Wavelet-based Image Compression of Quasi Encrypted Grayscale Images

S. Suresh Kumar
Department of Electronics and Communication Engineering,
Coimbatore Institute of Engineering and Technology,
Coimbatore,
Tamilnadu,
India.

H. Mangalam
Department of Electronics and Communication Engineering,
Sri Krishna College of Engineering and Technology,
Coimbatore,
Tamilnadu,
India

ABSTRACT

As data is exchanged quickly in electronic way, information security plays a vital role in transmission and storage. Digital images are widely used in industrial purpose, so it is necessary to protect image from unauthorized access. Quasi group encryption is used to encrypt the grayscale image to provide security during transmission. Computer images are extremely data intensive and hence require large amounts of storage space. As a result, the transmission of an image from one machine to another can be very time consuming. By using image compression techniques, it is possible to remove some of the redundant information contained in images, requiring less storage space and less time to transmit. This paper is focused on selecting the most appropriate wavelet function for a given encrypted grayscale image compression. The Discrete Meyer wavelet function gives high compression ratio and the improved PSNR (peak signal to noise ratio) value for an encrypted grayscale image at decomposition level three.

Keywords

Quasi-group, PSNR (peak signal to noise ratio), wavelet function, compression ratio, data intensive.

1. INTRODUCTION

With the growth of multimedia technology over the past decades, the demand for digital information increases dramatically. The advances in technology have made the use of digital images prevalent to a large extent. Still images are widely used in applications like medical and satellite images. Digital images are comprised of an enormous amount of data. Reduction in the size of the image data for storing and transmission of digital images are becoming increasingly important as they find more applications. When the storage space or communication bandwidth is low, image is often compressed. It is necessary to reduce the size of the image with respect to bandwidth limited channel. In transmission and storage of images, security is an important issue, and one way to ensure security is the use of encryption. Consider an example, the plaintext X and the encryption function is a stream ciphertext represented by Y=$X \oplus K$, where K is the secrete key/hidden key and Y is the ciphertext. The operator (encryption) $\oplus$ is the exclusive bitwise operator [1].

Symmetric encryption is a form of cryptosystem in which encryption and decryption are performed using the same key. The most widely used symmetric cipher are DES (Data Encryption Standard) and AES (Advanced Encryption Standard). A symmetric encryption scheme has five components, a) Plain text-original data b) Encryption algorithm-performs various substitutions and transformations on plain text c) Secrete key-value is independent of the plain text d) Ciphertext-scrambled data e) Decryption-reverse of the encryption algorithm to produce/reconstructed original data. The Data Encryption Standard has been the most widely used. Cipher uses 64-bit block and a 56-bit key. The Advanced Encryption Standard is a block cipher intended to replace DES for commercial applications. It uses 128-bit block size and key size of 128,192 or 256 bits. RC4 is a variable key size stream cipher with byte-oriented operations. RC4 algorithm is based on the use of a random permutation [2].

Secure encryption algorithm must withstand the attacks such as cipher text-only attack, known-plaintext attack, chosen-plaintext attack and exhaustive key attack [3]. This paper proposes a symmetric cryptographic technique called quasi-group. The quasi-group encryptor has a very good scrambling property. The purpose of the scrambler is to maximize the entropy at the output.

The basic goal of image compression is to represent an image with minimum number of bits of an acceptable image quality. All image compression algorithms strive to remove statistical redundancy and exploit perceptual irrelevancy while reducing the amount of data as much as possible. Image compression schemes can be broadly classified into two types: Lossless compression and Lossy compression. In lossless compression, the image after compression and decompression is identical to the original image and every bit of information is preserved during the decompression process. The reconstructed image after compression is an exact replica of the original one. Although lossless compression methods have the appeal that there is no deterioration in image quality, this scheme only achieves a modest compression rate. The lossless compression scheme is used in applications where no loss of image data can be compromised. Lossless compression scheme is preferred in the case of medical image compression. In lossy compression, the reconstructed image contains degradations with respect to the original image. Here prefect reconstruction of the image is sacrificed by the elimination of some amount of redundancies in the image to achieve a higher compression ratio. In lossy compression, a higher compression ratio can be achieved when compared to lossless compression [4].

