Implementation of Wavelet based Algorithm for Image Compression and Parametric Assessment of Digital Signature Technique

Sunil Dhankhar[1], Neetu Gupta[2]
RCEW Jaipur[12]

ABSTRACT

Security in personal data and network is a basic need now in these days. This paper is motivated by the security issues in networked system. In this paper we propose a content-based image authentication scheme that exploits structural digital signature scalability in order to achieve a good tradeoff between security and data transfer. Here we propose the multi-scale features are used to make digital signatures robust to image degradations and key dependent parametric wavelet that are characterized by excellent energy compaction and de-correlation properties and filters are employed to improve the security against forgery attacks based on the wavelet transform due to its excellent multi scale and precise localization properties. and propose a new method to design the digital signature which is fast in execution and secure in transmission media .In this paper we design and implement both technique and compare them on the basis of their performance. We include the performance parameters i.e. accuracy, memory used and build time. Experimental results demonstrate the effectiveness and validity of the proposed scheme.

Keywords: digital signature, performance analysis, Wavelet transforms, security, content-based image authentication

1. INTRODUCTION:

A digital signature or digital signature scheme is a mathematical scheme for demonstrating the authenticity of a digital message or document. A valid digital signature gives a recipient reason to believe that the message was created by a known sender, and that it was not altered in transit. Digital signatures are commonly used for software distribution, financial transactions, and in other cases where it is important to detect forgery or tampering.

Digital signatures are often used to implement electronic signatures, a broader term that refers to any electronic data that carries the intent of a signature.

Digital signatures employ a type of asymmetric cryptography. For messages sent through a non secure channel, a properly implemented digital signature gives the receiver reason to believe the was sent by the claimed sender.

Digital signatures are equivalent to traditional handwritten signatures in many respects, but properly implemented digital signatures are more difficult to forge than the handwritten type. Digital signature schemes in the sense used here are cryptographically based, and must be implemented properly to be effective. Digital signatures can also provide non-repudiation, meaning that the signer cannot successfully claim they did not sign a message, while also claiming their private key remains secret; further, some non-repudiation schemes offer a time stamp for the digital signature, so that even if the private key is exposed, the signature is valid nonetheless. Digitally signed messages may be anything representable as a bit string: examples include electronic mail, contracts, or a message sent via some other cryptographic protocol.

Two main properties are required for digital signature.

First, signature generated from a fixed message and fixed private key should verify the authenticity of that message by using the corresponding public key.

Secondly, it should be computationally infeasible to generate a valid signature for a party who does not possess the private key.

IMPLEMENTATION METHODOLOGY

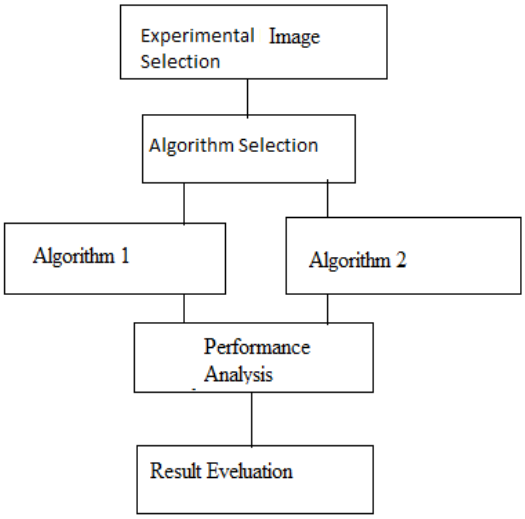

Fig. 1.1 Block diagram

Above given diagram is a basic system design of the system. Here we select the algorithm import the image over system to process it and after that we calculate the performance of the system.

Haar Wavelet Transform(Algorithm1):

Image compression is a fast paced and dynamically changing field with many different varieties of compression methods available. Images contain large amount of data hidden in them, which is highly correlated. A common characteristic of most images is that the neighboring pixels are correlated and therefore contain redundant information.

Research advances in wavelet theory have created a surge of interest in applications like image compression. In wavelet image compression, parts of an image is described with reference to other parts of the same image and by doing so, the redundancy of piecewise self-similarity is exploited.

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. A smaller file size is generated in order to achieve a faster transmission of electronic files and a smaller space for its downloading. With the increasing demand of manipulations, storage and transmission of the images, great effort has been made to develop the compression algorithms that can provide better compression ratio.

