A Secure Image Transformation Comprising Digital Signature over Wireless Networks

Shanthi Pannala, G.Sumalatha
SreeNidhi Institute of science and Technology

***Abstract*—**with the combination of persistent distribution of the digital images and the rise in concern issues regarding their originality pave way for the urgency in the authentication of images received by unreliable channels. This scheme shows the scalability of a structural digital signature to get a good tradeoff between security transfers for networked image. Under this condition, the inclusion of few multi scale features can be implemented to create digital signatures robust to the degradation of image. The digital signature of the image can be obtained by secure hash algorithm (SHA) and is encrypted by using ElGamal cryptosystem. This scheme will enable us to distinguish tampering areas in the attacked image.

***Keywords*—** *Authentication, Digital image, structural digital signature.*

I. INTRODUCTION

A large number of networked multimedia applications have been created due to drastic developments in the area of networking and digital media technologies. Distributed network environment is being used to deploy these applications. But, this leads to the multimedia content vulnerable to malicious attacks. There is a possibility to corrupt the image content by an enemy in insecure distributed network environment. To ensure content integrity and prevent forgery many image authentication techniques have been developed. These techniques should posses the normal image processing and transmission error handling in addition to detect tampering of images. The application areas of these techniques include law, commerce, journalism and national defense. We can group image authentication techniques as either digital signature based or watermarking based [3,13].

In Digital signature based authentication, an extra file is used to store an essence of an image which will be used for authentication. Signature based methods can work on integrity protection of the image [6].

In watermarking authentication, message is hidden with an image data in order to send information without knowing the existence of the message in an image. At the receiver side the actual message is derived from the image content received.

Watermarking requires other content to hide the actual message whereas digital signature method doesn't require other content to transfer. In Wireless environment, there exist severe limitations on security and the data transmission capability. In order to overcome these limitations we are developing Signature Based image authentication method. During transmission, this method generates only one fixed-length digital signature per image irrespective of the image size and the packet loss.

In order to achieve a good balance between security and image transmission our proposed method ensures the scalability of Secure Digital signature. The proposed method can locate the tampered areas in the corrupted image and can also analyze them. For making digital signature robust multi-scale features are being used.

The proposed signature based authentication will consider the small manipulations on the image as acceptable and it can locate the corrupted area accurately with the help of Stuctural Digital Signature (SDS). This scheme has more efficient to deal with security attacks by combining SDS and key dependent parametric wavelet filters, supports efficient tamper localization even existence of information loss.

II. BACKGROUND

Content authentication of digital media and integrity are the main application areas of Multimedia authentication techniques. We can group image authentication techniques as either digital signature based or watermarking based.

Digital Watermarking is hiding of information such as text, in digital media (images, audio or video). The hiding process is done by changing the content of the digital data. This process should be in such a way that the changes of the media are minimal. For images this means that the changes of the pixel values have to be invisible.

Furthermore, the watermark must be either fragile or robust, depending on the application. By "robust" we mean the capability of the watermark to resist manipulations of the media, such as loss compression where compressing data and then decompressing it retrieves data that may be different from the original, but is close enough to be useful in some way, scaling, and cropping, just to enumerate some. In some cases the watermark may need to fragile. "Fragile" means that the watermark would resist only up to a certain, predetermined extent or should not resist tampering. The first applications are come to mind were related to copyright Protection of digital media [11].

In the past duplicating art work was quite complicated and required a top level of expertise for the counterfeit to look like the original. However, in the digital world this is never correct. Now it is possible for almost anyone to manipulate digital data or duplicate data and not lose data quality. Similar to the process when artists creatively signed their paintings with a brush to claim copyrights and artists of today can watermark their work by hiding their name within the image [8].

This embedded watermark permits identification of the owner of the work. It is clear that this concept is also applicable to other media such as digital audio and video. Currently

unauthorized distribution of digital audio over the Internet in the MP3 format is a big problem. In this scenario a digital watermarking may be useful to set up controlled audio distribution and to provide efficient means for copyright.

III. ANALYSIS OF PROPOSED SCHEME

The first step in developing anything is to state the requirements. This applies just as much to leading edge research as to simple programs and to personal programs, as well as to large team efforts. Being vague about your objective only postpones decisions to a later stage where changes are much more costly.