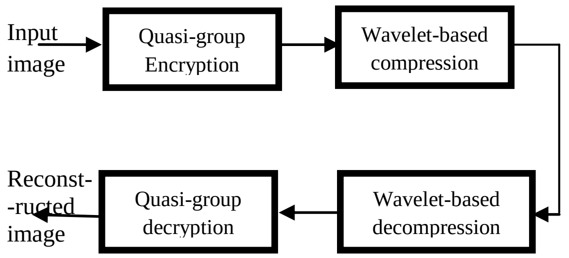

Figure 1 Proposed approach

When network bandwidth and storage space is limited, data is often compressed. It is necessary to protect the image during transmission from unauthorized access. So encryption is performed prior to compression. At the receiver side, compressed image is decompressed first and then decrypted.

2. QUASI-GROUP ENCRYPTION AND DECRYPTION

A quasi-group encryptor has a very good scrambling property and therefore it has a potential use in symmetric cryptography. The purpose of scrambler is to maximize the entropy at the output [5]. If $a_1,a_2,a_3,\ldots,a_n$ belong to a quasigroup(Q) then the encryption operation QE(Quasi-Encryptor) which is defined over elements, maps those elements to another vector $b_1,b_2,b_3,\ldots,b_n$.

The mathematical equation for encryption is defined by,

$$E(a_1,a_2,a_3,\ldots,a_n)= b_1,b_2,b_3,\ldots,b_n \quad \text{----------.} \ (1)$$

where $b_1=a*a_1,b_i=b_{i-1}*a_i$, i increments from 2 to the number of elements that are to be encrypted and a is the secrete key/ hidden key.

A quasi-group decryption process is similar to the encryption, the main point to note is generation of inverse matrix.The mathematical equation for decryption is defined by,

$$D(a_1,a_2,a_3,\ldots,a_n)=e_1,e_2,e_3,\ldots,e_n \quad \text{-----------} \ (2)$$

where $e_1=a/a_1$ and $e_i=a_{i-1}/a_i$

2.1 Encryption Algorithm

Input: *Image, Encryption Key*
Output: *Encrypted Image*

1. Get the size of the image and store it.
2. Convert image matrix into a vector.
3. Construct a new image matrix by filling the odd position values followed by even position values.
4. Convert a new image matrix into a vector.
5. Binary key *data* is embedded in the vector and the resulting vector is stored.
6. Convert the vector into image matrix.

2.2 Decryption Algorithm

Input: *Encrypted Image, Decryption Key*
Output: *Decrypted Image*

1. Convert the encrypted image matrix into a vector.
2. The binary key is initially used for decryption and stored as a vector.
3. Vector is converted to image matrix.
4. Image matrix is divided into two vectors and new image matrix is created by filling the odd and even positions.
5. The resulting image matrix is the decrypted image.

The encrypted images are compressed by either loss or lossless compression scheme before transmitting it in the bandwidth limited channel. Table 1 shows the duration for performing the encryption and decryption operation on various images.

Table 1
Quasi-group Encryption and Decryption duration in seconds

Image	Encryption(s)	Decryption(s)
Cameraman	0.2563	0.3643
Lena	0.2560	0.3704
Barbara	0.2600	0.3699

The encryption and decryption durations of Quasi-group are compared with Mirror-like Image Encryption (MIE) algorithm and Visual Cryptography (VC) algorithm in table 2. Mirror-like Image Encryption algorithm is based on a binary sequence and it includes 7 steps. Visual Cryptography method includes two steps. First it transforms grayscale image into four halftone images (Cyan, Magenta, Yellow and Black) and then in second step two transparencies of VC are generated. The secret image is obtained by stacking two transparencies [6].

