ROBUST AND SECURE DIGITAL SIGNATURE FOR IMAGE AUTHENTICATION OVER WIRELESS CHANNELS

J Sravanthi[#1], Dr. MHM Krishna Prasad[*2]

[#]*Dept. of Computer Science, UCEV*
Vizianagaram, Andhra Pradesh, India

[*]*Associate Professor &Head, Dept. Of IT,*
UCEV, Vizianagaram, Andhra Pradesh, India

ABSTRACT:

Now a days the transmission and distribution of the digital images by appending the digital signatures and content based image authentication schemes facing some triggers which are suitable for the insecure network and robust to transmission errors. The invasive distribution of digital images and the growing concern on their integrity and originality triggers an emergent need of authenticating corrupted images by transmission. To meet this need, this paper proposes a content-based image authentication scheme that exploits structural digital signature scalability in order to achieve a good tradeoff between security and data transfer. In this paper 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 multiscale and precise localization properties. Experimental results demonstrate the effectiveness and validity of the proposed scheme.

INDEX TERMS— CONTENT-BASED IMAGE AUTHENTICITY VERIFICATION ,WIRELESS IMAGE AUTHENTICATION .

1 INTRODUCTION:

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, over a lossy channel. In other words, we demand a digital signature scheme working at semi-fragile level: some manipulations on the image will be considered acceptable (e.g. lossy compression and packet loss) while some are not allowable (e.g. content copy-paste). At semi-fragile level, watermark-based approaches only work for protecting the integrity of the image but not for preventing sender repudiation [1]. Signature-based methods can work on both the integrity protection of the image and the repudiation prevention of the sender, but prior robust digital signature is unavoidably very large because its size is usually proportional to the image size [2, 3]. In order to solve these problems, efforts towards the combination of digital signature and watermarking are being explored in this paper.

To Guarantee Security, trustworthiness, image authentication techniques have proposed to confirm content integrity and prevent forgery. These authentication methods should be robust against various attacks. Such authentication techniques have wide applicability in law, commerce, journalism and national defense. 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

vulnerable to privacy and unknown attacks. For insecure environments, it is possible for an enemy to tamper with images during transmission [1].To guarantee trustworthiness, image authentication techniques have emerged to confirm content integrity and prevent forgery. These techniques are required to be robust against normal image processing and transmission errors, while being able to detect malevolent tampering on the image. Networked multimedia applications are often deployed in a distributed network environment that makes multimedia contents vulnerable to privacy and malicious attacks. For insecure environments, it is possible for an enemy to tamper with images during transmission.

Existing methods with Content-Based Digital Signature Authentication will assume reliable noise-free transport. These methods do not work well when used to transmit images over the error-prone wireless channel. For example, any transmission bit error will render traditional authentication a failure. It is clear that traditional authentication algorithms do not cope well with lossy networks and the loss-tolerant nature of the multimedia data.

The Proposed method, The Image Authentication over Wireless Networks. Here requires careful design of the authentication methodology. It Overcome all issues that we discussed above. The proposed scheme generates only one fixed-length digital signature per image regardless of the image size and the packet loss during transmission.In this scheme, 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.

2 GENERAL FRAMEWORKS FOR SIGNING PROCEDURE:

To handle the problems like the size of the generated signature is proportional to the size of the content and it makes the signing very time consuming, the other is that the basis of authentication is the correlation between feature sets and not bit-bit comparison that could cause some security problems [3]. The below figures shows the brief introduction of a semi-fragile signature used for image authentication. When it was not sacrificing accuracy and increasing the complexity, a content-dependent key (hash) has been proposed. A hash function takes a message of an arbitrary finite length and produces an output of fixed length. A robust visual hashing scheme usually relies on a technique for feature extraction as the initial processing stage [7]. Subsequently, the features are further processed to increase robustness and/or reduce dimensionality. To ensure the security of the algorithms, its features are required to be key-dependent and must not be computable without the knowledge of the key used for hash construction.

