International Journal of Applied Engineering Research ISSN 0973-4562 Volume 12, Number 11 (2017) pp. 2675-2679

Design of a Secure Digital Signature for Image Authentication over Wireless Networks

Dr. Chinthagunta Mukundha

Associate Professor, Department of IT, Sreenidhi Institute of Science and Technology
Ghatakesar, Hyderabad, Telangana-501301, India.
ORCID: 0000-0003-2182-9558

Dr. I. Surya Prabha
Professor, Department of IT, Institute of Aeronautical Engineering,
Dundigal, Hyderabad, Telangana-500043, India.

Dr. M. Nagalakshmi
Associate Professor, Department of CSE, MLR Institute of Technology,
Dundigal, Hyderabad-500043, India.

Abstract
With the Launch of 4G wireless communication systems, combined with the invasive distribution of Digital images and the spreading concern on their individuality triggers an emergent need of authenticating Images received by untrusted channels, such as public Internet and wireless networks. To achieve this need, a content-based image authentication scheme that is exactly opt for an robust to Transmission errors are proposed and insecure network. The proposed scheme exhibits the changing of a structural digital signature in order to meet a good tradeoff between security and image transfer for networked image applications. In the proposed technique, multi-scale features are recycled to make digital signatures robust to image deterioration and key-dependent parametric wavelet filters are occupied to enhance the security across forgery attacks. This technique is also able to differentiate tampering areas in the attacked image. Preliminary reports show the robustness and validity of the proposed scheme.

Keywords: Digital Images, Security, Attack, Wireless Networks, Digital Signature

INTRODUCTION

Normally, image data can allow for loss representations with purify degradation. The information carried by image data is maximum accepted even when the image has gone through some measurable number of filtering, geometric distortion or noise corruption. So verifying bit-by-bit image data validation is no longer a suitable way to validate image data and an image authentication techniques that approves the content is more desired [1, 2]. Content-based authentication is an efficient approach, which refine images as authentic when the image data not change. The work extending the digital signature scheme from information (hard or fragile) authentication (i.e. even a difference of 1 bit is not allowed) to content (soft or semi-fragile) authentication (i.e. some acceptable additions such as loss compression need to be tolerated) may be traced back to.

Current developments in the area of networking and digital media technologies have given birth to a large number of multimedia applications that relate to networking. Those applications are often launch in a distributed network paradigm that makes multimedia data vulnerable to privacy and malicious attacks. For untrusted environments, it is possible for an attacker to tamper with images during transmission. To guarantee image authentication, trustworthiness techniques have emerged to confirm content integrity and prevent imposition. This type of approaches are required to be robust against normal transmission of image data and processing errors, while being able to detect malevolent change on the image [1]. This type of authentication techniques has more applications in the areas of commerce, journalism, law and national defense.

In the early discussions made on techniques of image content authentication can be grouped into either watermarking based or digital signature based. A digital signature is a set of extracted features, which captures the essence of image content in compact mode [1]. It is preserved as an extra file and later used for validation purpose. Signature- based methods can work on both the repudiation prevention of the sender and integrity protection of the image.

Watermarking is another tool to provide an invasive performance that really embeds a message into an image data and the buried message is after extracted to verify the authenticity of image content [3]. Watermark-based approaches only work for preserving the integrity of the image data. The major difference between a watermark and a digital signature is that the combining process of the former needs the information of the media to modify.

For image authentication, it is desired that the validation method be able to prohibit content preserving modifications while being sensitive to content modifications. The introduction of 4G wireless communication systems, together with the invasive distribution of digital images and the spreading concern on their actual data triggers an emergent need of authenticating images received by unreliable channels, such as wireless networks and public Internet. To

meet this need, a content-based image authentication method that is suitable for an insecure transmissions and robust to transmission errors is proposed. The proposed method accomplishes the scalability of a structural digital signature in order to achieve a good tradeoff between image transfer and security for networked image applications.

LITERATURE SURVEY

There are two categories of image content authentications methods first is digital signature based or watermarking based. A digital signature (or crypto-hash) is a group of extracted functions, which acquires the essence of image content in compact representation. It is preserved as an extra file and later used for authentication. Signature based methods can work on both the repudiation prevention of the sender and integrity protection of the image. Second method is watermarking, is an invasive technique that really inserts a message into an image data and the hidden message is after extracted to validate the authenticity of image data. Watermark-based approaches only work for protecting the integrity of the image. The main contrast between a digital signature and watermark is that the inserting process of the former requires the data of the image to change.