Table 2
Comparison of Encryption and Decryption algorithms duration in seconds

Algorithm	Image	Encryption(s)	Decryption(s)
MIE	Lena	.27	.22
MIE	Baboon	.49	.22
VC	Lena	1.98	-*
VC	Baboon	3.57	-*
QG	Lena	.2560	.3704
QG	Baboon	.2686	.3658

MIE-Mirror-like Image Encryption
VC-Visual Cryptography for Images
QG-Quasi-Group

It can be observed that quasi-group algorithm takes less time for performing encryption and decryption as compared to VC and takes less time for performing encryption as compared to MIE.

3. WAVELET TRANSFORM

Wavelet transform (WT) represents an image as a sum of wavelet functions (wavelets) with different locations and scales. Any decomposition of an image into wavelets involves a pair of waveforms: one to represent the high frequencies corresponding to the detailed parts of an image (wavelet function) and one for the low frequencies or smooth parts of an image (scaling function).Wavelet transform has achieved considerable attention in the field of image processing due to its flexibility in representing non-stationary image signals and its adapting to human visual characteristics. Their inherent capacity for multiresolution representation akin to the operation of the human visual system motivated a quick adoption and widespread use of wavelets in image processing applications. A wavelet transform divides a signal into a number of segments, each corresponding to a different frequency band [7].

A Fourier transform does not give information about the time at which particular frequency has occurred in the signal. Hence, a Fourier transform is not an effective tool to analyse a non-stationary signal. To overcome this problem, windowed Fourier transform, or short-time Fourier transform was introduced. Even though a short-time Fourier transform has the ability to provide time information, multiresolution is not possible with the short-time Fourier transforms. Wavelet is the answer to the multiresolution problem. A wavelet has the important property of not having a fixed-width sampling window. The wavelet transform can be broadly classified into (i) Continuous wavelet transform and (ii) Discrete wavelet transform. For long signals, continuous wavelet transform can be time consuming since it needs to integrate over all times. To overcome the time complexity, discrete wavelet transform was introduced. Discrete wavelet transform can be implemented through sub-band coding. The DWT is useful in image processing because it can simultaneously localise signals in time and scale, whereas the DFT or DCT can localise signals only in the frequency domain. The Discrete Wavelet Transform (DWT) is obtained by filtering the signal through a series of digital filters at different scales. The scaling operation is done by changing the resolution of the signal by the process of sub sampling [8].

3.1 Wavelet Families

There are many members in wavelet families, they are a) Haar b) Daubechies c) Symlets d) Coiflets e) Meyer f) Mexicanhat g) Morlet. The haar, daubechies, symlets, coiflets wavelets are supported by orthogonal wavelets. The meyer, mexicanhat, morlet wavelets are symmetric in shape. Based on their scaling function (or shape) and ability to analyze the signal, the wavelets are chosen for particular application [9].

(a) Haar:Any discussion of wavelets begins with Haar wavelet, the first and simplest. Haar wavelet is discontinuous, and resembles a step function. It represents the same wavelet as Daubechiesdb1. Figure 2 shows the wavelet function of haar in which x-axis represents the time and y-axis represents the frequency.

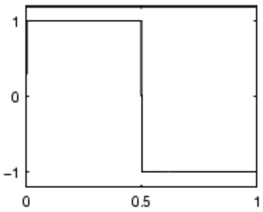

Figure 2 Wavelet function of Haar

(b) Daubechies: The daubechies wavelets are compactly supported orthonormal wavelets thus making discrete wavelet analysis possible. Daubechies family wavelets are written dbN, where N is the order, and db the "surname" of the wavelet. The db1 wavelet, as mentioned above, is the same as Haar wavelet. Figure 3 shows the wavelet function of daubechies in which x-axis represents the time and y-axis represents the frequency.

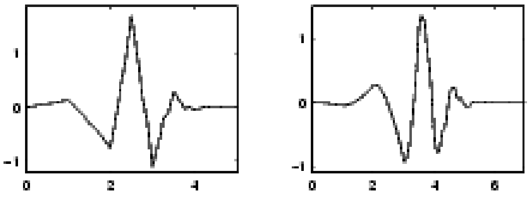

Figure 3a **Figure 3b**

Figure 3(a,b) Wavelet function of daubechies (db3,db4) families

(c) Symlets: The symlets are nearly symmetrical wavelets proposed by Daubechies as modifications to the db family. The properties of the two wavelet families are similar. Figure 4 shows the wavelet function of symlet in which x-axis represents the time and y-axis represents the frequency.