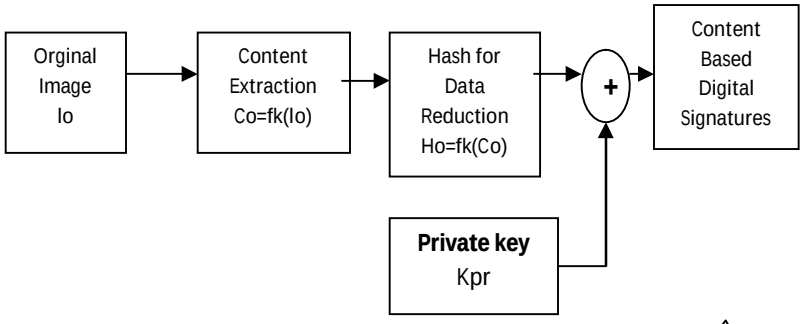


Figure 1(a): Generating Content based signature

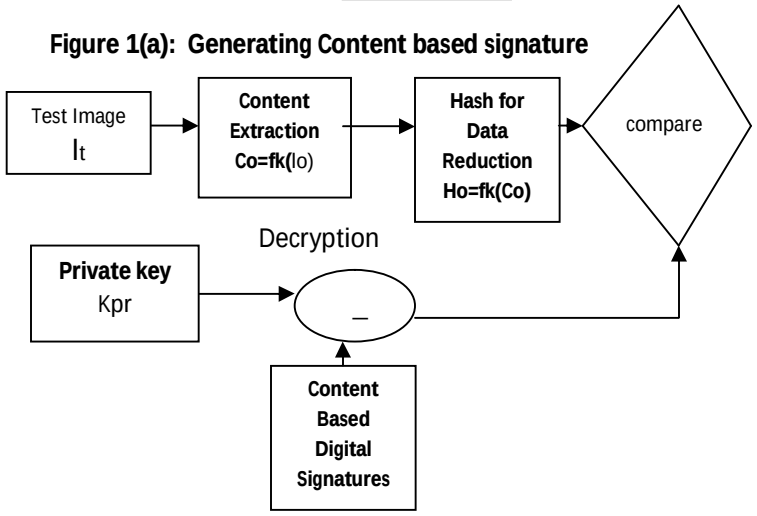


Figure 2(b): verifying Content based signature

In the construction of secure hash values is the selection of image features that are resistant to common transformations we have to face some problem. When the features to represent its corresponding content are selected, one needs to consider not only its robustness to the acceptable manipulations but also its security (sensitivity) against malicious modifications. Actually, these two requirements are contradictive and application dependent. A typical approach is to extract image features that are invariant allowing content preserving image processing operations. Our main objective of this paper is to conduct an illustrative security study of features in order to improve the

security of wireless image authentication systems without additional computational complexity.

3 OVERWIEW OF WIRELESS IMAGE AUTHENTICATION:

As discussed in the above section authenticating an image over loss wireless channels has its limits and drawbacks. We proposed a modified wireless image authentication scheme. This scheme is based on robust digital signatures generated from a secret wavelet transform of the reconstructed degraded images via an error concealment technique.

3.1 Procedure for Imaging Signing:

In the image signing procedure as depicted in Fig. 2 given 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 senders private key; and (4) Send the image and its associated crypto signature to the recipient. In consideration of robustness, no compression and coding is used, since they will cause error propagation.

