

Comparative Analysis of Image Compression Using Wavelet Transform

Dhanashri Kansal¹, Dr.Hemant Kumar Gupta², Dr. Rahul Srivastava³

M.Tech. Scholar, Department of Electronics and Communication Engineering, Arya College of Engineering & IT, Kukas, Jaipur, India¹

Professor, Department of Electronics and Communication Engineering, Arya College of Engineering & IT, Kukas, Jaipur, India²

Professor, Department of Electronics and Communication Engineering, Arya College of Engineering, Kukas, Jaipur, India³

ABSTRACT: Image authentication techniques have recently gained great attention due to its application in a large number of multimedia applications. Digital images are increasingly transmitted over non-secure channels such as the Internet. The recent growth of data intensive multimedia-based web applications has not only sustained the need for more efficient ways to encode signals and images but have made compression of such signals central to storage and communication technology. Data compression which can be lossy or lossless is required to decrease the storage requirement and better data transfer rate. One of the best image compression techniques is using wavelet transform. It is a new technique and has many advantages over other techniques. Wavelet transform uses a large variety of wavelets for decomposition of images. The state of the art coding techniques like EZW, SPIHT (set partitioning in hierarchical trees) and EBCOT(embedded block coding with optimized truncation) use the wavelet transform as basic and common step for their own further technical advantages. The wavelet transform results therefore have the importance which is dependent on the type of wavelet used. In our project, we have used HAAR wavelets to perform the transform of different test image and the results have been discussed and analyzed. The analysis has been compared based on accuracy, memory requirements and time complexity.

I. INTRODUCTION

Normally, image data can allow for lossy representations with refined degradation. The information carried by image data is mostly retained even when the image has undergone reasonable levels of filtering, geometric distortion or noise corruption.

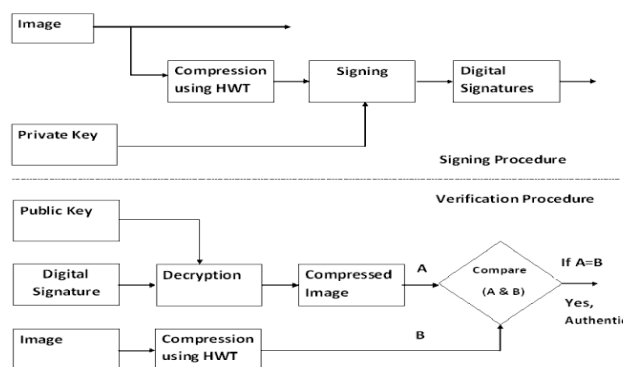


Fig. 1. Digital signature based image authentication

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Website: www.ijirset.com

Vol. 6, Issue 8, August 2017

A digital signature is used to authenticate digital information, by using computer cryptography. It is a set of features created from a medium itself. These features can be encrypted by using an encryption algorithm and store them into a file.

Digital signatures help to establish the following assurances:

1. Authenticity- The digital signature helps to assure that the signer is who he or she claims to be.
2. Integrity-The digital signature helps to assure that the content has not been changed or tampered with since it was digitally signed.

Digital Images and encryption techniques play an important role in today's multimedia world. Many encryption schemes have been proposed to provide security for digital images. Usually the symmetric key ciphering algorithms are used in encrypting digital images because it is fast and use the techniques for block and stream ciphers.

Current methods for image authentication using Digital Signatures use compression of image through wavelet transformation techniques and then this compressed image is transmitted in encrypted form as digital signatures, which are generated by the private key. At the receiver section-

1. Original Image is compressed again using same transformation technique.
2. Encrypted Compressed image is decrypted using decryption algorithm.

If both Compressed images are identical, then the received original image is authentic.

II. RELATED WORK

A number of symmetric key cryptography algorithms are developed in recent decades. In this research, technique for generating the digital signature using Data Encryption Standard (DES) has been implemented. DES is symmetric key encryption algorithm. In spite of the successful cracking of the data encryption standard by massive brute force attacks, data encryption standard algorithm is an entrenched technology and still useful for many purposes. It is fast and it achieves a good encryption rate for image ciphering using different modes of operation. DES uses a single key of length 64 bits for both encryption and decryption. The two communication parties have to share that key. The encrypted data in symmetric key cryptography can only be read by parties who have been given the necessary key to decrypt the cipher text back into its original plaintext form.