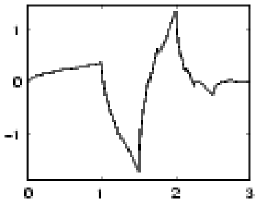

Figure 4 Wavelet function of Sym2

(d) Coiflets: The wavelet function has 2*N* moments equal to 0 and the scaling function has 2*N*-1 moments equal to 0. The wavelet function and scaling function have a support of length 6*N*-1. Figure 5 shows the wavelet function of coiflet in which x-axis represents the time and y-axis represents the frequency.

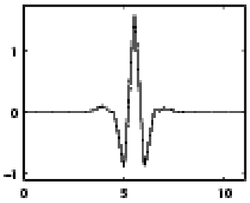

Figure 5 Wavelet function of coif2

(e) Meyer: The wavelet and scaling function are defined in the frequency domain. Figure 6 shows the wavelet function of meyer in which x-axis represents the time and y-axis represents the frequency.

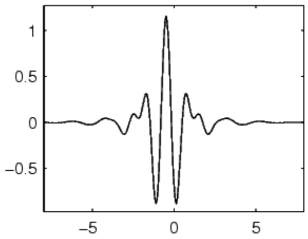

Figure 6 Wavelet function of meyer

4. COMPRESSION METRICS

The steps involved in compression and decompression are 1) Load the image 2) Generate the compressed image 3) Calculate compression ratio 4) Calculate MSE and PSNR for original and output image. 5) Obtain reconstructed image. Depending on the type of compression technique employed, the type of compression metrics used for digital image varies. The basic metric, compression ratio (3) is used to evaluate the performance of compression algorithm.

$$\text{Compression ratio} = \frac{\text{Output file size(bytes)}}{\text{Input file size(bytes)}} --(3)$$

The mean square error (MSE) is useful to measure an average value of energy lost in lossy compression of original image. A very small MSE (4) value can be taken to mean that the image is very close to original.

$$\text{MSE} = \frac{1}{\text{MN}} \sum_{\text{Y}=1}^{\text{M}} \sum_{\text{X}=1}^{\text{N}} [\text{I}(\text{X},\text{Y}) - \text{I}'(\text{X},\text{Y})]^2 --- (4)$$

The peak signal-to-noise ratio (PSNR) is the ratio peak signal power to noise power. The common use of the PSNR is to measure the quality of reconstructed images that have been compressed. Each picture element (pixel) has a color value that can change when an image is compressed and then uncompressed. Signals can have a wide dynamic range, so PSNR (5) is usually expressed in decibels, which is a logarithmic scale.

$$\text{PSNR} = 20 * \log_{10}\frac{255}{\sqrt{MSE}} ------ (5)$$

5. EXPERIMENTAL RESULTS

The image processing software package (MATLAB) is used for the image processing experiments. For the above mentioned wavelets, image compression is performed and calculated the compression ratio with different wavelet families. Results of compression ratio for different wavelet families are shown in Table 3. We have taken the test images (lena, cameraman and Barbara) and have used the Haar wavelet (haar), Daubechies wavelet (db1,db2,db5,db10) Coiflet wavelet (coif1, coif3, coif5) Symlet wavelet (sym2,sym4,sym6, sym8) and Discrete Meyer wavelet (dmey). From the results it is observed that Discrete Meyer wavelet has the higher compression ratio.