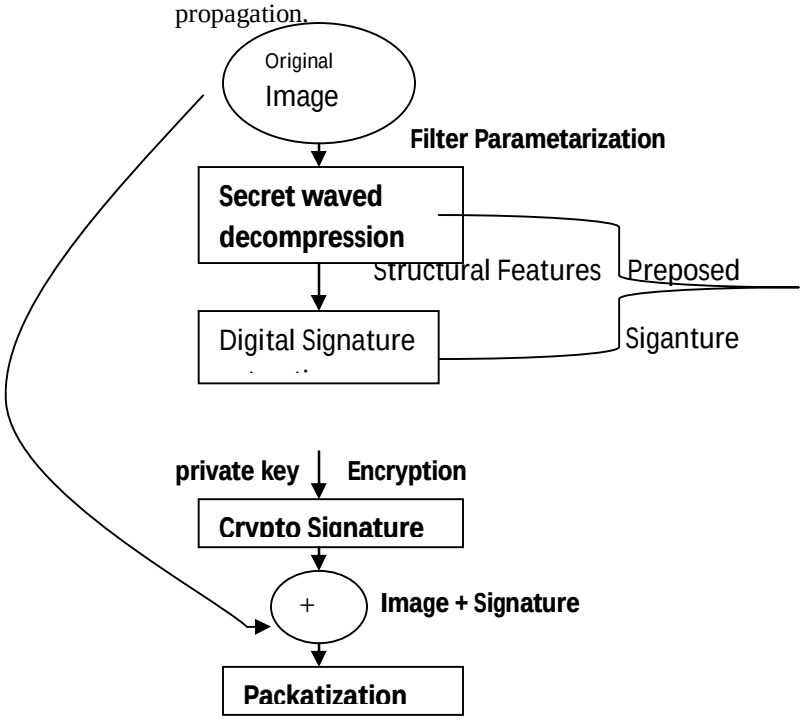


Figure 3: Diagram of image signing procedure

3.1.1 Wavelet parameterization: Wavelets have shown their importance in numerous applications mainly centered on image processing. Wavelets are functions that are localized in both time and frequency and are used to efficiently represent data. The most popular wavelets used today are the result of the seminal work of Ingrid Daubechies and are referred to as the Daubechies' wavelets. The effectiveness of a wavelet is in its ability to make a good approximation of signals or data, but each wavelet has a wide range of properties.

Transformation of the Wavelet is characterized by excellent energy compaction and de-correlation properties. Wavelets are also tolerant with respect to color intensity shifts, and can capture both texture and shape information effectively. The generated image's signature is constructed in the wavelet domain. Most conventional wavelet-based image authentication schemes reported in the literature have three shortcomings (1) Their security is questionable without protecting the coefficients used to construct the signature from malicious attacks; (2) Low robustness to some content preserving attacks; and (3) High computational complexity.To handle the above shortcomings, the concept of lifting based wavelet filter parameterization has been suggested as an effective method to improve the security and processing speed of the wavelet transform [9]. Given N parameter values

$$-\pi<\alpha_{i<}\ \pi,\ 0<i<N,$$

The recursion

$$\varepsilon_{0=}½ \text{ and } \varepsilon_1 =½ \quad \varepsilon_{k=}½((C_{k-2}{}^{n-1} + C_k{}^{n-1})(1+\cos\alpha_{n-1})) + (C2(_{n+1})^{n-1}\text{-k-1} - C2(_{n+1})^{n-1}\text{-k-3})(-1)^k \sin\alpha_{n-1)}$$

The recursion can be used to determine the filter coefficients $C_k{}^{N,}0<=k<2N+2$ and $C_k=0$ for $k<0$ and $k>=2N+2$

The parameter values used for construction and the resulting wavelet filter coefficients are kept secret. A problem with constructed parametric wavelet filters is that the high-pass/ low-pass sub-band property is partially lost. In this paper, the algorithm used by Fridrish et al. [4] has been considered to deal with this dilemma by calculating the second-order variation of the wavelet sequence.

$V^{(2)}=\xi | C_n^{(j)} - C_{n-1}^{(j)} + C_{n-2}^{(j)} |$

Employing secret filter parameterization in image authentication systems has the following advantages. First, security is improved because hostile attacks have to operate in the transform domain used for signing and authentication procedures. Secondly, filter coefficients can be constructed in an image-adaptive manner to maximize robustness against attacks. Thirdly, there is no need to modify proven authentication schemes. A wavelet transform based on secret filters can act as a security framework independent of the signing algorithm.

3.1.2 Overview of compression with feedback process: This is a wavelet-based image compression process. The overall wavelet compression-with-feedback process is shown in the below figure 3. (Feedback is shown with the dotted line.) The process can be broken down into 3 basic steps: (a) Compressing the image by encoding the wavelet coefficients of the input image, (b) Decompressing (reconstructing) the image and (c) Updating the parameters to generate a new wavelet. The image compression step consists of performing a full wavelet decomposition on the input image and then encoding the wavelet coefficients. The decompression step is just the opposite of the compression step; it is only done so that the error term can be calculated [8].

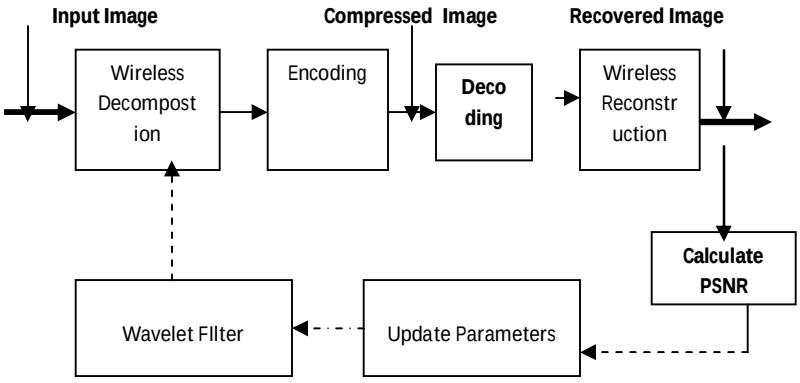


Figure 4: Outline of the wavelet-based image compression technique that modifies the wavelet based on feedback. The feedback path is shown with a dotted line.

