Volume 2, No. 2, Mar-Apr 2011
ISSN No. 0976-5697
International Journal of Advanced Research in Computer Science
RESEARCH PAPER
Available Online at www.ijarcs.info

An Image AuthenticationTechnique Using Watermarking and Hash Function

M.Kameswara Rao*
Lecturer, P.B.Siddhartha College,
P.G.Centre,
Vijayawada,India
kamesh.manchiraju@gmail.com

Y. Rama Krishna
Assistant Professor, KITE Women's
College of Professional Engineering Sciences,
Shabad, India
rkypragada@yahoo.co.in

K.Kiran Kumar
Reader, P.B.Siddhartha College,
P.G.Centre,
Vijayawada, India
kiran5434@yahoo.com

Abstract : The rapid expansion of the Internet has increased the availability of digital data such as audio, images and videos to the public. The advances in multimedia and communication technology have introduced new methods for manipulation and unauthorized use of digital content. Protecting multimedia information becomes more and more important from illegal duplication. Digital watermarking of images is one of the approaches to protect image data by embedding secret data within the image. This embedded data can be detected and extracted for substantiating the validity of the content at times of controversies. In this paper, watermarking based image content authentication technique is developed using hash function. The proposed method first extracts the hash value of the image, embeds it in to the image and later verifies for content authentication. Experimental simulations are provided using MATLAB 7.1. The scheme contains three phases: Hash value generation phase, embedding phase and verification phase.

Keywords— copyright protection, hash function, watermarking.
Paper submitted: Date, Revised: Date (only if applicable), Accepted: Date

I. INTRODUCTION

Due to the popularity of digital technology, more and more digital images are being created and stored every day. It is possible to duplicate digital information and distribute it over the internet. But, the availability of modern image processing tools threatened the image authenticity, by letting the user to do even imperceptible changes in the original work. Authentication verifies the integrity of an original work. In this regard, digital watermarking gave promising solution for ownership identification and authentication of work using digital images, audio, and video or text document [1]. Digital watermarking is an emerging technology for digital image authentication and copyright protection. Copyright protection is achieved by robust watermarking while image authentication is usually achieved by fragile schemes. A fragile watermarking scheme detects any manipulation made to a digital image to guarantee the content integrity while a robust scheme prevents the watermark removing unless the quality of the image is greatly reduced.

[a] Applications of Digital Watermarks:

[i] Copyright Protection & Owner Identification:
The data owner can embed watermark representing copyright information of his data. This application can be a really helpful tool in settling copyright disputes.

[ii] Copy protection: The watermarked information can directly control digital recording device. The embedded key can represent a copy-permission bit stream that is detected by the recording device which then decide if the copying procedure should go on (allowed) or not (prohibited) [3].

[iii] Data Authentication**:** Fragile watermarks are used to detect any corruption of an image or any other type of data. If the w watermark is detected, the data is genuine, if not, the data has been corrupted and cannot be considered [3].

Our proposed method creates a fragile watermark by extracting the hash value of the image and embedding the hash value in the image .At the receiver's end the hash value of the received image is recalculated and compared with the embedded hash. Any corruption in the image produces a different hash value and can be detected.

[b] Hash Function

A hash function is a function that converts an input from a (typically) large domain into an output in a (typically) smaller range (the *hash value*, often a subset of the integers). Hash functions vary in the domain of their inputs and the range of their outputs and in how patterns and similarities of input data affect output data. Hash functions are used in hash tables, cryptography and processing. In cryptography, a cryptographic hash function is a hash function with certain additional security properties to make it suitable for use as a primitive in various information security applications, such as authentication and message integrity. A hash function takes a long string (or message) of any length as input and produces a fixed length string as output, sometimes termed a message digest or a digital fingerprint [9].

A. Cryptographic Properties:

[i] Given h it should be hard to find m such that $h = \text{hash}(m)$.

[ii] Given an input m_1, it should be hard to find another input, m_2 (not equal to m_1) such that hash(m_1) = hash(m_2).

[iii] Collision-resistant: it should be hard to find two different messages m_1 and m_2 such that hash(m_1) = hash(m_2)[10].

[c] Applications of Hash Functions:

Important application of secure hashes is verification of message integrity. Determination of whether or not any changes have been made to a message (or a file), for example, can be accomplished by comparing message digests calculated before, and after, transmission (or any other event). A message digest can also serve as a means of reliably identifying a file. A related application is password verification. Passwords are usually not stored in clear text, for obvious reasons, but instead in digest form. To authenticate a user, the password presented by the user is hashed and compared with the stored hash.For both security and performance reasons, most digital signature algorithms specify that only the digest of the message be "signed", not the entire message. Hash functions can also be used in the generation of pseudorandom bits. MD2 ,MD4 ,MD5 ,N-Hash ,RIPEMD-160 ,SHA -1,Whirlpool are among the most commonly-used message digest algorithms[10].

