A Tamper Proof Noise Resilient End to End Image based Authentication System over Wireless Transmission with AWGN Channel using Wavelet based Templates and AES

Fouzia Sultana† **Stephen Charles††** **A.Govardhan†††**

Prof.SSIET KURNOOL Principal SSIET KURNOOL Director Evaluation JNTU HYD

Summary
Introduction of 3G wireless communication systems, ogether with the invasive distribution of digital images and the growing concern on their originality triggers an emergent need of authenticating images received by unreliable channels, such as public Internet and wireless networks. To meet this need, a content-based image authentication scheme that is suitable for an insecure network and robust to transmission errors is proposed. The proposed scheme exploits the scalability of a structural digital signature in order to achieve a good tradeoff between security and image transfer for networked image applications. In this scheme, multi-scale features extracted from wavelet transform 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. Features are irrevocable i.e; Image cannot be reconstructed from the given features. We also use AES based encryption of the image data. The scheme is tested with baseband modulation, AWGN (Additive White Gaussian Noise) noise and random tampering. No explicit error correction code is implemented. We use weighted sum decoder, this scheme is also able to distinguish tampering areas in the attacked image. Experimental results show the robustness and validity of the proposed scheme

Key words:
Image authentication, watermarking, content-based, digital signature, structural signature design.

1. Introduction

Recent advances in networking and digital media technologies have created a large number of networked multimedia applications. Those 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. 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. Such authentication techniques have wide applicability in law, commerce, journalism and national defence.

In the literatures, methods of image content authentication can be categorized into either digital signature based or watermarking based. A digital 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, really embeds a message into an image data and the hidden message is later extracted to verify the authenticity of imagecontent.Watermark-based approaches work only for protecting the integrity of the image. The major difference between a watermark and a digital signature is that embedding process of the former requires the content of the media to change.

Normally, image data can allow for lossy representations with refined degradation. The information carried by image data is mostly retained even when the image has undergone reasonable levels of filtering, geometric distortion or noise corruption. Therefore bit-by-bit verification is no longer a suitable way to authenticate image data, and an image authentication tool that validates the content is more desired. Content-based authentication is an efficient approach, which passes images as authentic when the content does not change. The work extending the digital signature scheme from data (fragile or hard) authentication (i.e. even a difference of 1 bit is not allowed) to content (semi-fragile or soft) authentication (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 must be able to resist content-preserving modifications while being sensitive to content-changing modifications.

The application of image authentication over wireless channels has attracted much attention since it requires not only careful design of the authentication methodology, but also appropriate selection of the set of channel codes for effective forward-error-correction. Recently, a number of good solutions have been proposed for authenticating the image data stream in the presence of random packet loss. However, their computational difficulty is often high, so

Manuscript received May 5, 2013
Manuscript revised May 20, 2013

that their application may become critical in case of mobile devices, where the signature scheme is efficient enough to permit authentication on the fly without introducing delays. A choice has been made to develop a simple, yet valuable wireless image authentication scheme that enhances the state-of-the-art schemes to improve robustness and security.

2. Problem Statement

There are several image authentication schemes which claim to produce good authentication rate over wireless media. These techniques use mainly convolution or other error correction codes to recover from the channel noises. But sending the image data itself over the channel or sending encrypted image data consumes lot of bandwidth which reduces the effectiveness of such techniques.

Hence in this work we propose a technique for secured transmission over wireless channel using image features extracted depending upon wavelet transform and protect the same with AES encryption technique.We show that the technique can produce good authentication rate even when channel error and tampering attempts are mores.

3. Related Work

Recent advances in networking and digital media technologies have created a large number of networked multimedia applications. Those 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.

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 [1]. Such authentication techniques have wide applicability in law, commerce, journalism and national defence.

In the literatures, methods of image content authentication can be categorised into either digital signature based or watermarking based. A digital signature (or crypto-hash) is a set of extracted features, which captures the essence of image content in compact representation [1]. 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 invasive method that really embeds a message into an image data and the hidden message is later extracted to verify the authenticity of image content [2]. Watermark-based approaches only work for protecting the integrity of the image.