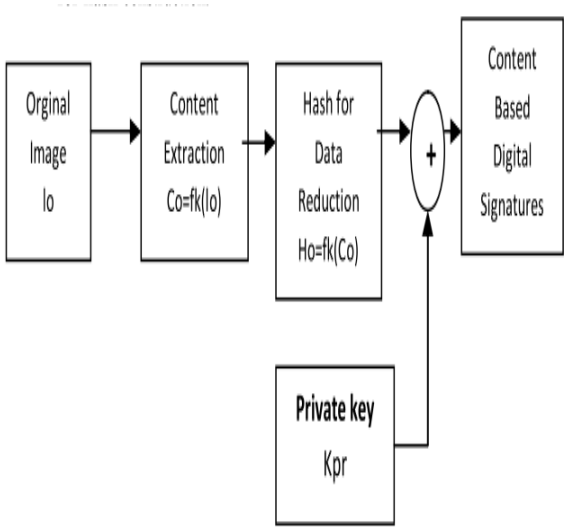

Fig. 2.2: Generating digital signature

Above given diagram shows the sub system diagram of algorithm 1

1. First required to add an image to system
2. after that extract a low frequency image using wavelet transform from the given original image.
3. Now required to add a signature over the image and send it to the client end for that purpose we prepare a hash key and use a private string to encrypt the low frequency image.
4. And combine both images encrypted low frequency image and actual image into one RAR file. This signature is sanded to the client end to recover it.

Recovery of the image and authentication of process is given below.

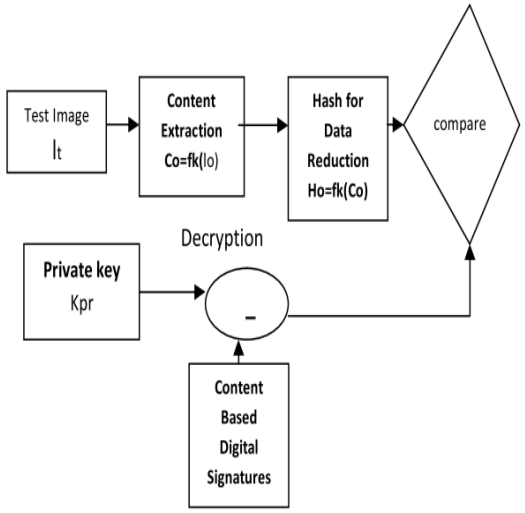

Fig. 2.3: verifying digital signature

1. To perform evaluation of the image first required unzipping the image
2. Now we get two images one actual image and other the encrypted image to compare and know is we get the correct signature.
3. We input the actual image make the same process i.e. reconstruct the low frequency image from original image
4. And in other part we decrypt the image from the same key as supplied in the previous encryption process.

After recovering image from both sources we can compare images.

Proposed Algorithm(Algorithm2):

1. in this method of generation first required the image which is used as signature.
2. Now there is a process to convert the image into matrix
3. after that we include the DES encryption technique to encrypt the complete matrix bytes. The encrypted byte matrix write into a text file or binary file for authentication we combine both files actual image and the encrypted image matrix into a ZIP file and send it to the client end.

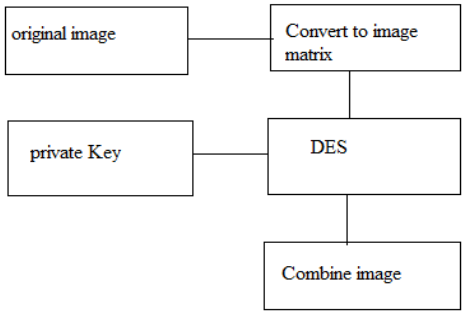

Fig. 2.4: Block diagram

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

1. First we read the text file and apply decryption process using same key supplied at the sender side
2. and recover the file after recovery we match it with the original image.

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

3. RESULTS AND DISCUSSIONS:

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

$$Accuracy = \frac{total\ values - wrong\ values}{total\ values}\ X\ 100$$

To simulate the results we use first five results of our experiment.

S. No	Algorithm 1	Algorithm 2
1	99.28	96.441
2	100	96.52
3	94.392	91.28
4	100	97.49

Table 3.1:Table shows the performance in terms of accuracy

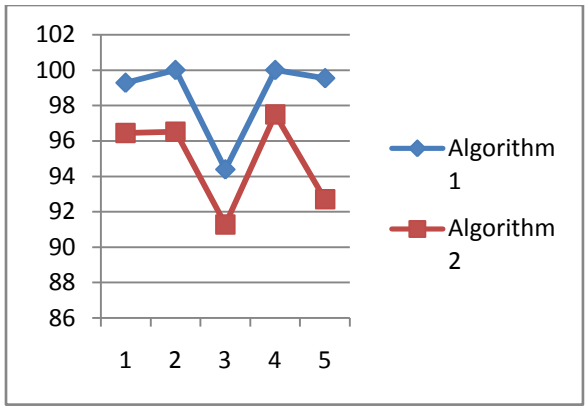

Fig. 3.1:Graph shows the performance in terms of accuracy

We can clearly see that the wave transformed image reconstruction as shown in blue color is much better than our designed algorithm and accuracy of algorithm 1 is better than our designed model.

Memory used: requirement of main memory to execute the algorithm is defined as memory uses. The results simulate the memory used in terms of MB.