[d] Whirlpool Hashing Function

In this paper, we used Whirlpool, which is a block-cipher-based secure hash function. WHIRLPOOL is a one-way collision resistant hash function designed by Vincent Rijmen and Paulo S. L. M. Barreto. It operates on messages less than 2^{256} bits in length, and produces a message digest of 512 bits[4]. The Whirlpool algorithm is considered secure in that it is considered computationally infeasible to find the message that produced the message digest[10].

The Whirlpool hash function can be expressed as follows:

H_0=Initial value

$H_i=W(H_{i-1}, m_i) \oplus H_{i-1} \oplus m_i$ =intermediate value

where $m_1, m_2, m_3, \ldots\ldots m_i$ are the message blocks and thus Hi is the hash code value. W is the Whirlpool block cipher. One iteration of Whirlpool is shown in the Fig 1.

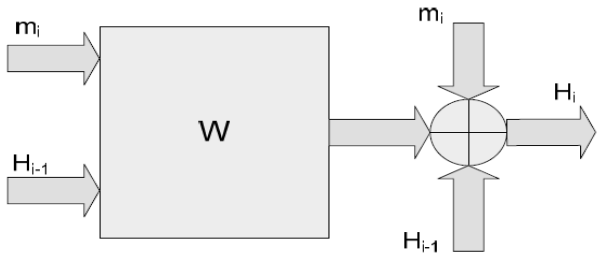

Figure 1 One iteration of Whirlpool

The complete digest is produced in four steps.

Step 1: Padding

Message is padded to odd multiple of 256 bits. In the case where the unpadded message is already of that length it is padded with 512 bits (2x256), which is the maximum padding length. Minimum is naturally 1 bit. The first padding bit is always 1 and the rest are zeros.

Step 2: Message length

The length of the unpadded message is appended to the message. The length is expressed as a 256 bit unsigned integer, with the most significant byte being the leftmost. After this step the message length is n x 512 bits (n=1, 2, …).

Step 3: Hash matrix initialization

The results of the hash function (both intermediate and final) and stored in an 8x8 matrix. Each element of the matrix is 8 bits (a byte) of the message, thus the hash matrix holds 512 bits in total.

The first matrix H0 is initialized with zeros (each byte is 0000 0000)

Step 4: Block cipher

The block cipher processes the message in 512-bit blocks.

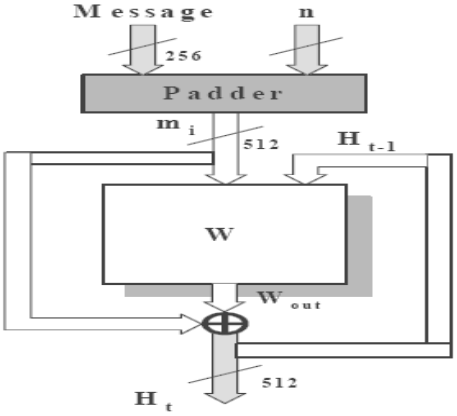

Figure 2 Generation of Whirlpool Digest

II. PROPOSED IMAGE AUTHENTICATION METHOD

Consider a image A of NR ×NC. Each pixel of A can take any of 256 gray-levels. Image A is represented by an integer matrix A:

A = [aij]NR×NC , where i = 1, 2, . . . , NR,

j = 1, 2, . . . , Nc, and aij € {0, 1, . . . ,255}.

The proposed method includes the following steps

Step 1: Create a bit string by concatenating 4 MSB's of each pixel of the original gray scale image .

Step 2: Calculate the hash value of the bit string using WHIRLPOOL hash algorithm.

Step 3 : Embed the hash value in the nth bit plane of the original image .The nth bit plane can be any of the 8 bit positions of a pixel.

Step 4 : The Hash Value is extracted from the nth bit plane and verified by recalculating the hash of the 4 MSB's of the received image .

III. EXPERIMENTAL RESULTS

The simulations were conducted on Intel machine with 2.4 GHz processor and 512 MB of RAM. MATLAB 7.1 was used for implementation of proposed scheme and image processing operations respectively.

Applying the proposed method on 512X512 Lena JPEG image.

Figure 3 Original Lena 512X512 image
Figure.3 shows the original Lena JPEG image

Hash value is calculated over the 4 MSB's of each pixel in the image using Whirlpool hash algorithm. It produces a message digest of 512 bits. The gray scale image contains 8 bit planes and the hash value can be embedded in any of the bit planes

Figure 4(a) Lena Image with Embedded hash in 1st bit plane

Figure 4(b) Lena Image with Embedded hash in 2nd bit plane

Figure 4(c) Lena Image with Embedded hash in 3rd bit plane

Figure 4(d) Lena Image with Embedded hash in 4th bit plane

Figure 4(e) Lena Image with Embedded hash in 5th bit plane

Figure 4(f) Lena Image with Embedded hash in 6th bit plane

Figure 4(g) Lena Image with Embedded hash in 7th bit plane

Figure 4(h) Lena Image with Embedded hash in 8th bit plane

Figure 4(a)-(h)shows the Lena Image with Embedded hash in the 1st,2nd ,3rd,4th,5th,6th,7th,8th bit planes .