Normally, image data allows lossy representations with refined degradation, but information carried by image data is same even though the image has undergone filtering, geometric distortion or noise corruption. Hence bit-by-bit verification is not suitable way to authenticate image data and an image authentication tool that validates the content is more desired [1, 3].

Content-based authentication is an efficient approach, which passes images as authentic when the content does not change. The work extending the digital (i.e. even a difference of 1 bit is not allowed) to content (semi-fragile or soft) authentication (i.e. some acceptable manipulations such as lossy compression need to be tolerated) may be traced back [3]. For image authentication, it is desired that the verification method be able to resist content preserving modifications while being sensitive to content changing modifications.

Most previous efforts in content-based image authentication have concentrated on developing methods under the ideal assumption of reliable noise-free transport [4–7]. However, 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.

In addition, synchronization may become a problem for conventional security techniques in the case of packet loss. This would imply a significant increase of latency because of the need of retransmission and/or the bit overhead caused by forward-error-correction [8]. However, requiring all bits to be received correctly overlooks the fact that many image applications can tolerate certain bit errors or data loss that are perceptually less important. It is clear that traditional authentication algorithms do not cope well with lossy networks and loss-tolerant nature of the multimedia data.

The application of image authentication over wireless channels has deservedly attracted much attention since it requires not only careful design of the authentication methodology, but also appropriate selection of the set of channel codes for effective forward-error-correction. Recently, a number of good solutions have been proposed for authenticating the image data stream in the presence of random packet loss [9–12].

However, their computational difficulty is often high, so that their application may become critical in the case of mobile devices, where the signature scheme should be efficient enough to permit authentication without any delays.

The contribution of this paper is to develop a signature based image authentication scheme, which tries to overcome the severe constraints on security and the data transmission capability imposed by a wireless environment

using state-of-the-art techniques improving robustness and security.

To obtain such results, the proposed scheme generates only one fixed-length digital signature per image regardless of the image size and the packet loss during transmission. The robustness of the generated scheme is achieved by employing the concept of structural features, whereas security is achieved by adopting a filter parameterisation technique.

The major differences that differentiate the proposed scheme from existing state-of-the-art approaches [10, 11] are: (1) it works at a semi-fragile level, which means that some manipulations on the image will be considered acceptable; (2) more robustness – it can tolerate a range of attacks while accurately locating the tampered area which is achieved by exploiting the concept of structural digital signature (SDS); (3) the integration of the SDS and key dependent parametric wavelet filters makes the scheme more efficient to security attacks; (4) the computation complexity is reduced because of the framework of a lifting-based wavelet transform; and (5) the ability to support efficient and accurate tamper localization in spite of information loss in large areas or high variant areas.

4. Methodology

First a user is registered with the system. Registration process generates a unique 16 byte Key for the user. The Key is saved in a database. At the time of registration user ID is checked. If the id does not exist than only user is registered.

2. Once several users are registered, user U selects a transmission process. For transmission user selects an image from the set of images available in the database.

3. Wavelet features from the images are extracted. Wavelet features are nothing but mean and standard deviation of the decomposition images, decomposed using Haar_wavelet transform.

4. Features of 16 values are now encrypted with Rinjdeal, which is a symmetric Encryption technique. For encrypting the data user's key is used.

5. Encrypted Image features are converted into binary value and are transmitted.

6. For transmission, baseband modulation is used. A Baseband modulation is a technique where the actual binary sequence is transmitted without multiplying with any carrier.

7. We use bi-polar coding to convert {0, 1} data to {-1, 1} data. We use a chunk of 10. i.e; for every input bit 10 bits are generated and transmitted. Hence for a feature value '5' the transmitted sequence is:

5-> Binary-> 101-> Bipolar->1-11->Modulation->11111111 -1-1-1-1-1-1-1-1-1-1 1111111111

8. White Gaussian noise is added with this signal with specific SNR. The resultant signal amplitude becomes fluctuating. For example one of the set of above data for SNR=50 produces following result

.9 .1 .833 .97 1.1 .339 1.3 .9 .9.....-.2 .9 0.....

