graphics, including images, curves, surfaces, and the solutions to lighting simulations.

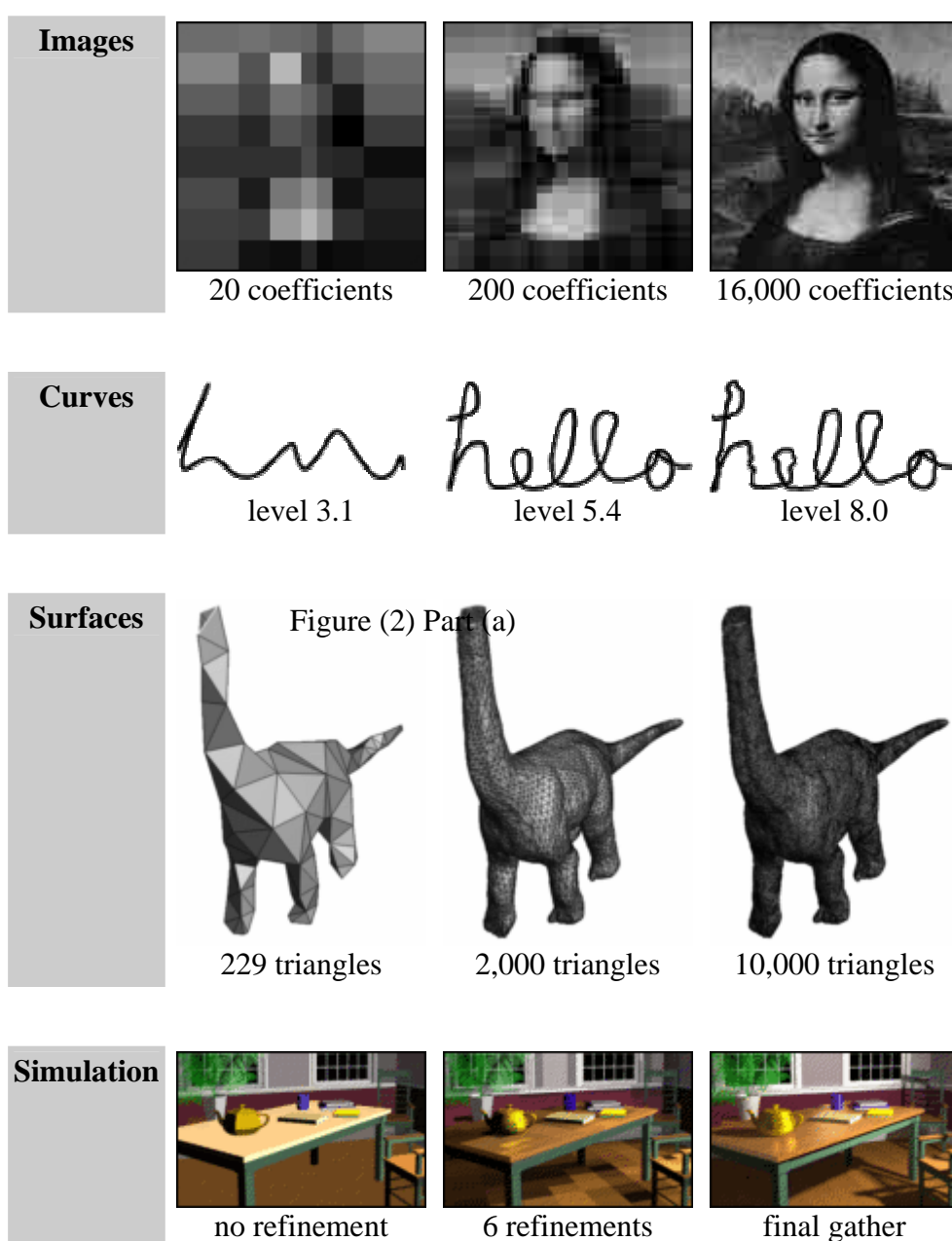


Figure (2): Wavelet applications [10], [11].

1.5.1 Morlet Wavelet and Transform

The Morlet wavelet is arguably the original wavelet. Although the discrete Haar wavelet predates Morlet's, it was only as a consequence of Morlet's work that the mathematical foundations of wavelet as a better formulation of time-frequency methods were laid [12].

The wavelet defined by Morlet is given in equation (8):

$$\hat{g}(\omega) = e^{-2\pi^2} (v - v_0) \quad (8)$$

Where $\hat{g}(\omega)$ it is a complex wavelet which can be decomposed in two parts, one for the real part, and the other for the imaginary part as shown in equation (9) and (10):

$$g_r(x) = \frac{1}{\sqrt{2\pi}} e^{-\frac{x^2}{2}} \cos(2\pi v_0 x) \quad (9)$$

$$g_i(x) = \frac{1}{\sqrt{2\pi}} e^{-\frac{x^2}{2}} \sin(2\pi v_0 x) \quad (10)$$

Where $g_r(x)$ is a real part, $g_i(x)$ is an imaginary part, v is a vector space and v_0 is a constant. The admissibility condition is verified only if $v_0 > 0.8$. Figure (3) shows these two functions.