The basic block diagram of computational process used in this dissertation is shown in Fig. 2. In this dissertation two algorithms are implemented for generating robust and secure digital signature for image authentication. After implementing the algorithms their performance has been evaluated based on various parameters like Accuracy, Memory Used and Execution Time taken. At last these three parameters evaluated from both of the algorithms are compared and analyzed.

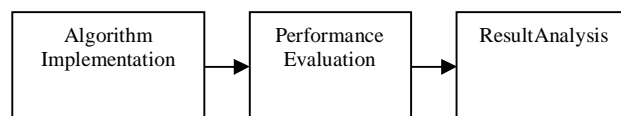


Fig. 2. Basic block diagram of computation process

The contents of proposed system have been divided in three modules:

1. Implementation of algorithm for generation and verification of digital signatures using image compression by HAAR wavelet transform (Algorithm 1).
2. Implementation of algorithm for generation and verification of digital signatures using proposed method (Algorithm 2).
3. The proposed methodology results have been compared with results from digital signatures for compressed image using HAAR wavelet transform.

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Website: www.ijirset.com

Vol. 6, Issue 8, August 2017

A. Digital signatures using image compression by HAAR wavelet transform (Algorithm 1):

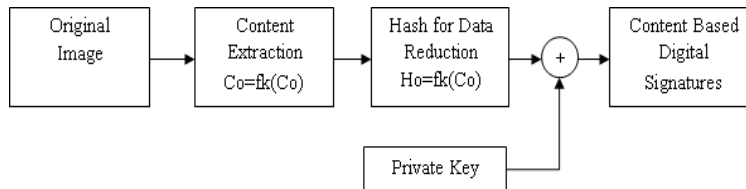


Fig.3. Generating Content based signature

Above diagram shows the sub system diagram of algorithm 1 where sender is performing the operations:

- First take an image that is to be sent.
- Compress that image using Haar wavelet transform.
- Now compressed image is encrypted using DES algorithm. Password is taken as a key.
- Now encrypted compressed image and original image is combine save into a zip file.
- This zip file is send to the receiver.

Recovery of image authentication is shown below:

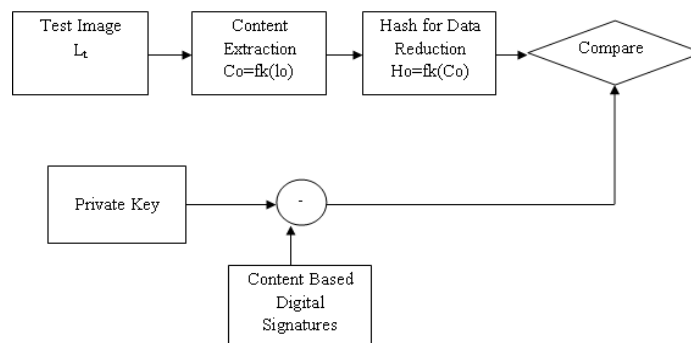


Fig. 4. Verifying content based signature

- To perform evaluation of the image first image is unzipped
- Now get two images one actual image and other the encrypted compressed image to compare.
- Input the actual image makes the same process i.e. reconstruct the low frequency image from original image.
- In other part decrypt the image from the same key as supplied in the previous encryption process.
- After recovering image from both sources compare images.

B. Digital signatures using proposed method (Algorithm 2):

Below is our proposed method to generate digital signature in this method of generation

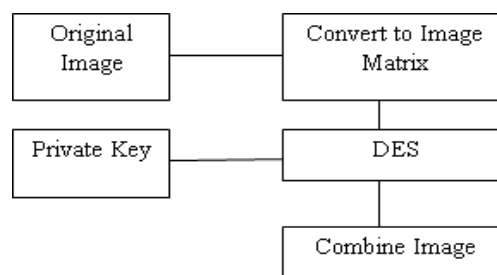


Fig. 5. Block diagram of proposed method

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Website: www.ijirset.com

Vol. 6, Issue 8, August 2017

- First image is required which is used as signature.
- After that image is converted into matrix.
- Include the DES encryption technique to encrypt the complete matrix bytes. For that purpose password is taken as a key.
- The encrypted byte matrix is written into a text file or binary file.
- For authentication combine both files actual image and the encrypted image matrix into a ZIP file.
- Send it to the client end.

At the other end extract original image and encrypted image and required to recover and match the images is it correct signature or not.

