Authentication of an Image over Wireless Channels Based on Secure Digital Signature Scheme

A. Swetha[1], P. Chenna Reddy[2]

[1]P.G student, J.N.T.U.A College of Engineering Pulivendula, India

[2]Professor, J.N.T.U.A College of Engineering Pulivendula, India

Abstract: ***Internet is a popular communicating channel. Because of the advance in networking and multimedia applications, multimedia contents can easily be attacked by the unauthorized persons. To confirm content integrity and to prevent duplication, image authentication techniques have been emerged. A secure digital signature scheme is one of the image authentication techniques that is suitable for an insecure environment, and is robust to transmission errors. This scheme exploits the scalability of a structural digital signature in order to achieve a tradeoff between security and image transfer for networked image applications. In order to make the digital signatures robust to image degradations multi-scale features are used, and to improve the security against forgery attacks key-dependent wavelet filters are employed. Further, this secure digital signature scheme is able to identify the tampered areas in the attacked image, and is very robust to cutting and pasting counterfeiting attacks. It can also tolerate different image processing manipulations at the cost of only extra payload introduced into the channel by associating the signature with the image. The main objective is to test the robustness against transmission errors, and some acceptable image processing manipulations, and to show the excellent ability in detecting the tampered areas, and removes the areas which do not belong to an object. . Experimental results show the robustness, and the validity of the proposed scheme.***

Keywords: Authentication, Secure digital signature, Digital signature, Content authenticity verification, Error concealment.

1. Introduction

A large number of networked multimedia applications have been created because of the advances in digital media technologies and networking. Those networked multimedia applications are often employed in a distributed wireless network environment that makes multimedia contents able to be attacked or harmed by the attackers. For insecure environments, it is possible for an attacker to interfere with images without permission during transmission. To guarantee honesty and reliability, image authentication techniques have been introduced to confirm content integrity nothing but the quality of being honest, and prevent forgery. These techniques are needed to be able to withstand difficult conditions against normal image processing and transmission errors, while being able to identify the one who are wishing to interfere without permission with the images. These authentication techniques have wide relevant to someone or something in journalism, commerce, law, and national defense.

Image content is stored as an extra file in compact representation and later can be used for authentication. Signature-based methods can work on both the quality of the image nothing but being honesty and repudiation prevention of the sender. Watermarking, on the other hand, is an invasive method nothing but which involves secret messages like that really embedding a message into an image data and the secret message can later be extracted to verify the authenticity of image content. Watermark-based method only work for protecting the quality of being honesty of the image. The major difference between a watermark and a digital signature is that the embedding process referring to the first of the two things mentioned requires the content of the media to change.

Normally, image data can allow for lossy representations which makes something breakdown. The information carried by image data continues to be retained even when the image has undergone reasonable levels of noise corruption or geometric distortion, filtering. Therefore bit-by-bit verification does not suits well for authenticating image data, therefore image authentication tool image authentication tool that validates the content is mostly desired. Content-based authentication, which passes images as authentic when the content does not change is an efficient approach. The work extending the digital signature scheme from fragile (data or hard) authentication nothing but even a difference of 1 bit is not allowed i.e., some acceptable manipulations such as lossy compression need to be tolerated may be traced back. For image authentication, it is desired that the verification method needs to be able to resist content-preserving modifications and needs to be sensitive to content-changing modifications.

Most previous attempts in content-based image authentication have focused on developing methods under the ideal assumption nothing but something must be true of reliable noise-free transport. However, these methods do not suit when used to transmit images over the error-prone wireless channel. For example, any transmission bit error will render traditional authentication a failure. In addition in the case of packet loss, synchronization may become a problem for conventional security techniques. Because of the need of retransmission and/or the bit overhead caused by forward-error-correction [2], this would imply a significant increase of latency. However, all the bits to be received correctly require that many image applications are needed to tolerate certain bit errors or data loss, are perceptually less important. It is clear that for the cases of lossy networks and the loss-tolerant nature of the multimedia data traditional authentication algorithms does not suits well.

Since the application of image authentication over wireless channels requires not only appropriate selection of the set of channel codes for effective forward-error-correction but also careful design of the authentication methodology, has deservedly attracted much attention. Recently, wide varieties of image authentication techniques have been emerged for authenticating the image data stream in the presence of random packet loss. However, their application may become critical in the case of mobile devices because their computational difficulty is often high, so that the signature scheme must be efficient enough to permit authentication without introducing delays. A choice has been made available to introduce an easy, yet valuable wireless image authentication scheme nothing but secure digital signature scheme that increases the state-of-the art schemes to increase security and robustness.