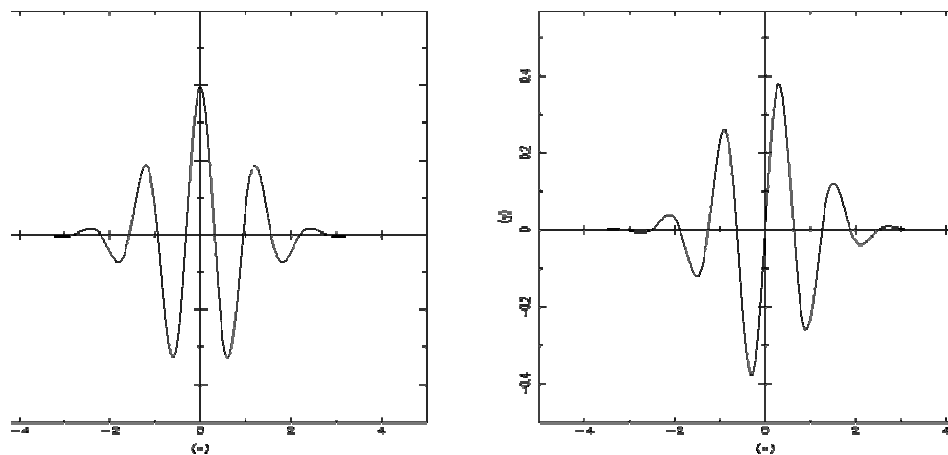


Figure (3): Morlet's wavelet: real part at left and imaginary part at right [12].

1.5.2 Wavelet Algorithm

In fact the compression algorithm that used wavelet transform contain three parts, one of them is transform and the second is the quantization and the last is coding. Figure (4) shows the wavelet algorithm

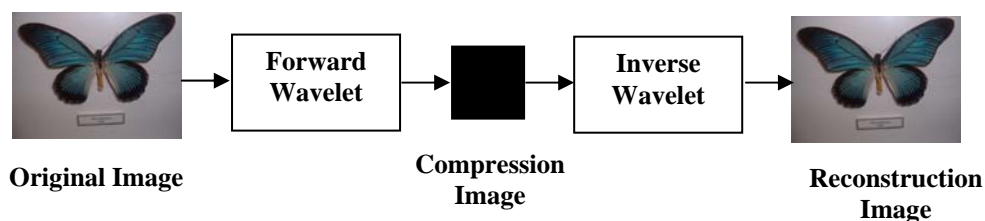


Figure (4): Wavelet algorithm.

1.6 The New Algorithm

The new algorithm is a result of merging between RSA algorithm for encryption and Morlet wavelet which is used for compression data file. Figure (5) shows how the algorithm works. The detailed explanation for the new algorithm is as below:

At the beginning the image file will be read after that it will be encrypted using public key, the result will be encrypted in a file which will be considered as the original file prepared to compression. After that the file will enter the forward wavelet and this operation uses the Morlet wavelet after that we will get a compressed file and in fact the file is also encrypted and this file will be send to the authorized person. After receiving the encrypted and compressed file the decompression process will be done by use of Inverse wavelet, to get open but encrypted image after that by using private key to decrypt the image to get the original one.

These processes increased the information security that the file contained and with this the goal of this algorithm is accomplished.

