Wavelet Signature for the Image and Document Authentication

Sridevi Tengale
Student, M tech IV SEM,
PDA College of Engineering Gulbarga

Padmapriya Patil
PDA College of Engineering
Gulbarga

ABSTRACT
This paper takes a content-based robust and secure image and document authentication technique which makes use of structural digital signature scalability in order to achieve a good tradeoff between security and data transfer. Here the multi-scale features are used to make digital signatures robust to image degradations and key dependent parametric wavelet 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.

General Terms
DWT (discrete wavelet transform), information security, AES encryption algorithm.

Keywords
Wavelet signature, image authentication, DWT

1. INTRODUCTION
Recent advances in networking and digital media technologies have created a large number of networked Multimedia applications. These multimedia application often implemented in distributed network environment. Distributed network environment makes multimedia contents (image, document (text files), audio, and video) vulnerable to privacy and unknown attacks. For insecure environments, it is possible for an enemy to tamper with images and alter the content of any documents during transmission. To guarantee trustworthiness, image authentication techniques have emerged to confirm content integrity and prevent forgery.

When a person wish to send documents via mail or upload resume for job application then there are, the chances of third party to alter the contents of document. And equally the authentication of documents issued by the government such as birth certificates, driver licenses, and passports is a must. To protect the authenticity of multimedia images, many approaches have been proposed. These approaches consist of conventional cryptography, the fragile and semi-fragile watermarking and digital signatures that are based on the image content. The aim of this paper is to present emerging technique for image as well as document authentication with the use of a wavelet signature.

Documents can be authenticated using wavelet signature. The wavelet signature can be obtained by encrypting hashed value of message with the private key which is the wavelet coefficients obtained by the DWT of sender /author image for authentication purpose.

The objective is to design a digital signature scheme that allows two parties to exchange images while guaranteeing both image integrity and non-repudiation from the image sender, and also to prevent the modification of contents of documents over a lossy channel. At semi-fragile level, watermark-based approaches only work for protecting the integrity of the image but not for preventing sender repudiation. Signature-based methods can work on both the integrity protection of the image and the repudiation prevention of the sender.

2. RELATED WORK
Methods of image content authentication can be categorized into either digital signature based or watermarking based. Signature (or crypto-hash) is a set of extracted features, which captures the essence of image content in compact representation. It is stored as an extra file and later used for authentication. Signature based methods can work on both the integrity protection of the image and repudiation prevention of the sender.

Watermarking, on the other hand, is an method that really embeds a message into an image data and the hidden message is later extracted to verify the authenticity of image content. Watermark-based approaches only work for protecting the integrity of the image. The major difference between a watermark and a digital signature is that the embedding process of the former requires the content of the media to change.

The relationship between the content-based feature and the system security [4] proposed. It consists of feature selection for semi-fragile signature-based authentication systems. The histogram of an image represents the relative frequency of occurrence of the various gray levels in the image **[I] [S].** It is actually a global measure of an image and unable to characterize the local changes in the image. Therefore it is too robust to be used as the feature for image authentication in most cases. The histogram of original image and its attacked image is taken histograms look very similar although they are different images.

The digital signature is proposed [3] that is composed of structural information is content-dependent and provides security against forgery attacks. The SDS is constructed in the wavelet transform. In the wavelet domain of an image, the so-called joint (inter-scale) parent-child pairs exist. Parent-child pairs have been confirmed to be uncorrelated but statistically dependent. This dependency mainly arises from the perceptually important semantic features, e.g., edges and textures. Based on these semantic features, the so-called structural digital signature is constructed to simultaneously resist against incidental manipulations (e.g., JPEG/JPEG2000 compression) and reflect malicious distortions.

Each parent-child pair maps to a set of spatial pixels, which is of *non-fixed* size and possesses certain contextual dependencies. Under these circumstances, there is no clue (how to determine the size of a block?) that can be utilized to make the collage attack success. This is the advantage of adopting the multi-scale structure of wavelets in designing an image's signature.

The methodology for designing content based digital signatures is been [2] proposed which can be used to authenticate images. Here the intensity histogram is used to sign the image however; the histogram of the entire image itself is not very useful, since it contains no spatial information about the image intensities.

Thus the images were divided into blocks and the intensity histogram for each block was computed separately. This allows some spatial information to be incorporated into the signature since the location of these blocks is fixed.

3. PROPOSED METHODOLOGY

3.1 Generation of Wavelet Signature for Image Authentication

In the proposed scheme "The Image Authentication over Wireless Networks" The wavelet signature is used for image authentication. **Image signing**: In this scheme "The Image Authentication over Wireless Networks" the image to be sent over the wireless channels, the system generates a digital signature by performing a signing process on the image in the following order:

(1) Decompose the image using parameterized wavelet filters; (2) Extract the SDS; (3) Cryptographically hash the extracted SDS, generate the crypto signature by the image sender's private key. This generated crypto signature is called as wavelet signature.