This paper's contribution is to develop a secure digital signature scheme, where as it tries to overcome the severe problems on the data transmission capability imposed by a wireless environment and the security. To get such results, the secure digital signature scheme generates only one fixed-length digital signature per image regardless of the packet loss and the size of the image during the transmission. In this secure digital signature scheme, for improving the security against the attackers key dependent parametric wavelet filters have been emerged, and for making the digital signatures robust against image degradations, multi-scale features are used. This paper's organization is done according to the following way:

Section 2 briefly discusses the secure digital signature scheme, and its algorithm. Section 3 describes about the error concealment procedure. Section 4 describes about the content authenticity verification and its attack location. Section 5 and 6 shows about the experimentation results and its conclusions respectively. Section 7 describes about the future scope.

2. Secure Digital Signature Scheme

In order to overcome the security problems and for achieving a good robustness against transmission errors, a secure digital signature scheme is proposed. The secure digital signature scheme is done by using the following algorithm: Assume two large prime number values as P, Q, such that their size should be approximately equal and their product n= PQ should be equal to the required bit length. Calculate the values o f n = pq and (φ) phi = (p-1)(q-1). Then choose an integer *e*, 1 < e < phi. Compute the secret exponent *d*, 1 < d < phi, such that ed ≡ 1 (mod phi). Analyze the public key value as (n, e) and the private key value as (n, d). Keep all the values d, p, q and phi secret. For encrypting [1], the image the sender should obtain the recipient B's public key (n, e) and represents the plaintext message as a positive integer *m*. Then compute the cipher text $c = m^e \bmod n$ and send the cipher text *c* to B. For decryption [1], of the image the receiver uses his private key (n, d) to compute $m = c^d \bmod n$ and then extracts the plain text from the message representative m.

Before sending an image to the destination, the sender performs digital signing, and sends the signature to the recipient. And the recipient performs signature verification to identify whether the received image is identical to the original image or not. The digital signature can be done by using the following algorithm; the sender creates a message digest of the information to be sent and represents this digest as an integer *m* between 0 and *n*-1 and uses her private key (n, d) to compute the signature $s = m^d \bmod n$, sends this signature *s* to the recipient, B. The signature verification can be done by using the following algorithm; the recipient uses sender A's public key (n, e) to compute integer $v = s^e \bmod n$ and extracts the message digest from this integer and independently computes the message digest of the information that has been signed. If both message digests are identical, the signature is valid. Otherwise the image is attacked and then the attacked areas are identified.

3. Error Concealment

In common wireless scenarios, the image is transmitted over the wireless channels block by block. Because of severe fading, entire image blocks can be lost. In the image authentication procedure, error concealment can be done by either using the contextual relationship of adjacent blocks or through embedded watermarking of information [3]. In this paper, an error concealment algorithm based on edge-directed filters is applied to achieve better visual quality. A summary of this algorithm is explained as follows: Firstly, the damaged or the attacked image blocks are identified by exploring the contextual information in images (e.g. edge continuity). The statistical characteristics of missing blocks are then estimated based on the types of their surrounding blocks.

4. Content Authenticity Verification

The basic idea of this content authenticity verification is to use patterns to distinguish distortions by transmission errors from those of attacks, firstly the patterns should be converted into rules, and then the degree of authenticity and the degree of un-authenticity should be calculated, and finally the authentication results will be obtained. The local distortion of an attacked image is often concentrated on some content of interest and the global distortion from transmission is more randomly distributed over the whole image. Furthermore, the attacked areas are more likely to be connected. From the above facts, given M, the difference map between the extracted SDS feature vector from the received image and the decrypted signature associated with the image, the degree of authenticity and un-authenticity is defined as

DY =min (R1, R2S)
DN = min (1 ɜ R1, R2L)

where R1 is the degree of global or local distortions, and R2S and R2L are the degrees of acceptable manipulation size or tampering operation size. R1 is computed by

R1= 1 /1+exp((aN/XY)-b) (1)

Where X and Y are the number of differences in the histogram of horizontal and vertical projections of M, respectively; N is the total number of differences in M; and a

and b are constants that are experimentally equal to 100 and 10, respectively, R2S and R2L are defined as

R2L =1 if m≥ L and Exp (-(m-L) 2/2δ2 (2)
R2S =1 if m≤ S and Exp (-(m-S) 2/2δ2 (3)

where m is the size of the maximum connected areas in M; L represents the large size and S denotes the small sizes, respectively; and these values are compared with the m value

*s*2 = (L S)2=8* ln 2.

The value of DY is compared with the value of DN, if the value of DY is greater than DN, the image is defined as authentic image, and otherwise the image is defined as an attacked image and the attacked areas are to be detected.