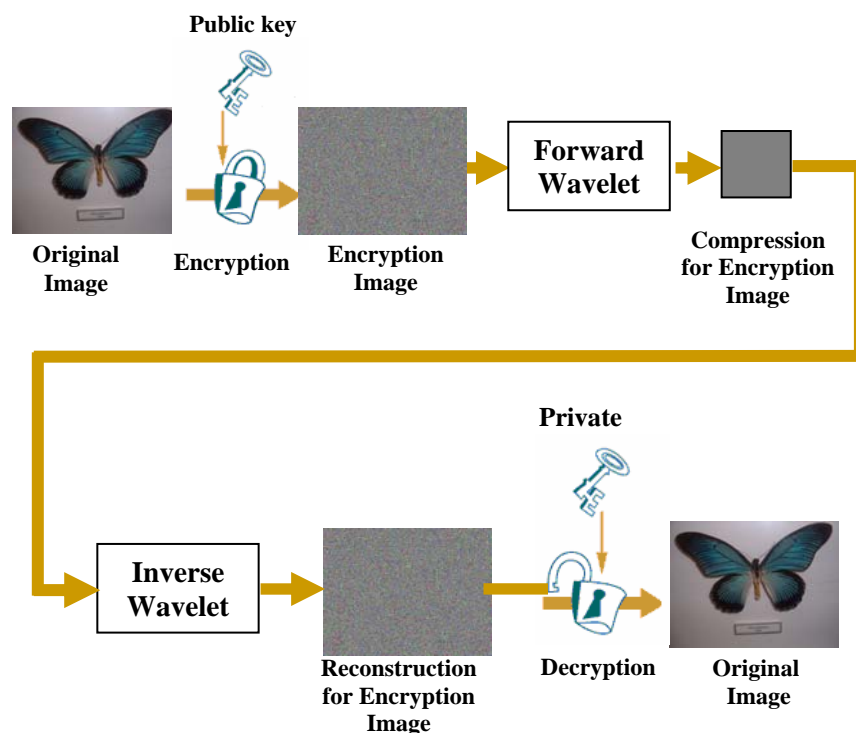


Figure (5): The process for a new algorithm.

1.7 Results Analysis

The proposed algorithm has been applied on a group of images which is randomly choused of Bmp type with different in size and content. The results of proposed algorithm shown in Figures (6, 7 and 8).

Each figure consists of three columns, the first column contains the original image (name and size), the second column contains the compression for encryption and the third column contained the image after removing the compression and encryption. In Figure (6) the compressed ratio used is 50 %. The file size still large compared with the

compressed ratio 75 % and 100 %, and in Figure (7) the compressed ratio used is 75 %. The file size still large compared with compressed ratio 100 % finally in Figure (8) the compressed ratio which is used is 100 %. This ratio compressed the file to best size compared with other compressed ratios.

Note in the third column of Figure (6, 7 and 8), because of the usage of wavelet we can notice in the reconstructed image there is a simple lose and this lose is directly proportion with compression ratio.





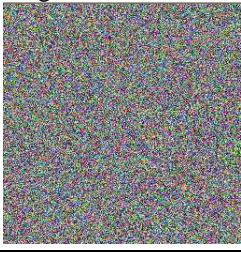










Original Image Athena.bmp with size 11kb 	Compression for Encryption Image with size 9.64kb 	Decompression and Decryption Image with size 10.999kb 
Original Image Frt.bmp with size 193kb 	Compression for Encryption Image with size 21.5kb 	Decompression and Decryption Image with size 192.99kb 
Original Image Butterfly.bmp with size 910kb 	Compression for Encryption Image with size 5.44kb 	Decompression and Decryption Image with size 909.990kb 
Original Image Tulip.bmp with size 49kb 	Compression for Encryption Image with size 5.56kb 	Decompression and Decryption Image with size 48.99kb 
Original Image F362.bmp with size 1,407kb 	Compression for Encryption Image with size 152.9kb 	Decompression and Decryption Image with size 1,4064kb 

Figure (6): The result of the proposed algorithm with 50 % compressed ratio.





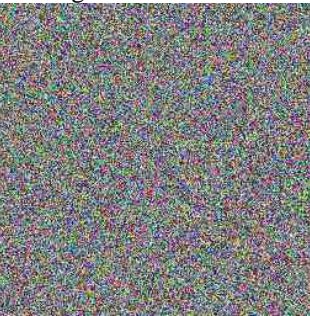


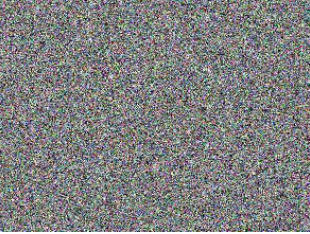







<p>Original Image Athena.bmp with size 11kb</p> 	<p>Compression for Encryption Image with size 7.42kb</p> 	<p>Decompression and Decryption Image with size 10.998kb</p> 
<p>Original Image Frt.bmp with size 193kb</p> 	<p>Compression for Encryption Image with size 15.3kb</p> 	<p>Decompression and Decryption Image with size 192.98kb</p> 
<p>Original Image Butterfly.bmp with size 910kb</p> 	<p>Compression for Encryption Image with size 97.8kb</p> 	<p>Decompression and Decryption Image with size 909.98kb</p> 
<p>Original Image Tulip.bmp with size 49kb</p> 	<p>Compression for Encryption Image with size 4.08kb</p> 	<p>Decompression and Decryption Image with size 48.98kb</p> 
<p>Original Image F362.bmp with size 1,407kb</p> 	<p>Compression for Encryption Image with size 110.7kb</p> 	<p>Decompression and Decryption Image with size 1,40632kb</p> 

Figure (7): The result of the proposed algorithm with 75 % compressed ratio.