S. No.	Algorithm 1	Algorithm 2
1	7.6	3.2
2	7.3	3.6
3	6.8	4.6
4	8.3	4.1
5	8.8	4.9

Table. 3.2: Table shows the memory used by system in term of MB

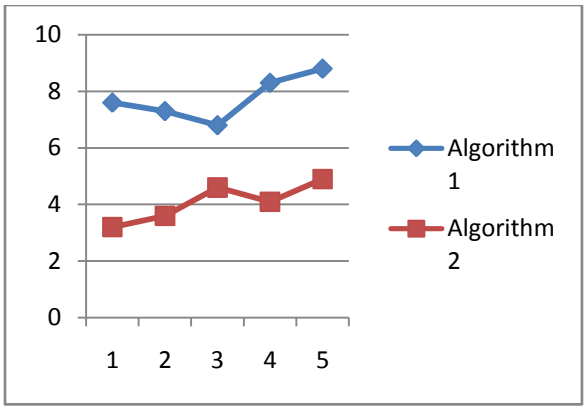

Fig. 3.2: Table and graph shows the memory used by system in term of MB

Execution Time:

To find the execution time we calculate the time required to build model results evaluation time included and we found that below given results. The results given below is defined in terms of milliseconds.

S. No.	Algorithm 1	Algorithm 2
1	239	98
2	252	105
3	284	91
4	217	97
5	296	118

Fig. 3.3 Table is shows the Execution time of the system

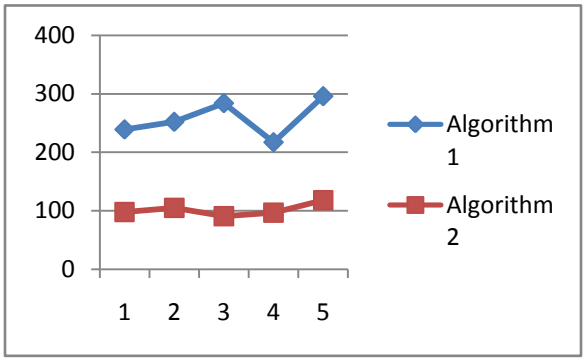

Fig. 3.3 Graph is shows the Execution time of the system

We can clearly see that the time consumed to reconstruction of image and comparing them is too long rather than our proposed model.

4. Conclusion

After implementation and result analysis of the system we find the following facts.

Algorithm	Memory Used	Time	Accuracy
Algorithm 1	High	High	High
Algorithm 2	LOW	LOW	High

Table 4:Table shows the Performances of the two systems

As we can see our conclusion table the algorithm 1 consumes maximum resources as time and memory. But as targeted network i.e. wireless network it perform high accurate results. But the system lake due to the resources likes memory and time.

But in our defined system consumes less memory and time to execute.

References:

1. SCHNEIDER M., CHANG S.-F.: 'A content based digital signature for image authentication'. Proc. IEEE Int. Conf.Image Processing (ICIP'96), 1996, pp. 227–230.
2. SUN Q., YE S., LIN C.-Y.: 'A crypto signature scheme for image authentication over wireless channel', Int. J. Image Graph., 2005, 5, (1), pp. 1–14.
3. Chengqing Li, "On the security of a class of Image Encryption Scheme", IACR's Crytology ePrint Archive: Report 2007/339, August 2007.
4. *1P. Raviraj and 2M.Y. Sanavullah:* 'The Modified 2D-Haar Wavelet Transformation in Image compression' Middle-East Journal of Scientific Research 2 (2): 73-78, 2007, ISSN: 1990-9233.
5. 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, 36:1, IJAM_36_1_9,Feb 2007.

6. Aamer Nadeem, Dr M. Younus Javed, " A Performance Comparison of Data Encryption Algorithms ", IEEE International Conference on Networking, 2009.
7. A. Pande, J. Zambreno "The secure wavelet transform" Journal of Real-Time Image Processing, vol. 18, no. 3, pp. 844-856, 2010.
8. J Sravanthi, Dr. MHM Krishna Prasad: 'ROBUST AND SECURE DIGITALSIGNATURE FOR IMAGEAUTHENTICATION OVER WIRELESS CHANNELS'International Journal of Computer Trends and Technology- July to Aug Issue 2011, ISSN: 2231-2803,pp.245-250.
9. 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 796 Volume: 02, Issue: 05, Pages: 796-803 (2011).

10. Geetika, Jyoti Chopra :' Novel Image Compression Technique With Improved Wavelet Method'. International Journal of Recent Technology and Engineering (IJRTE)
ISSN: 2277-3878, Volume-1, Issue-2, June 2012
109-114.

About the Author's

Sunil Dhankar has received his Master's in Computer Sciences. He has been associated with various National & International Societies in the field of Computer Science. He is currently associated with RCEW, Jaipur. His area of Interest includes the Image Processing & Cryptography.

Neetu Gupta has received his Bachelor's in Computer Sciences from MITS, Laxmangarh, Sikar, Rajasthan. She has been associated with various National & International Societies in the field of Computer Science. She is currently associated with RCEW, Jaipur as Research Scholar. Her area of Interest includes the Image Processing & Cryptography.