9. At the receiver side weighted demodulator is used. i.e; all the 10 bits representing a single bit of the encrypted signal are added. If the sum is greater than 0, it is considered to be 1 else 0.

10. Further as per user's choice some of the bits are changed. This is the tampering process done by changing the bits, actual encrypted data is changed.

11. Receiver does not know which image's features have come, which user has sent it, whether the data is noise affected or not. Hence receiver selects all the images from directory and extract features. Say {f1, f2...ft} where t is the number of images.

It now decrypts the message with all the keys available with the database. Say {d1, d2...dn} where n is the number of users.

Now distance of R11= {d1, f1}, R12= {d1, f2} ...Rn, t is calculated as the Manhattan distance between the decrypted message and the image features.

R1=sum (R11, R12...R1t);

R2=sum (R21, R22...R2t);

A=smallest (R1, R2...Rn) is the person who is authenticated.

Assuming the fact that sender knows the user trying to authenticate, we compare both A and U, if they are same, we say the authentication is correct else it is considered to have failed.

5. Proposd System

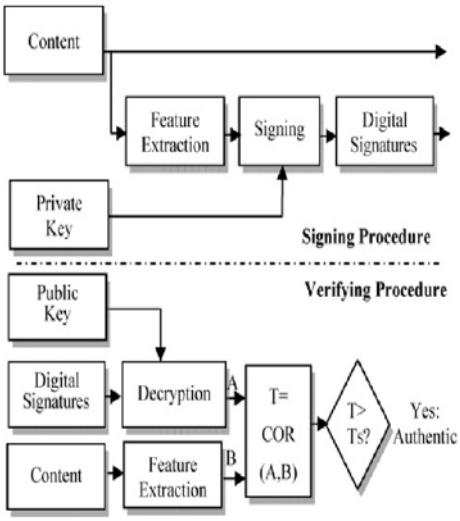


Fig. 1.Diagram of a semi-fragile signature used for image authentication.

Fig. 1 shows the brief diagram of a semi-fragile signature used for image authentication. There are two main problems in this diagram. One is that the size of the generated signature is proportional to the size of the content and it makes the signing very time consuming; on the other hand it is the basis of authentication that the correlation between features sets and not bit-bit comparison that could cause some security problems.

To tackle these problems while not sacrificing accuracy and increasing the complexity, a content-dependent key (hash) has been proposed. A hash function takes a message of an **a**rbitrary 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. 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.

A key problem in the construction of secure hash values is the selection of image features that are resistant to common transformations. When the features that 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.

Some of the features that have been proposed in the literature include block-based histograms, image-edge information and the wavelet transforms. However, since these features are publicly known, using such features alone makes the scheme susceptible to forgery attacks, even when the final hash is obtained by encrypting these features. Therefore the security mechanism should be combined into the feature extraction stage. Previous works mainly focus on the robustness study of features. The 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.

5.1 Wireless Image Authentication Scheme

As discussed in Section 1, authenticating an image over lossy wireless channels has its limits and drawbacks. Traditionally, security is viewed as an independent feature with little or no relation to the remaining data communication tasks and, thus, state-of-the-art authentication algorithms are insensitive to the physical nature of the wireless medium. In this section, a modified wireless image authentication scheme has been proposed. This scheme based on robust digital signatures generated from a secret wavelet transform of the reconstructed degraded images via an error concealment technique.

5.2 Image Signing Procedure

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 based by the image sender.