To authenticate image content, it is required that the verification method be able to resist content preserving modifications while being sensitive to data changing modifications. Most of the previous content-based image authentication have developing methods under the ideal assumption of reliable noise-free transport like extraction of structural data authentication signature and the digital signature [4] is based on the invariance of the link between discrete cosine transform coefficients [5] at the same position in different blocks of an image. However, these techniques do not suitable to work l when used to transfer images over the noise wireless channel. For example, any transmission bit error will say that conventional authentication a failure. In addition to that, synchronization may lead to a problem for traditional security methods in the case of packet drop. This would involve a compelling increase of latency because of the need of retransmission and/or the bit overhead is occurred by forward-error-correction. However, requiring all bits to be received correctly overlooks the case that many image applications can abide certain data loss or bit errors that are perceptually less important. It is very clear that conventional authentication procedures do not cope well with loss networks and the loss-tolerant nature of the multimedia data.

Over wireless channels the applications of image authentication have appropriately attracted much attention since it requires not only attentive design of the authentication technique, but also appropriate selection of the set of channel codes for efficient forward-error-correction. Recently, a number of good solutions have been proposed for authenticating the image content stream in the existence of random packet loss.

For example:

a. **A novel mutual image-based authentication framework [6]**: In this frame work implemented a challenge-response scheme depending on image scrambling and visual password. The application window is broken into *k* grids, each one makes of *h number of cells*. At the time of the pass image/s selection process the user has perfectly identify the *k* pass image/s among *N* images, randomly cull the cells from the JPEG2000 database. At the same, in the choice selection process single secret detail must be identified for each pass image with the repetitive zooming process. The shown password codes are transferred one by one, reducing the risk of sniffing. Whenever the server identifies an authentication failure, the validation success until the last step. Only then, the user is rejected and a notification policy is adopted.

b. Self-Authentication-and-Recovery Images (SARI) [7] : system for the purpose of error detection and concealment in datagram-oriented image/video transmission. A SARI image embeds two kinds of information watermarks: authentication bits and reconstruction bits. The content-based watermark bits produced from a block set, which includes two blocks for acquiring authentication bits and four blocks for producing recovery bits, are embedded into other blocks in the image. The place of damaged blocks are identified by the inserted authentication information, while the drop blocks in a SARI image are nearly recovered depending on the recovery information.

c. Massage authentication code [8]: A robust digital signature of image can be generated as follows. First, the image is divided and converted into 8x8 blocks. Those blocks are named as either T block or E block. We select T blocks for cull MACs and E blocks for watermarking. The identification and relations of T and E blocks can be specified by random seeds that are embedded in the digital signature. For each T block, we take up its DC and 3 AC to generate MACs. These 4 coefficients are computed by preset authentication strength matrix Q,. These 4 hits are then watermarked into its corresponding E blocks. We insert the watermark of T block by directly changing some AC coefficients in E. A typical ratio of T and E blocks is 1: 8. In 8 E blocks of a T block, we only insert the watermark into those 3 blocks with highest AC energy. A one-way crypt hash function such as MD5 or SHA-1 is applied to the MACs added from all T blocks. In concatenation of these hash values, other auxiliary data embeds the size of image, and the authentication strength matrix *(Q,)* is mixed together and is encrypted using the sender's private key to get the crypto signature.

Anyway, All the above techniques are having high computational problems, so that their application may become complex in the case of small devices like mobile devices, where the signature scheme must be efficient enough to permit validation on the fly without introducing delays. A choice has been made to implement a simple, yet valuable wireless image authentication scheme that improves the state-of-the art schemes to improve robustness and security.

SECURE DIGITAL SIGNATURE SCHEME

The main variations that differentiate the proposed method from existing state-of-the-art [7,8] approaches are:

(1) It works at a semi-fragile level; it means that some modifications on the image will be considered acceptable;

(2) More robustness – it can accept a range of attacks while exactly placing the tampered area ; it is reached by exploiting the concept of structural digital signature (SDS);
(3) The mixture of the key dependent parametric wavelet filters and SDS makes the method more proficient to security attacks;
(4) The capability to support accurate and efficient tamper localization in spite of data loss in big areas or high variant areas.

The major problem is to implement a signature based image validation scheme, which tries to swamp the several constraints on security and the data transmission capability imposed by a wireless networks. The robustness of the generated method is reached by governing the concept of structural features, whereas security is accomplished by adopting a filter parameterization technique.