SDS: Digital signature scheme is based on the wavelet transform due to its excellent multi-scale and precise localization properties. Basically, the multi-scale representation of an image is by nature highly suitable for designing a structural digital signature. The same SDS algorithm [8] as used with the employment of wavelet filter parameterization to increase security in our proposed system.

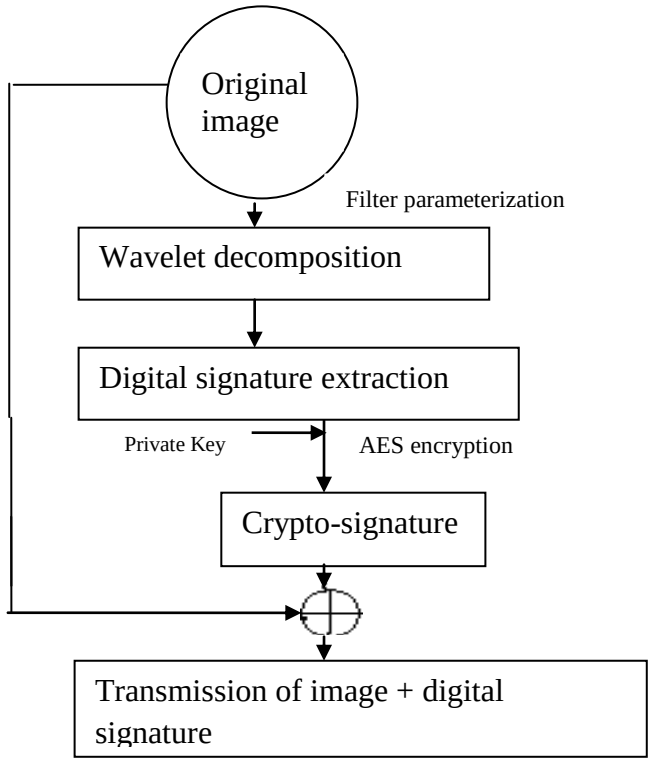


Fig 1: Block diagram of image signing procedure

3.2 Wavelet transform

Before going to wavelet transform we must know about the wavelets. A wavelet is a waveform of effectively limited duration that has an average value of zero. In mathematical term wavelets are mathematical functions that cut up data into different frequency components, and then study the each component with a resolution matched to its scale. Fig.2 shows the comparison of wavelets with that of sine waves, which are the basis of Fourier analysis. Sinusoidal signals don't have limited duration they extend from minus to plus infinity. Where the sinusoids are smooth and predictable, wavelets will become irregular and the asymmetric. The Fourier analysis consists of breaking up a signal into sine waves of various frequencies. In the same way, wavelet analysis is the breaking up of a signal into shifted and scaled versions of the original (or mother) wavelet.

Fig 2: Comparison of sine wave and wavelet

Fig.2 shows that signals with sharp changes might be better analyzed with an irregular wavelet than with a smooth sinusoid. It also makes sense that local features can be described better with wavelets that have local extent. So wavelet has advantages over traditional Fourier methods in analyzing physical situations where the signal contains discontinuities. Wavelets were developed independently in the fields of maths, quantum physics and electrical engineering.

Wavelet Transform is used to split the signal into a bunch of signals and represents the original signal, but all them corresponds to different frequency bands. The principle advantage is they provide what frequency bands exists at what time intervals. Wavelet transform of any function f at frequency a & time b is computed by correlating f with wavelet atom as

$$W\ f\ (a, b) = \frac{1}{\sqrt{a}} \int_{-\infty}^{\infty} f(t)\, \psi(t - b/2)dt \quad (1)$$

It provides time-frequency localization. Wavelet transform is always defined in terms of a 'mother' wavelet ψ and a scaling function φ, along with dilated and translated versions. Applying wavelet transform on 1D signal, it can correctly detect the similarity in a signal. For the images, the 2D scaling function [φ (x, y)] and the mother wavelet [ψ (x, y)] is defined as tensor products of the following 1-D wavelets ψ (x), ψ (y) and scaling functions φ(x), φ(y).

Scaling function

$$\phi(x, y) = \phi(x) \times \phi(y) \quad (2)$$

Vertical wavelets

$$\psi\hat{}\ y(x, y) = \phi(x) \times \psi(y) \quad (3)$$

Horizontal wavelets

$$\psi\hat{}\ x(x, y) = \psi(x) \times \phi(y) \quad (4)$$

Diagonal wavelets

$$\psi\hat{}\ d(x, y) = \psi(x) \times \psi(y) \quad (5)$$

The use of wavelet transform on image shows that the transform can analyze singularities easily that are horizontal, vertical or diagonal. So we can use the directional resolving power of wavelet in the image.

4. DOCUMENT AUTHENTICATION USING WAVELET SIGNATURE

Distributed network environment makes multimedia contents (image, document (text files), audio, and video) vulnerable to privacy and unknown attacks. Documents can be authenticated using wavelet signature. The wavelet signature can be obtained by encrypting hashed value of message with the private key which is the cipher text obtained by encrypting the features of the sender/author image for authentication purpose.