Table 3
Compression Ratio (CR) for different wavelet families with decomposition level 3

Wavelet Families	Cameraman	Lena	Barbara
Haar	97.9026	99.2093	98.6056
Db1	97.9026	99.2093	98.6056
Db2	98.0523	99.3008	98.8533
Db5	98.5288	99.4481	99.2458
Db10	98.9055	99.5835	99.4484
Coif1	98.3235	99.3292	99.0355
Coif3	98.7791	99.5563	99.4376
Coif5	99.1167	99.6627	99.5843
Sym2	98.0523	99.3008	98.8533
Sym4	98.4016	99.3867	99.1466
Sym6	98.5358	99.4851	99.2891
Sym8	99.6899	99.5245	99.4112
Dmey	99.7519	99.8559	99.7490

Quasi-group encryption is performed prior to protect the privacy. Figure 7 shows the original image. Figure 8 shows the quasi-group encrypted image. A good reconstructed image is one which has high PSNR and low MSE value. From the results, we concluded that Discrete Meyer wavelet is good for compressing the encrypted image. Figure 9 shows the first level decomposition of Discrete Meyer wavelet, figure 10 shows the second level decomposition of Discrete Meyer wavelet and figure 11 shows the third level decomposition of Discrete Meyer wavelet for encrypted image. It provides low MSE and high PSNR value at the decomposition level three. Figure 12 shows the reconstructed image and Figure 13 shows the decrypted image. Table 4 shows the MSE, PSNR and Bit rate for various images after applying Discrete Meyer wavelet function with decomposition level three.

Table 4
MSE, PSNR and Bit rate value for Discrete Meyer wavelet with decomposition level 3

Image	MSE	PSNR	Bit rate
Cameraman	2.3445	44.4303	2.4571
Lena	2.5530	44.0603	2.4764
Barbara	9.4575	38.3730	2.7319