- First read the encrypted text file and apply decryption process using same key supplied at the sender side
- Recover the file
- After recovery, we match it with original image

It takes less time than wavelet transformation method because we are not performing the same process on actual image here to verify the image. It requires less time than wavelet method.

III. SIMULATION TOOLS

Software and hardware requirements on the development side system are:

1. Tools - User Interface Design (UI Design) - NetBeans IDE 6.7.1
2. Technology/Framework-Framework-JDK 1.6
3. Hardware Specifications - 3 GB storage disk, 512 MB RAM (Min), Intel P4 Processor or higher
4. Software Specifications - Windows XP or higher

IV. RESULTS

To demonstrate the results start with the formal definition of different keywords used in the evaluation.

A. Accuracy:

Here the term accuracy is defined as the difference between actual image and reconstructed images in terms of %. To calculate the accuracy we use the following given formula.

$$\text{Accuracy} = \frac{\text{totalpixelvalues} - \text{wrongpixelvalues}}{\text{totalpixelvalues}} \times 100$$

First four samples are taken to simulate the results.

S. No	Algorithm 1	Algorithm 2
1	100	99.86
2	100	100
3	100	100
4	100	100

Table 1. Performance in terms of accuracy

Accuracy of original image and decrypted image is almost same for both methods which can be shown by below graph as well. As both the methods have almost 100% accuracy, this method can be used.

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Website: www.ijirset.com

Vol. 6, Issue 8, August 2017

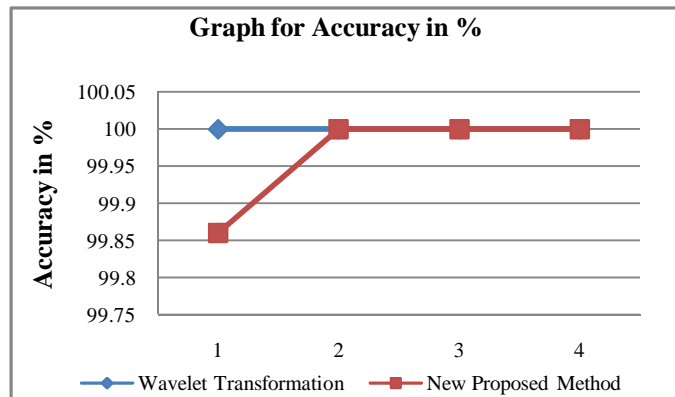


Fig. 6 Graph shows performance in terms of accuracy

B. Memory used:

Requirement of main memory to execute the algorithm is defined as memory usage. The result simulates the memory used in terms of MB.

S. No	Algorithm 1	Algorithm 2
1	18.57	13.47
2	19.25	10.55
3	19.33	13.20
4	17.71	13.91

Table 2. Performance in terms of memory

The memory used by wavelet transform image compression method is too large than proposed method as shown in below graph as well. There is significant amount of savings around 50% reduction in memory.

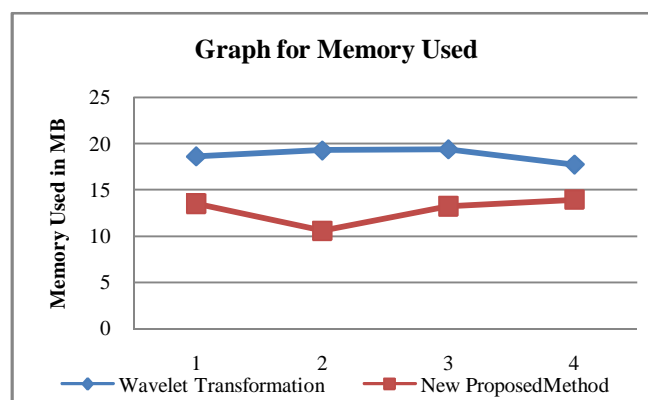


Fig. 7. Graph shows the memory used by system in terms of MB

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Website: www.ijirset.com

Vol. 6, Issue 8, August 2017

C. Execution Time:

Execution time is calculated as the time required to perform decryption and compare with the original image .The results is defined in terms of milliseconds.

The results given below is defined in terms of milliseconds

S. No	Algorithm 1	Algorithm 2
1	127	27
2	240	43
3	98	30
4	125	29

Table 3. Performance in terms of execution time

The time consumed to reconstruction of image and comparing them with original image is too long than proposed model. We can see significant reduction in time with Algorithm2. As we are going to world where the time is going to be critical, the new algorithm will help.