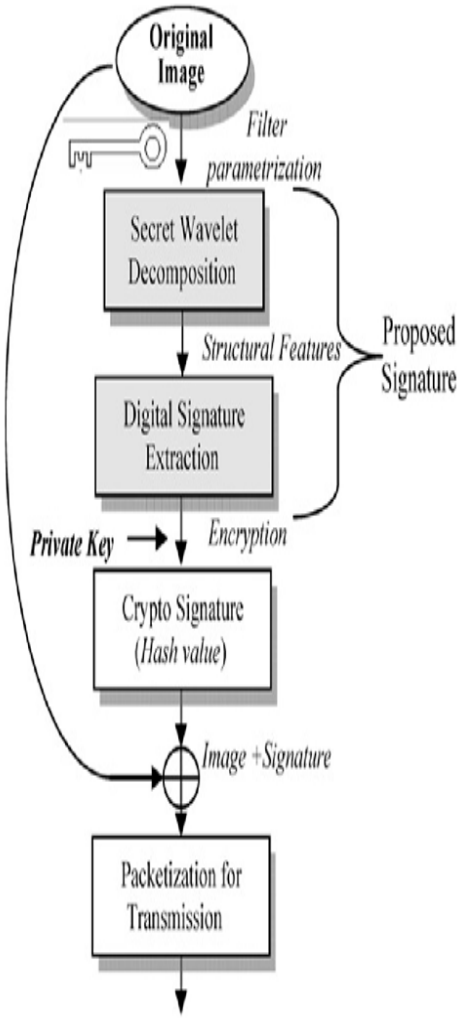


Fig.2 Diagram of image signing procedure

(4) send the image and its associated crypto signature to the recipient. In consideration of robustness, no compression and coding are used, since they will cause

error propagation.

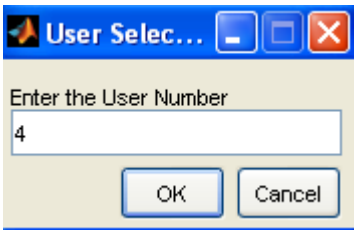
5.3 Wavelet Parameterization

The generated image's signature is constructed in the wavelet domain. Wavelet transform is characterized by excellent energy compaction and de-correlation properties; hence, it is employed to effectively generate a compact representation that exploits the structure of the image. Wavelets are also tolerant with respect to colour intensity shifts, and can capture both texture and shape information effectively. Further, wavelet transforms can generally be computed in linear time, thus allowing for fast algorithms.

6. Result Snapshot and Graphs

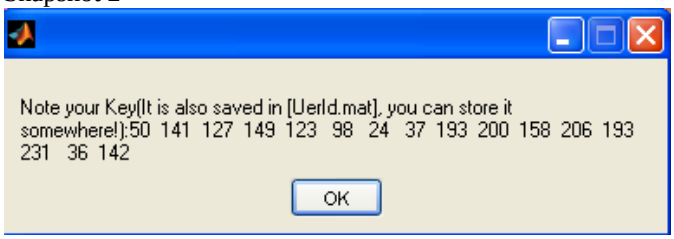
I. Registration Phase

Snapshot 1



User gets registered.

Snapshot 2

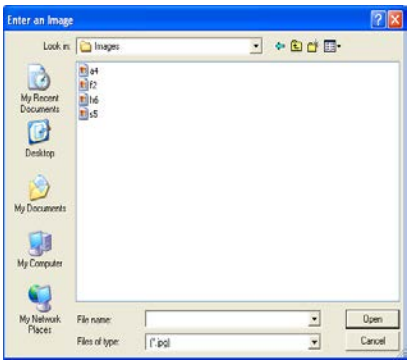


Simultaneously, a 16 bit key is also generated for the user

II. Transmission Phase

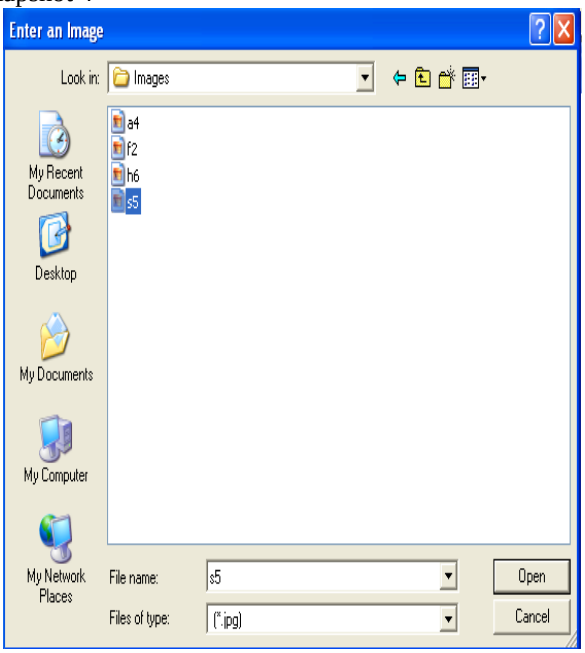
To transmit an image, the user has to select and load the key file. Asks user to enter an image from the image database.