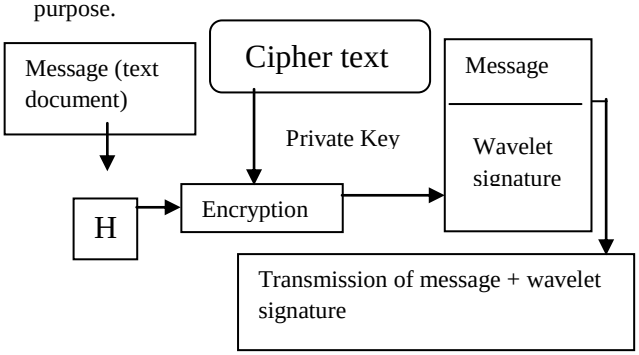


Fig 3: Diagram of document signing procedure

5. RESULTS
Image encryption:

EXAMPLE.1 (a) girlface.jpg

1(b) Result of wavelet decomposition on image

1(C) AUTHENTICATED IMAGE

DOCUMENT AUTHENTICATION:

msg =

imshreedevidoingaprojectonrobustdigitalsignaturefori
mageencryption

A =

-
«5ä- .¥[ÒqÔ ×RRRRRRRRRRRRRRRRRRRRRR
RRRRRRRRRRRRRRRRRRRRRRRRRRRR

result
= ë Ñ Õ ¹³ÂÄÁ¼·µÆÁÀÄÁ´ÇÅ
Æ¶»¹»Æ³¾Å»¹À³ÆÇÄ·¸ÁÄ»¿³¹··ÀµÄËÂÆ»ÁÀ

AR =

-
«5ä- .¥[ÒqÔ ×RRRRRRRRRRRRRRRRRRRRRR
RRRRRRRRRRRRRRRRRRRRRRRRRRRR

dec =

imshreedevidoingaprojectonrobustdigitalsignaturefori
mageencryption

FINAL RESULT

user =

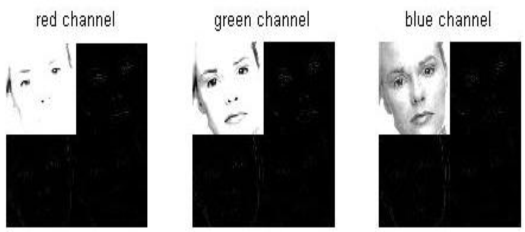
1

Authenticated

image =

EXAMPLE.2 (A) RUBY.JPG

2(B) RESULT OF WAVELET DECOMPOSITION ON IMAGE



AFTER TAMPERING ATTEMPT AND NOISE ADDITION

2(C) UNAUTHENTICATED IMAGE

DOCUMENT AUTHENTICATION:

msg =

imshreedevidoingaprojectonrobustdigitalsignatureforimageencryption

A =

Î□¼©z1Å}□Õ¶·°k¾¾¾

result =

□□□□ì□□áä²□□□□Ù□□

AR =

Î□¼©z1Å}□Õ¶·°k¾¾¾

dec =

imshreedevidoingaprojectonrobustdigitalsignatureforimageencryption

FINAL RESULT:

user =

1

UNAuthenticated

image =

7

6. REFERENCES

[1] Lou D.C., Liu J.L., Li C.-T.: 'Digital Signature-Based Image Authentication', in LU C.S. (EDS.): Multimedia security: steganography and digital watermarking techniques for protection of intellectual property' (Idea Group Inc., 2003).

[2] Schneider M., Chang S.-F.: 'content based digital signature for image authentication'. Proc. IEEE

Int. Conf. Image Processing (ICIP'96), 1996, pp. 227–230.

[3] Lu C.S.: 'On the security of structural information extraction/embedding for image authentication'. Proc. IEEE ISCAS'04, 2004, pp. 169–172.

[4] Sun Q., HE D., YE S.: 'Feature selection for semi fragile signature based authentication systems'. Proc. IEEE Workshop on Image Signal Processing, 2003, pp. 99–103.

[5] 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.

[6] Ye S., Sun Q., Chang EE-C.: 'Error resilient content based image authentication over wireless channel'. Proc.IEEE ICIP'06,2006

[7] Swami Nathan A., Mao Y., Wu M.: 'Robust and secure image hashing', IEEE Trans. Inf. Forensics Sec., 2006, 1, (2), pp.215–229

[8] Lu C.S., LIAO H.M.: 'Structural digital signature for image authentication: an incidental distortion. Resistant Scheme', IEEE Trans. on Multimed., 2003,5, (2), pp

[9] Ye S., Sun Q., Chang E.C.: 'Edge directed filter based error concealment for wavelet-based images'.Proc.IEEE Int .Conf. Image Processing, Singapore, 2004.

[10] Kanchan K Doke., S. M Patil "Digital signature scheme for image" IJCA(0975-8887) Volume49-No,16,july

[11] Lin C.-Y., Chang S.-F.: 'A robust image authentication method distinguishing JPEG compression from malicious manipulation', IEEE Trans. Circuit Syst. Video Technol., 2001, 11, (2), pp. 153-168

[12] Mark Fontenot.: 'WAVELETS INTROUCTION.' CCSC: South Central Conference, February2002