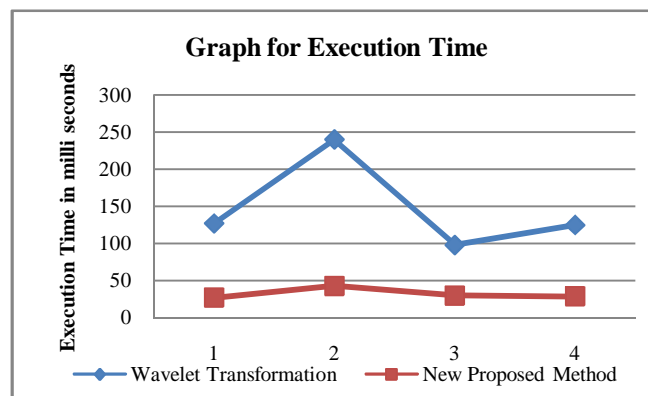


Fig. 8. Graph shows the execution time

VI. CONCLUSION AND FUTURE WORK

In this paper, the work carried out with a modified digital signature scheme for image authentication. Content-dependent structural image features and wavelet filter parameterization are incorporated into the traditional crypto signature scheme to enhance the system robustness and security. The analysis and the experimental results confirm that the proposed scheme can achieve good robustness against transmission errors and some acceptable manipulation operations. This dissertation includes the development of computationally efficient and effective algorithm for lossy image compression using wavelet techniques. The promising results obtained concerning reconstructed image quality as well as preservation of significant image details, while on the other hand achieving high compression rates. Some of the applications require a fast image compression technique but most of the existing technique requires considerable execution time and memory requirement. Results show the reduction in encoding time without degradation in image quality compared to existing methods. While comparing the developed method with proposed method memory requirement and execution time is also decreased.

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Website: www.ijirset.com

Vol. 6, Issue 8, August 2017

REFERENCES

- [1] Kamrul Hasan TalukderI and Koichi HaradaII, "Haar Wavelet Based Approach for Image Compression and Quality Assessment of Compressed Image", IAENG International Journal of Applied Mathematics, vol.- 36, issue-1, Feb 2007 pp. 1-9 , ISSN: 1311-1728.
- [2] Said F. El-Zoghdy, Yasser A. Nada, A. A. Abdo, "How Good Is The DES Algorithm In Image Ciphering?", Int. J. Advanced Networking and Applications, Vol.- 02, Issue- 05, pp. 796-803, 2011, ISSN:0975-0290.
- [3] Stallings. W, Cryptography and Network Security, (Prentice Hall, New Jersey, 2003).
- [4] P. Raviraj and M.Y. Sanavullah, "The Modified 2D-Haar Wavelet Transformation in Image compression", Middle-East Journal of Scientific Research, vol- 2,issue-2, pp. 73-78, 2007, ISSN: 1990-9233.
- [5] J Sravanthi, Dr. MHM Krishna Prasad, "ROBUST AND SECURE DIGITAL SIGNATURE FOR IMAGE AUTHENTICATION OVER WIRELESS CHANNELS", International Journal of Computer Trends and Technology, vol.- 2,issue 4, July to Aug Issue 2011,ISSN: 2231-2803, pp.245-250.
- [6] Y.-G. Wu, "GA-based DCT quantisation table design procedure for medical images", IEEE Proc.-Vis. Image Signal Process, Vol.-151, issue-5, pp 353 – 359, October 2004, ISSN: 1751-9632.
- [7] Amir Said and William A. Pearman, "An Image Multiresolution Representation For Lossless And Lossy Compression", IEEE Transactions on Image Processing, vol.-5, issue -9 ,pp. 1303-1310, 1996, ISSN. 1057-7149.
- [8] SUN Q., YE S., LIN C.-Y., "A crypto signature scheme for image authentication over wireless channel", IEEE Int. J. Image Graph., vol. - 5, issue-(1, pp. 1–14, 2005, ISSN: 0219-4678.
- [9] SCHNEIDER M., CHANG S.-F., "A content based digital signature for image authentication", Proc. IEEE Int. Conf. Image Processing (ICIP'96, pp. 227–230), 1996.
- [10] Amara Graps, "An Introduction to Wavelets" ,IEEE Computational Science and Engineering, Vol.- 2, issue- 2,1995, pp. 50-61ISSN: 1521-9615.