Snapshot 3



User will select any image from the database

Snapshot 4



User selects s5 image

Snapshot 5

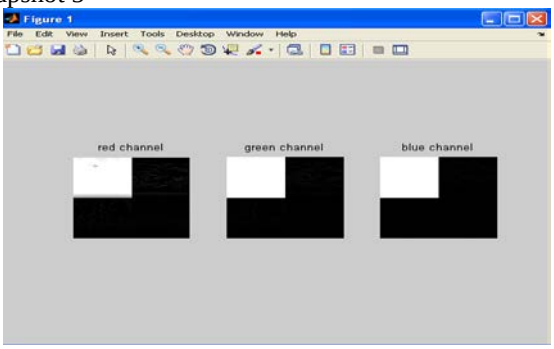
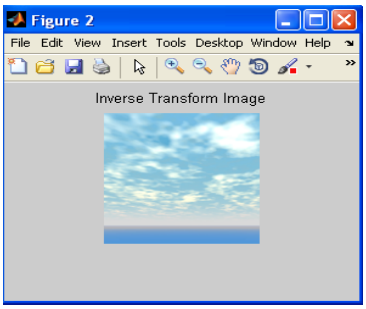


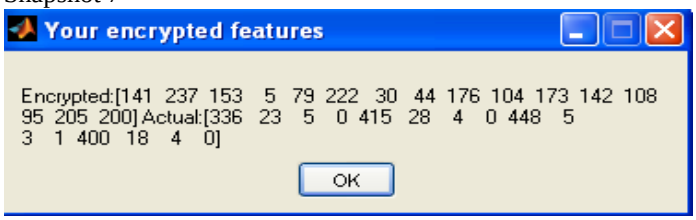
Image is differentiated for red blue green channels

Snapshot 6



Inverse transform image of the selected image is formed using wavelet transforms

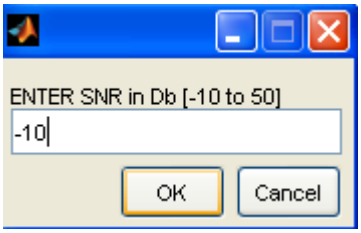
Snapshot 7



Features from the image are encrypted.

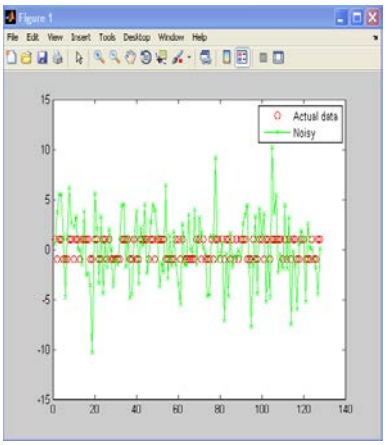
III. Channelization

Snapshot 8



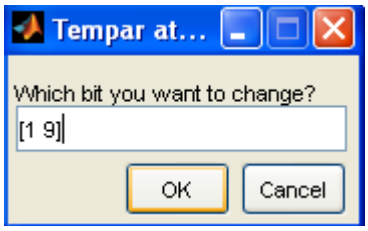
Adding noise during transmission over the channel