Image signing procedure
In the image signing procedure as depicted in Figure.1given the image to be sent over the wireless channels. The system produces a digital signature by doing a signing process on the image in the following order:

1. Break down the image using secrete parameterized wavelet filters;
2. Excerpt the SDS;
3. Cryptographically produce the crypto signature by the image senders private key.
4. Send the image and its correlated crypto signature to the recipient. In the view of no compression, robustness and coding is used, since they will cause error propagation.

Break down the image using secrete parameterized wavelet filter:
The produced images signature is constructed in the wavelet domain. Wavelet conversion is characterized by good energy compaction and de-correlation properties; hence, it is organized to effectively generate a compact representation that exploits the structure of the image [9, 10]. Wavelets are also receptive with respect to colour intensity shifts, and can get both texture and shape data effectively. Further, wavelet transforms can normally be computed in linear time, thus allowing for speed algorithms. Most traditional wavelet-based image authentication schemes reported in the literature have three shortcomings [6-8]:
1. Security of the image signatures is point out without protecting the coefficients used to construct the signature from malicious attacks.
2. Depressed robustness to some content preserving attacks.
3. High computational complexity.

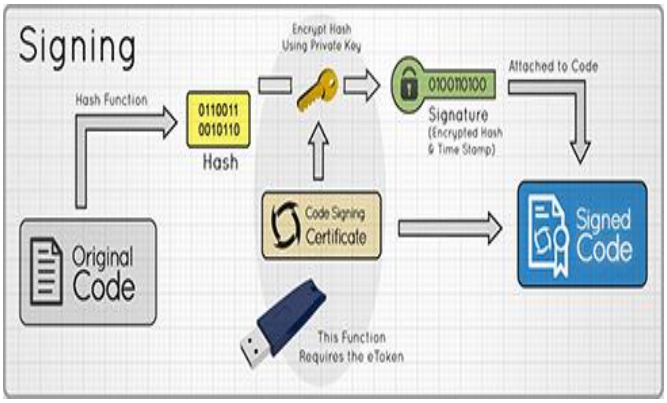

Figure 1: Image Signing Procedure

To manage the above shortcomings, the approach of lifting based wavelet filter parameterization has been suggested as an efficient technique to enhance the security and processing speed of the wavelet transform [16]. Given N parameter values $-\pi \le \alpha i \le \pi$, $o \le i \le N$, the recursion

$$C_0^o = 1/\sqrt{2}, \quad C_1^o = 1/\sqrt{2}$$

$$C_k^n = \frac{1}{2}\left(\left(C_{k-2}^{n-1} + C_k^{n-1}\right)(1 + cos\ \propto_{n-1})\right.$$
$$\left. + \left(C_{2(n+1)-k-1}^{n-1} - C_{2(n+1)-k-3}^{n-1}\right)(-1)^k sin\ \propto_{n-1}\right)$$

can be used to determine the filter coefficients cNk , $0 \le k \le 2N + 2$ and ck for $k < 0$ and $k \ge 2N + 2$. The parameter values used for construction and the resulting wavelet filter coevals are kept secret. Consequently, the technique divides the host image using a wavelet filter constructed with the above specified parameterization. A wavelet transform depends on secret filters can act as a security framework independent of the signing algorithm.

Generation of Structural signature:
This technique uses the same SDS algorithm [4, 11] with the organization of wavelet filter to improve security. In the wavelet domain of an image, the joint parent–child pairs exist. Each child-parent pair maps to a group of spatial pixels, which is of a non-fixed size and possesses certain contextual dependencies [9]. This dependency occurs from the perceptually important features, for example, edges and textures as illustrated in Figure.2.

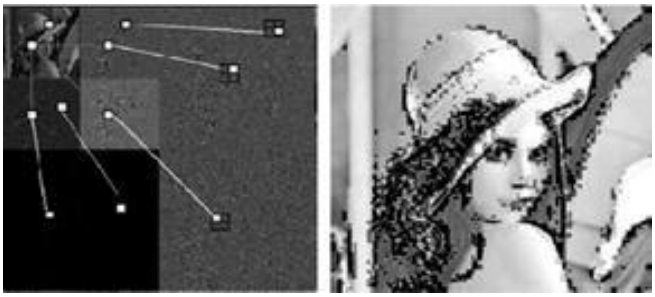

Figure 2: Structural Signature

The basic theory of the SDS algorithm relies on the fact that the parent–child pairs with large magnitudes are not vulnerable to attacks, whereas those with lesser 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 ∂, select each parent–child pair <p, c> with

$$\|<p,c>\| \geq \partial$$

the SDS array is recorded as

$$\mathrm{SDS}[i,j] = \lambda \quad \forall i,j$$

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

$$\lambda = \begin{cases} 1 & :p > 0, |p| > |c| \\ 2 & :p < 0, |p| > |c| \\ 3 & :c > 0, |p| < |c| \\ 4 & :c < 0, |p| < |c| \end{cases}$$