3.1.3 Structural signature: Digital signature scheme is based on the wavelet transform due to its excellent multiscale and precise localization properties. Basically, the multiscale representation of an image is by nature highly suitable for designing a structural digital signature [5]. The same SDS algorithm as used with the employment of wavelet filter parameterization to increase security in our proposed system. In the wavelet domain of an image, the so-called joint (interscale) Parent –child pairs exist. Each parent–child pair maps to a set of spatial pixels, which is of a non-fixed size and possesses certain contextual dependencies. This dependency arises from the perceptually important features, for example, edges and textures as illustrated in [5].

The basic concept of the SDS algorithm relies on the fact that the parent–child pairs with large magnitudes are not vulnerable to attacks, whereas those with smaller magnitudes tend to be easily attacked. Therefore one can use the larger pairs to indicate robustness (content-changing manipulations) and use smaller pairs to reflect fragility (content-preserving manipulations). The construction of an SDS is summarized as follows. Given a pre-determined threshold d, select each parent–child pair <p, c> with

$$|\langle \mathbf{p}, \mathbf{c} \rangle| \geq \alpha \qquad (3)$$

The SDS array is recorded as

$$SDS[I,J] = \lambda \; A_{I,J} \qquad (4)$$

Where [i, j] is a child's coordinates of significant pairs in the parameterized wavelet domain, and λ is defined as

$$\lambda = \begin{cases} 1 : p>0, |p| > |c| \\ 2: p<0, |p| > |c| \\ 3: x>0, |p| < |c| \\ 4: x<0, |p| > |c| \end{cases} \qquad (5)$$

3.2 Procedure for Image authentication:

The digital signature and watermarking methods are used for image authentication. Digital signature encodes the signature in a file separate from the original image. Cryptographic algorithms have suggested several advantages over the traditional encryption algorithms such as high security, speed, reasonable computational overheads and computational power. A digital watermark and signature method for image authentication is using cryptography analysis.

The digital signature created for the original image and apply watermark. Images are resized before transmission in the network. After digital signature and water marking an image, apply the encryption and decryption process to an image for the authentication. The encryption is used to securely transmit data in open networks for the encryption of an image using public key and decrypt that image using private key.

Digital signature is a sort of Cryptography. Cryptography means keeping communications private. Its mainly used for the converting of the information is encryption and decryption. No one can't access the information without access key. The main process of the

digital signature is similarly as the handwritten signature and it's like paper signature and it having the digital certificate using this verifies the identity.

Watermarking is a sub-discipline of information hiding. It is the process of embedding information into a digital signal in a way that is difficult to remove. It's providing copyright protection for intellectual method that's in digital format.

The cryptography is providing better mechanisms for information security. In this analysis to provide the public and private keys for recovery the original information. The ability store and transfer sensitive information. By using the different encryption methods for generating public keys, decryption using for private keys. This method applied to digital signatures and water marking for to provide high security in transactions.

In the image authentication procedure shown in Fig. 4, given corrupted images by transmission and their associated digital signatures [6]. The proposed scheme authenticates both the integrity and the source of the received image by applying the following process on the image in the following order: (1) perform content-adaptive error concealment, if some blocks are damaged; (2) extract the SDS of the received image using the same method used in image signing; (3) decrypt the signature by using the sender's public key; (4) perform a content authenticity verification procedure using both the decrypted signature and the extracted one to calculate the degree of authenticity.