Snapshot 9



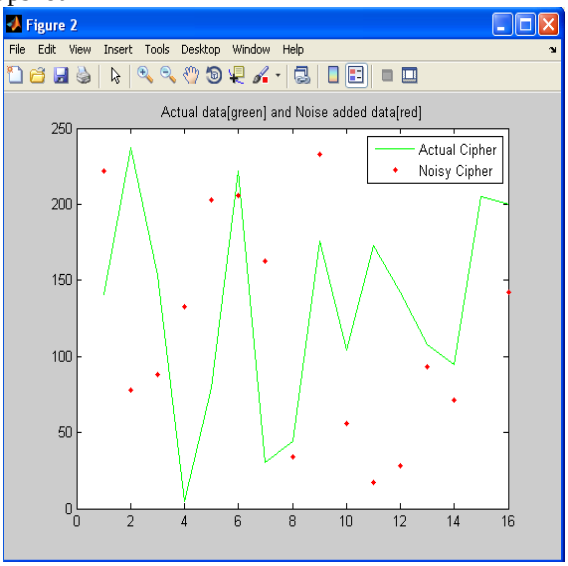
Graph showing actual data and noise.

Snapshot 10



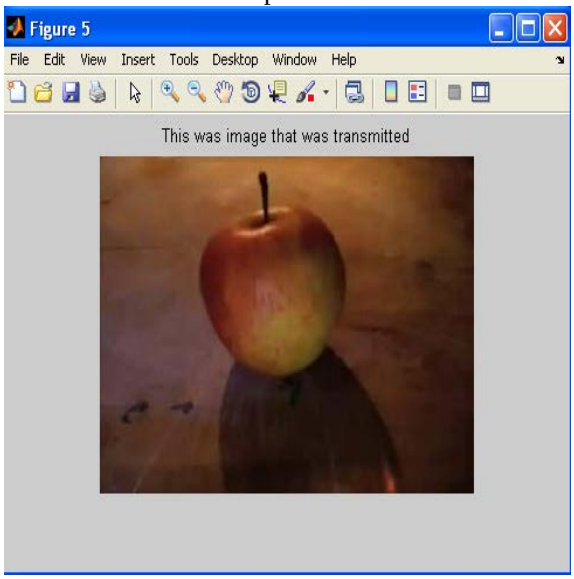
Selecting the bits to be tampered

Snapshot 11



IV. Testing Phase at Receiver End

Snapshot12



Same image has been transmitted that was selected for Transmission

Result shows that the same image has been transmitted that was selected for transmission.

Result graph

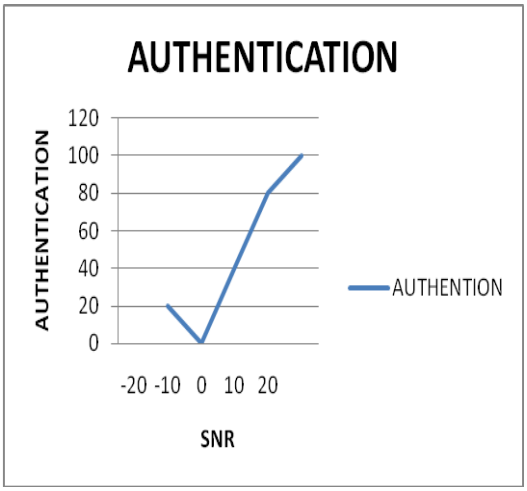


Fig.3 Graph for rate of Authentication

The graph of fig 3. shows that the rate of authentication improves with improving channel quality. However even for 10 dB, authentication rate is quite high.

Conclusion

In this work, a modified digital signature scheme for image authentication has been proposed. Content-dependent structural image features and wavelet filter parameterisation 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 can be done to conduct more tests on the quality of degraded images.

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.: 'content based digital signature for image authentication'. Proc. IEEE Int. Conf. Image Processing (ICIP'96), 1996, pp. 227–230.

[4] Anthony T., Ho S., Yong L.G.: 'Image content authentication using pinned sine transform', EURASIP.Journal of Appl. Signal Process. 2004, 14, pp. 2174–2184.

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

[6] 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.