Figure 7 Original image

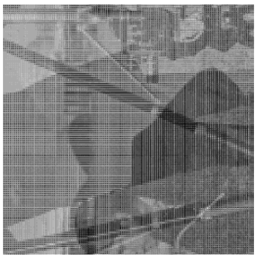

Figure 8 Encrypted image

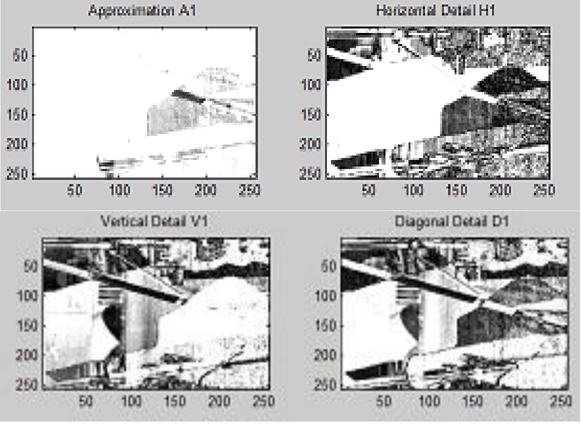

Figure 9 Discrete Meyer wavelet based compression with decomposition level 1

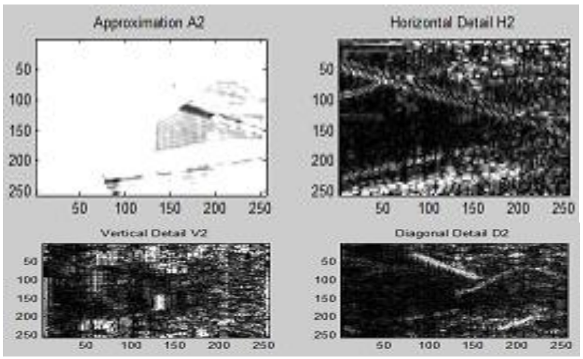

Figure 10 Discrete Meyer wavelet based compression with decomposition level 2

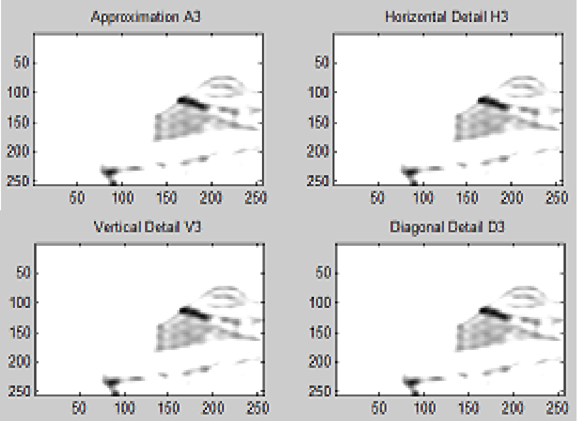

Figure 11 Discrete Meyer wavelet based compression with decomposition level 3

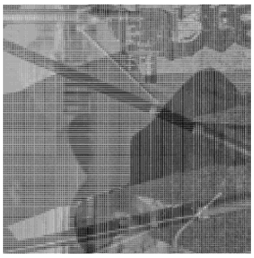

Figure 12 Level 3 reconstructed image

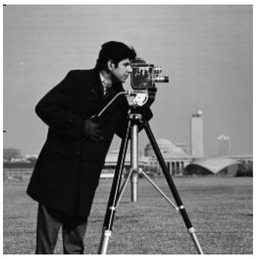

Figure 13 Decrypted image

6. CONCLUSION

In this paper we presented the compression of encrypted grayscale images. The quasi group has good scrambling, that constitutes an excellent method and generation of pseudo-random sequences. The encrypted image is compressed by using wavelet-based image compression scheme. We have applied different wavelet functions on encrypted images to get an improved PSNR value and compression ratio. We analyze the compression ratio obtained after each wavelet-based image compression and found that Discrete Meyer wavelet function provides maximum compression ratio for an encrypted image

7. REFERENCES

[1] Q.Yao, W.Zeng and W.Liu "Multi resolution based hybrid spatiotemporal compression of encrypted videos", in Proc IEEE Int.Conf.Acous.,Speech and Sig.Process.,Taipei,Taiwan,R.O.C.,Apr.2009 , pp.725-728.

[2] Howard Cheng and Xiaobo Li,"Partial Encryption of Compressed Images and Videos", IEEE Transaction on Signal Processing ,Vol.48,No.8,August 2000.

[3] William Stallings ,"Cryptography and network security", Pearson Education, second edition .

[4] Veerakumar, Jayaraman and Esakkirajan, "Digital image processing" , Tata McGraw Hill Education Private limited,2009.

[5] M.V.K.Satti, "Quasi group based cryptographic system".

[6] IsmetOzturk and Ibrahim Sogukpinar, "Analysis and comparison of Image Encryption Algorithms", World Academy of Science, Engineering and Technology 3,2005.

[7] SauravGoyal ,"Comparative study of Wavelet Families for Biomedical Image Compression", Patiala.

[8] Rafael Gonzalez and Richard Woods, "Digital Image Processing", Pearson Education, second edition,2002.

[9] Baluramnagaria, Farukhhashmi, "Comparative analysis of fast wavelet transform for image compression for optimal image quality and higher compression ratio" , IJEST,vol.3, no.5, May 2011,pp.no.4014-4019.

[10] W.C.Yen,S.C.Tai, "DCT based image compression using wavelet-based algorithm with efficient deblocking filter", In Proc of the fourth annual ACIS International Conference on Computer and Information Science, 2005.

[11] Albertus Joko Santoso, Dr. Lukito Edi Nugroho, Dr. Gede Bayu Suparta, Dr. Risanuri Hidayat, "Compression Ratio and Peak Signal to Noise Ratio in Grayscale Image Compression using Wavelet", IJCST Vo l. 2, Issue 2, Ju n e 2011.

8. AUTHORS PROFILE

H.Mangalam received her Bachelor degree in Electronics and Communication Engineering, Master degree in Applied Electronics and PhD in Information and Communication Engineering from Anna University Chennai. She currently works as a Professor in the department of Electronics and Communication Engineering at

Sri Krishna College of Engineering and Technology, Coimbatore, Tamilnadu. Her areas of research include Low power VLSI Design and testing, Digital and wireless communications, Signal and image processing. She has authored many research publications in journals and conferences.

S.Suresh Kumar received his Bachelor degree in Electronics and Communication Engineering, Master degree in Communication Systems and currently a Research scholar in department of Electronics and Communication Engineering at Anna University of Technology Coimbatore. He currently works as an

Assistant Professor in the department of Electronics and Communication Engineering at Coimbatore Institute of Engineering and Technology, Coimbatore, Tamilnadu.His areas of research include Image and video processing, communication, cryptography.