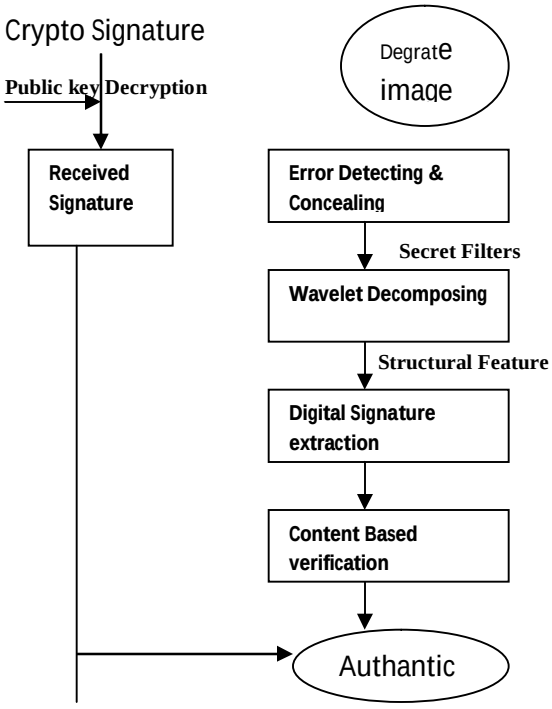


Figure 5: Diagram of image authentication procedure.

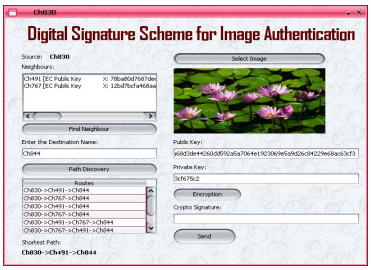
4 EXPERMENTAL EVALUATIONS:

In this paper we adopted some of the proposed scheme by testing its security, robustness against transmission errors, robustness against some acceptable manipulations and ability to distinguish tampered areas. All experiments were conducted with a number of classic benchmark images. The transmission error was replicated based on the Rayleigh model, which is commonly used for a wireless lossy channel. Using this model, the channel is characterized by the average bit error rate (BER). Mainly in our paper we discuss and compare the wavelet-based structural feature analysis. This experiment evaluation and comparisons with the adopted techniques are shown below.

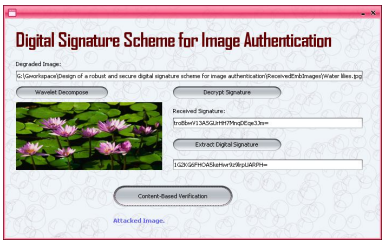
Experiment: (comparison with existing schemes):

In our experimental evaluation we compared with the proposed scheme, i.e. wavelet-based structural feature analysis with a state-of-the-art approach (DCT block-based analysis) introduced by Ye et al. [7] against forgery attacks.

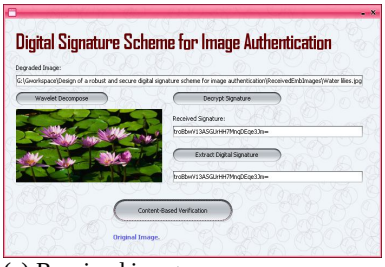
Some results are shown in Fig. 6 to demonstrate the unique anti-forgery of the structural information.



(a) Original



(b) Attacked image



(c) Received image

Figure 6: The examples of test results

5 CONCLUSIONS:

In this paper, we worked with a modified digital signature scheme for image authentication which is proposed. Content-dependent structural image features and wavelet filter parameterization are incorporated into the traditional crypto signature scheme to enhance the system robustness and security. Because the proposed scheme does not require any computational overhead, it is especially suited for wireless authentication systems and other real-time applications. The analysis and the experimental results confirm that the proposed scheme can achieve good robustness against transmission errors and some acceptable manipulation operations. The scheme is very robust to cutting and pasting counterfeiting attacks. It is also able to tolerate various common image processing manipulations, at the cost of only extra payload introduced into the channel by associating the signature with the image. Further work will conduct more tests on the quality of degraded images.

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] SEITZ J.: 'Digital watermarking for digital media' (Idea Group Publishing, 2005), Ch. 2.

[3] 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.

[4] FRIDRISH J., BALDOZA A.C., SIMARED R.J.: 'Robust digital watermarking based on key dependent basis functions'. Proc. Int. Conf. LNCS:IH, Portland, OR, USA, April 1998, vol. 1525, pp. 143–157.

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

[6] ANTHONY T., HO S., YONG L.G.: 'Image content authentication using pinned sine transform', EURASIP J. Appl. Signal Process., 2004, 14, pp. 2174–2184.

[7] 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.

[8] 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.

[9] PETER M., UHL M.: 'Watermark security via wavelet filter parametrization'. Proc. Int. Conf. ICASSP, USA, 2000.