If the image is verified as unauthentic, the attacked locations may be detected using information combining the image features and the digital signatures. A summary of this technique is as follows: firstly, morphological operations are used to compute connected areas and remove the isolated blocks and little connected areas. Then the difference map (M) is masked by the union of the SDS and image features. The masking operation can refine the detected areas by concentrating these areas around the objects in the attacked image. Those areas in M which do not belong to an object are removed, which may be a wrong alarm of some noise or acceptable image manipulations. By using isolated detecting blocks, those wrong alarms of image manipulations can be reduced.

5. Simulation Results and Discussions

This section evaluates the proposed scheme by testing its security, robustness against transmission errors, robustness against some acceptable manipulations and ability to distinguish tampered areas.

Experiment 1 (achieving good robustness against security attacks): For this test, the digital signature is generated using a secret filter (e.g.*a*0 ¼ 1:5758, *a*1 ¼ 1:0558). By randomly assuming the transformation parameters within the key space, one tries to extract it. Figure1 indicates that the signature can only be retrieved correctly with matching filters, and when it extracts a signature, it achieves a good robustness against security attacks.

Experiment 2 (resistance to attacks): To test the robustness of the proposed scheme against several acceptable manipulations, experiments are conducted by mounting a variety of attacks, many from the well-known StirMark (www.cl.cam.ac.uk/ fapp2/watermarking/StirMark) software package, on 25 grayscale images including Girl, Bike, Barbara Peppers, Women and other natural images. Table 1 tabulates the average of the degree of authentication (DoA) defined as DY =DN for many different images across several different distortions. In all the cases, Degree of Authentication without non-malicious attacks is always higher than 79% and all distorted images are authentic. The proposed secure digital signature scheme shows excellent capability in detecting the tampered areas of the attacked images, even in the case of multiple tampered areas. It can be concluded that the proposed secure digital signature scheme is more practical and is more suitable for image authentication, because it has a good performance in identifying the attacked areas of the image from normal content-preserving image processing.

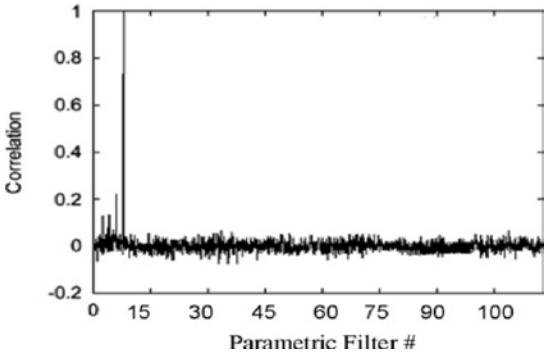

Figure 1: Correlation measure, the signature can only be retrieved with the correct filter

5.1 Experiment 3 (resistant to transmitting errors)

The authentication scheme can also obtain good robustness against transmission error, where the attacked or the damaged images first have error concealment. The error-concealed images are authentic. The results have revealed that the corrupted images with a BER below 3 ₃ 1023 can still pass the authentication after error concealment.

5.2 Experiment4 (comparison with existing schemes)

The fourth experiment compares the proposed scheme (wavelet-based structural feature analysis) with a state-of-the-art approach (DCT block-based analysis) against forgery attacks. Some results are shown in Fig.6.3 to demonstrate the unique anti-forgery of the structural information. The counterfeit images are created based on an 8 ₃ 8 block search and match and its SDS is extracted based on *d* ¼ 46.

Table 1: Average of DOA for many images across several attacks

Rotation (58)	93.3
Cropping (20%)	80.1
Scaling (20%)	95.7
Shifting (5%)	88.4
JPEG compression (QF ¼ 10%)	85.9
4 ₃ 4 median filtering	87.3
Noise addition (Gaussian 20)	85.8
Brightness adjustment	92.2
Deletion up to five lines	79.6
Histogram equalization	95.2

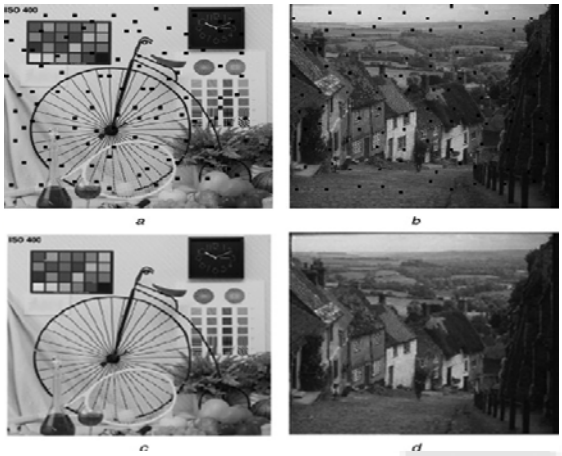

Figure 2: Robustness against transmission errors

Figure 3: (Left) visual similarity of Lena image under structural information forgery attacks; (right) their visual similarity under block-based counterfeit attack