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

[8] Ye S., Lin X., Sun Q.: 'Content-based error detection and concealment for image transmission over wireless channel'. Proc. IEEE Int. Symp. Circuits and Systems, Thailand, 2003.

[9] Ginseu G., Giusto D.D., Onali T.: 'Mutual image based authentication framework with JPEG2000 in wireless environment', EURASIP Journal of Wireless Communication Networks., 2006, pp. 1–14 (Article ID 73685).

[10] Lin C.Y., Sow D., and Chang S.F.: 'Using self authentication and recovery images for error concealment in wireless environment'. Proc. SPIE ITCom Conf., August 2001.

[11] 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.

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

[13] Kunder D., Hatzinakos D.: 'Digital watermarking using multiresolution wavelet decomposition'. Proc. IEEE Int. Conf. Acoustics, Speech and Signal Processing, Seattle, Washington, 1998.

[14] Peter M., Uhl M.: 'Watermark security via wavelet filter parametrization'. Proceedings International Conference ICASSP, USA, 2000.

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

[16] Fridish J., Baldoza A.C., and 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.

[17] Lu C.S., Liao H.M.: 'Structural digital signature for image authentication: an incidental distortion resistant scheme', IEEE Trans. on Multimedia. 2003, 5, (2), pp. 161–173.
[18] 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.
[19] MARTINIAN E., WORNELL G.W., CHEN B.: 'Authentication with distortion criteria', IEEE Trans. Inf. Theory, 2005, 3, pp. 1–22.
[20] Barros J., Rodrigues M.R.D.: 'Secrecy capacity of wireless channel'. Proc. IEEE Int. Symp. Information Theory, Seattle, USA, 2006 .

Authors Biography

Fouzia Sultana is a research scholar in Computer Science and Engineering faculty, pursuing PhD. from JNTU, Hyderabad in area of Network Security. She has completed her B.E in Computer Science and Engineering in the year 1989 from PDA College of Engineering, Gulbarga and M.E in Computer Science and Engineering in 1999 from KBN College of Engineering, Gulbarga affiliated to Gulbarga University, Gulbarga. She started the career as a lecturer at KBN College of Engg. in 1990 later then served same Institute as Asst. Professor and Head of the CSE Dept from 1999-2008.Worked as a Professor at Aurora's Engg. Colleges, Bhongir Hyderabad from 2008-2010.Her area of interests are Networking Network and Web Security.She was earlier a member College Academic committee at AEC. Bhongir and a Life member of **ISTE.**

Dr. Stephen Charles received ME degree from Bharathiar University, Coimbatore and PhD from Jawaharlal Nehru Technological University Hyderabad. He is working as a Principal in Stanley Stephen College of Engineering, Kurnool. He has 23 years of experience in teaching His research interests are digital signal processing, Network Security Information Security and Wireless networks.
He published 18 International journal Papers and 2 National Journal papers, 35 International conference papers. He has guided 3 candidates for their Ph.D.

Dr. A Govardhan did his Intermediate from APRJC Nagarjuna Sagar, during 1986-1988, BE in Computer Science and Engineering from Osmania University College of Engineering, Hyderabad in 1992, M.Tech from Jawaharlal Nehru University(JNU), Delhi in 1994 and he earned his Ph.D from Jawaharlal Nehru Technological University, Hyderabad in 2003.He is the Director Evaluation JNTU Hyderabad. He guided 10 Ph.D theses, 1 M.Phil and 123 M.Tech projects. He has 152 Research Publications in International/National Journals and Conferences. Dr. Govardhan is a Member in Executive Council, JNTUH; He is a member of Standing Committee for Academic Senate, JNT University Hyderabad and Academic Advisory Committee (AAC), UGC-Academic Staff College and Sports Council, JNT University Hyderabad. He is a Member on the Editorial Boards for Seven International Journals. He had attended an International Conference in Stockholm, Sweden. He is also a member in various Professional and Service-oriented bodies. He had received the best teacher award from Andhra Pradesh Govt. in the year 2011-12. This year he has been a selected for a prestigious "Dr Sarvepally Radhakrishna" NATIONAL Award