Applying the proposed method on 512X512 Earth PNG image.

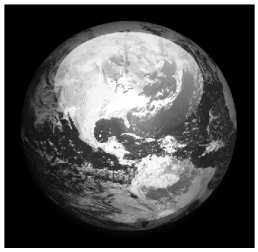

Figure 5 Original Earth 512X512 Earth PNG image

Figure.5 shows the original Earth image

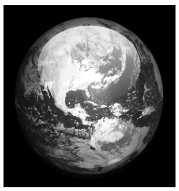

Figure5(a) Earth Image with Embedded hash in 1st bit plane

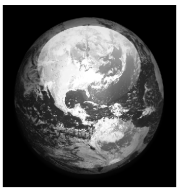

Figure 5(b)Earth Image with Embedded hash in 2nd bit plane

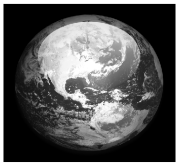

Figure 5(c) Earth Image with Embedded hash in 3rd bit plane

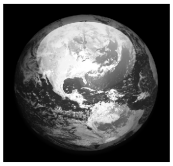

Figure 5(d) Earth Image with Embedded hash in 4th bit plane

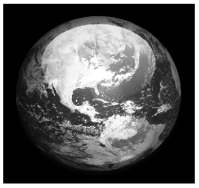

Figure 5(e) Earth Image with Embedded hash in 5th bit plane

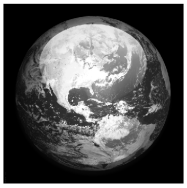

Figure 5(f) Earth image with Embedded hash in 6th bit plane

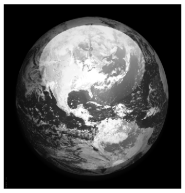

Figure 5(g) Earth Image with Embedded hash in 7th bit plane

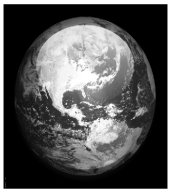

Figure 5(h) Earth Image with Embedded hash in 8th bit plane

Figure 5(a)-(h)shows the Earth Image with Embedded hash in the 1st,2nd ,3rd,4th,5th,6th,7th,8th bit planes .

It is observed that the loss of image quality is more in JPEG in comparison with the PNG image .The choice of the bit plane also affects the quality of the image.

IV. CONCLUSIONS

We have demonstrated a new image authentication technique using hash function. A hash data embedding method is proposed for image authentication. The scheme

can detect whether any modification is done on the original image. This technique works well with images of all sizes. Further this work can be extended for color images and also the method can be extended by using both symmetric and asymmetric cryptographic methods of generating digital signature of the image for authentication and copyright protection.

V. REFERENCES

[1] Samia Boucherkha and Mohamed Benmohamed "A Lossless Watermarking Based Authentication System For Medical Images", World Academy of Science, Engineering and Technology, 1-2005

[2] M. Hamad Hassan, and S.A.M. Gilani,"A Semi-Fragile Signature based Scheme for Ownership Identification and Color Image Authentication", World Academy of Science, Engineering and Technology 19 -2006

[3] Vallabha VH,"Multiresolution Watermarking for Digital Images Multiresolution Watermark Based on Wavelet Transform for Digital images".

[4] J. Fridrich et al, Lossless Data Embedding for All Image Formats, Proc.SPIE Photonics West, Security and Watermarking of Multimedia Contents, pp. 572–583, 2002.

[5] J. Fridrich, M. Goljan and R. Du, Invertible Authentication, Proc. SPIE Photonics West, vol. 3971, Security and Watermarking of Multimedia Contents III, pp. 197-208, 2001.

[6] J. Fridrich, M. Goljan, and R. Du. "Invertible Authentication Watermark for JPEG Images." ITCC 2001, Las Vegas, Nevada, April 2–4, 2001.

[7] F. Hartung and M. Kutter, "Multimedia watermarking techniques,"Proceedings of the IEEE, vol. 87, no. 7,pp. 1079–1107, July 1999.

[8] C.-S. Lu, H.-Y.M. Liao and C.-J. Sze, "Combined Watermarking for Image Authentication and Protection," Proc. IEEE Int. Conf. on Multimedia and Expo, vol.3, pp. 1415–1418, August 2000.

[9] D. R. Stinson, Cryptography, Theory and Practice, CRC Press, (1995).

[10] William Stallings,"Cryptography and Network Security"(Fourth Edition.Pearson,2005).