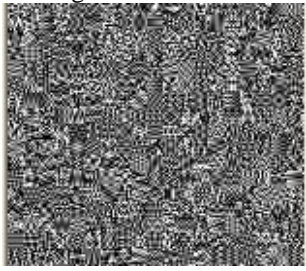


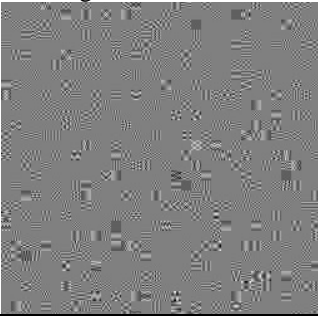


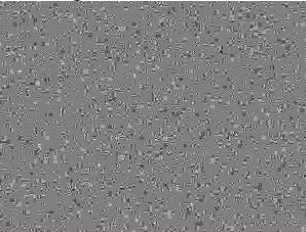


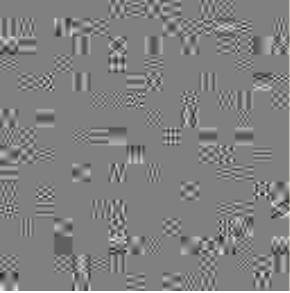


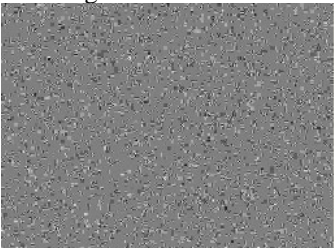

<p>Original Image Athena.bmp with size 11kb</p> 	<p>Compression for Encryption Image with size 1.88kb</p> 	<p>Decompression and Decryption Image with size 10.997kb</p> 
<p>Original Image Frt.bmp with size 193kb</p> 	<p>Compression for Encryption Image with size 1.35kb</p> 	<p>Decompression and Decryption Image with size 192.96kb</p> 
<p>Original Image Butterfly.bmp with size 910kb</p> 	<p>Compression for Encryption Image with size 70.8kb</p> 	<p>Decompression and Decryption Image with size 909.96kb</p> 
<p>Original Image Tulip.bmp with size 49kb</p> 	<p>Compression for Encryption Image with size 0.56kb</p> 	<p>Decompression and Decryption Image with size 48.96kb</p> 
<p>Original Image F362.bmp with size 1,407kb</p> 	<p>Compression for Encryption Image with size 8.26kb</p> 	<p>Decompression and Decryption Image with size 1,40621kb</p> 

Figure (8): The result of the proposed algorithm with 100 % compressed ratio.

1.8 Conclusions

From this research we conclude that the new algorithm which is a result of merging between RSA algorithm for encryption and Morlet Wavelet which is used for compression image data file gives good results for keeping the security of the information because the data file encryption at the beginning by a key and then compressed so that to get the file again it should be open the compressed and then the encryption as a result it will be difficult to recognized the file data for the unauthorized person. Delphi 6.0 language was used to write the algorithm and then applied it to a group of digital image.

References

- 1) A. Menezes, P. Van Oorschot, and S. Vanstone, Handbook of Applied Cryptography, CRC Press, 1996.
- 2) Tom Davis, RSA Encryption, tomrdavis@earthlink.net, math circles, October 10, 2003.
- 3) Weisstein, Eric W., RSA Encryption, Math World--A Wolfram, 2008.
- 4) Anil, K. J., Fundamentals of Digital Image Processing, Prentice-Hall of India Private Limited, New Delhi, 1995.
- 5) Dr Sandra I. Woolley, Multimedia Data Compression, Electronic, Electrical and Computer Engineering, UK, 2008.
- 6) Nelson, M. and Gailly, J. L., The Data Compression Book, M&T Books, New York, 1992.
- 7) Guy E. Blelloch, Introduction to Data Compression, Computer Science Department Carnegie Mellon University blelloch@cs.cmu.edu, October 16, 2001.
- 8) Umbaugh, Scott E., Computer Vision and Image Processing A practical Approach using CVIP Tools, Prentice Hall, Inc, 1998.
- 9) Amara Graps, An Introduction to Wavelets, Institute of Electrical and Electronic Engineers, USA, 2004.
- 10) Eric J. Stollnitz, Tony D. DeRose, and David H. Salesin, Wavelets for Computer Graphics: A Primer. IEEE Computer Graphics and Applications, July 1995.
- 11) Eric J. Stollnitz, Tony D. DeRose, and David H. Salesin, Wavelets for Computer Graphics: Theory and Applications, Morgan Kaufmann, San Francisco, 1996.
- 12) Jacques L., Morlet Wavelets and Transform, Mon Nov 13 EST, 1995.