6. Conclusion

In this paper, a modified digital signature scheme for image authentication has been 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, secure digital signature scheme is especially suited for wireless authentication systems and other real-time applications because this scheme does not require any computational overhead. The secure digital signature scheme can achieve good robustness against transmission errors and some acceptable manipulation operations. Further, this secure digital signature scheme is able to identify the tampered areas in the attacked image, and is very robust to cutting and pasting counterfeiting attacks. It can also tolerate different image processing manipulations at the cost of only extra payload introduced into the channel by associating the signature with the image. The main objective is to test the robustness against transmission errors, its resistance towards the attacks, and some acceptable image processing manipulations, and to show the excellent ability in detecting the tampered areas, and removes the areas which do not belong to an object. Experimental results show the robustness, and the validity of the proposed scheme.

7. Future Scope

Since the proposed scheme tests the robustness against transmission errors, its resistivity towards the attacks, and some acceptable image processing manipulations, further work will include more tests on the quality of degraded images to achieve a good authentication.

References

[1] CHUN-SHIEN LU,” On the security of structural information embedding or extraction for images”, Process in the 2004 International Symposium on Circuits and Systems, 2004. ISCAS’04, volume 2, pp. 169-172, 23-26 May 2004.

[2] XINGGANG LIN, YE S, SUN Q,” Content based error detection and concealment for image transmission over wireless channel”, Process in the 2003 International Symposium on Circuits and Systems, 2003. ISCAS’03, volume 2, pp. 368-371, 25-28 May 2003.

[3] CHING-YUNG LIN, QIBIN SUN, SHUIMING YE, SHIH-FU CHANG,” A crypto signature scheme for image authentication over wireless channel”, 2004 Institute of Electrical and Electronics Engineers International Conference on Multimedia system and Expo, 2004. ICME’2004, volume 3, pp 1931-1934, 27-30 June 2004.

[4] ZCHICHENG ZHOU, SUN Q, DAJUN HE, SHUIMING YE,” Feature selection for semi fragile signature based authentication systems”, Process ITRE International Conference in Information Technology: Research and Education, 2003, pp.99-103, 11-13 August 2003.

[5] RODRIGUES M. R. D, BARROS D, ”Secrecy capacity of wireless channels”, Institute of Electrical and Electronics Engineers International Symposium in Information Theory 2006, pp. 356-360, 9-14 July 2006.

[6] Lt ARNOLD C. BALDOZA , RICHARD J. SIMARD, JIRI FRIDRICH,” Robust digital watermarking based on key dependent basis functions”, Int. Conf. LINCS: IH, USA , OR, Portland proceedings, volume 1525, pp.143-157, April 1998.

[7] CHUN-SHIEN LU, LIAO, H-Y.M,”Structural digital signature for image authentication: an incidental distortion resistant scheme”, Institute of Electrical and Electronics Engineers Transactions in Multimedia system, volume 5 (2), pp.161-173, June 2003.

[8] SHIH-FU CHANG, KURATO MAENO, QIBIN SUN, MASAYUKI SUTO,” New Semi-Fragile Image Authentication Watermarking Techniques Using Random Bias and Nonuniform Quantization”, Institute of Electrical and Electronics Engineers Transactions in Multimedia system, volume 8 (1), pp. 32-45, February 2006.

[9] QIBIN SUN, SHIH-FU CHANG,” A Secure and Robust Digital Signature Scheme for JPEG2000 Image Authentication”, Institute of Electrical and Electronics Engineers Transactions in Multimedia system, volume 7(3), pp. 480-494, June 2005.

[10] SHIH-FU CHANG, ANTHONY T. S. HO, YONG LIANG GUAN,” Image content authentication using pinned sine transform”, European Association for Signal

Processing Journal on Applied Signaling Process, volume 14, pp.2174-2184, I January 2004.

Author Profile

A. Swetha received the bachelor's degree in Computer Science and Engineering in 2011 from JNTU Anantapur. She is currently pursuing the master's degree in CSE in the college of JNTUACEP.

Dr. P. Chenna Reddy M.Tech., PhD., he is working as a Professor in JNTU College of Engineering, Pulivendula, India. He published so many national and international papers. His research interests include computer networks.