Generate Crypto Signature:
The symbols and their locations in the wavelet domain are encrypted by RSA algorithm. The RSA algorithm works as follow:
1. Select two lager prime numbers p & q such that p≠q
2. Calculate n=p*q and phi=(p-1)*(q-1)
3. Select e such that 1<e<phi and e is coprime to phi
4. Calculate d=e-1 mod phi

This process generate Public key which is [e,n] and Private key [d,n]. The private key is used at the sender side for the encryption. To sign the SDS, compute: $S = M^d \pmod n$, where M is symbol and its location. Generated signature is send to the recipient. The public key is published to the receiver, which is later used for decryption of received signature.

Error Concealment
In general wireless networks methods, the image is transferred over the wireless channels block by block. Because of serious fading, total image blocks can be damaged. In the image validation process, error concealment can be done by through embedded watermarking of information or either using the contextual relationship of adjacent blocks [12]. In this paper, an error concealment algorithm depending on edge directed filters is applied to get better visual quality. A total of this algorithm is explained as follows: Firstly, the corrupted or the attacked image blocks are located by exploring the contextual information in images (e.g. edge continuity). The statistical characteristics of drop blocks are then estimated depending on the types of their surrounding blocks.

Content Authenticity Verification
The main theme of this content authenticity validation is to use patterns to differentiate distortions by transmission glitches from those of attacks, mainly the patterns should be changed into rules, and then the degree of authenticity and the degree of un-authenticity should be determined, and finally the authentication results will be secure. The local distortion of an attacked image is often fixed on some content of interest and the global distortion from transmission is more randomly spreads over the whole image. Furthermore, the attacked areas are more likely to be added. From the above given information, given M, the difference map between the extracted SDS feature vector from the received image and the decrypted signature correlate with the image, the degree of authenticity and un-authenticity is defined as

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

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

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

Here 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)

Here 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

$$s2 = (L\ S)2=8* \ln 2.$$

In this it correlates the of DY with the value of DN, if the value of DY is larger than the value of DN, the image is decided as authentic image, and otherwise the image is decided as an attacked image. All the attacked areas are to be notified. By combining the image features and digital signature the image attack locations are identified from the unauthentic images. Total summary of this method is as follows: First morphological operations are implemented to calculate connected locations and remove the same blocks and little connected locations. Then the difference map (M) is masked by the union of the SDS and image features. The masking operation can redefine the identified locations by concentrating these locations around the objects in the attacked image. Those locations 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.

ADVANTAGES

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 – is achieved by exploiting the concept of structural digital signature (SDS).
3. The integration of the SDS and wavelet filters makes the scheme more efficient to security attacks.
4. The proposed scheme generates only one fixed-length digital signature per image regardless of the image size and the packet loss during transmission.
5. The ability to support efficient and accurate tamper localization in spite of information loss in large areas or high variant areas.

APPLICATIONS

Displaying sample products via mobile terminals in m-commerce, sending critical medical images for remote diagnosis and consultation, transmitting portraits of criminal suspects from law enforcement headquarter to the police officers‟ mobile devices, intelligence satellites sending reconnaissance images of battlefields, and transmission of surveillance video to the mobile terminals.

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. 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.

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

[3] SEITZ J.: ‘Digital watermarking for digital media’ (Idea Group Publishing, 2005), Ch. 2.

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

[5] 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

[6] GINESU G., GIUSTO D.D., ONALI T.: „Mutual image based authentication framework with JPEG2000 in wireless environment‟, EURASIP J. Wirel. Commun. Netw., 2006, 2006, pp. 1–14 .

[7] LIN C.-Y., SOW D., CHANG S.-F.: „Using self authentication and recovery images for error concealment in wireless environment‟. Proc. SPIE ITCom Conf., August 2001

[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.1–1

[9] KUNDER D., HATZINAKOS D.: „Digital watermarking using multiresolution wavelet decomposition‟. Proc. IEEE Int. Conf. Acoustics, Speech and Signal Processing, Seattle, Washington, 1998

[10] Mark Fontenot.: „A WAVELETS INTRODUCTION.‟ CCSC: South Central Conference, February 2002.

[11] 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. 161–173 .

[12] 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.