The problem statement should state what is to be done and not how it is to be done. It should be a statement of needs, not a proposal for a solution. A user manual for the desired system is a good problem statement. The requestor should indicate which features are mandatory and which are optional, to avoid overly constraining design decisions. The requestor should avoid describing system internals, as this restricts implementation flexibility. Performance specifications and protocols for interaction with external systems are legitimate requirements. Software engineering standards, such as modular construction, design for testability, and provision for future extensions, are also proper.

Many problems statements, from individuals, companies, and government agencies, mixture requirements with design decisions. There may sometimes be a compelling reason to require a particular computer or language; there is rarely justification to specify the use of a particular algorithm. The analyst must separate the true requirements from design and implementation decisions disguised as requirements. The analyst should challenge such pseudo requirements, as they restrict flexibility. There may be politics or organizational reasons for the pseudo requirements, but at least the analyst should recognize that these externally imposed design decisions are not essential features of the problem domain.

A problem statement may have more or less detail. A requirement for a conventional product, such as a payroll program or a billing system, may have considerable detail. A requirement for a research effort in a new area may lack many details, but presumably the research has some objective, which should be clearly stated.

Most problem statements are ambiguous, incomplete, or even inconsistent. Some requirements are just plain wrong. Some requirements, although precisely stated, have unpleasant consequences on the system behavior or impose unreasonable implementation costs. Some requirements seem reasonable at first but do not work out as well as the request or thought. The problem statement is just a starting point for understanding the problem, not an immutable document. The purpose of the subsequent analysis is to fully understand the problem and its implications. There is no reasons to expect that a problem statement prepared without a fully analysis will be correct.

The analyst must work with the requestor to refine the requirements so they represent the requestor's true intent. This involves challenging the requirements and probing for missing information. The psychological, organizational, and political considerations of doing this are beyond the scope of this book, except for the following piece of advice: If you do exactly what the customer asked for, but the result does not meet the customer's real needs, you will probably be blamed anyway.

The proposed scheme consists two phases: Image Signing Procedure and Image authentication Procedure. These two methods are discussed below.

A. Image signing procedure

In the image signing procedure image is been sent through wireless channels then the system generates a digital signature by performing a signing process on the image in the following manner. First the image is decomposed by using parameterized wavelet filters, then extraction of digital signature cryptographically hash the extracted SDS by using secure hashing algorithm, and generate the crypto signature by the image sender's private key, and send the image and its associated crypto signature to the recipient. In order to obtain robustness, no compression and coding is used, since they will cause error propagation.

Wavelet parameterization:

The image's signature that is generated is constructed in the wavelet domain. Wavelet transform is characterized by energy compaction and de-correlation properties. Hence, it is employed to generate a compact representation that exploits the structure of the image effectively.

Structural signature:

The proposed scheme uses the same SDS algorithm in the development of wavelet filter parameterization to increase security. In the wavelet domain of an image, which is also called as joint (inter scale) parent–child pairs exist. Each parent–child pair maps to a set of spatial pixels which are of a non-fixed size and possesses certain contextual dependencies. This dependency arises from the perceptually important features.

B. Image authentication procedure

In the image authentication procedure, the corrupted images that are given by transmission and their associated digital signatures, the proposed scheme authenticates both the integrity and the source of the received image by applying the authentication process on the image in the following order. If some blocks are damaged then perform content-adaptive error concealment and extract the SDS of the received image using the same method that has been used in image signing procedure. Then decrypt the signature by using the sender's public key to calculate the degree of authenticity, perform a content authenticity verification procedure using both the decrypted signature and the extracted one.

Error concealment

In order to achieve better visual quality an error concealment algorithm based on edge-directed filters is applied. Overall summary of this algorithm is as follows. First, the damaged blocks of image are detected by exploring the contextual information in images. The statistical characteristics of missing blocks of image are then estimated based on the types

of their surrounding blocks. At last, a directional interpolation strategy for error concealment is applied.

Content authenticity verification

The proposed scheme implements the same verification procedure for content verification. The basic idea of this procedure is to use patterns to differentiate damages by transmission errors from those of attacks, convert these patterns into rules, calculate the degree of authenticity and un-authenticity, and finally obtain the authentication results.

IV. ILLUSTRATION OF THE PROPOSED SCHEME

The secure transmission of the image requires that the image is to be digitally signed and the signature is transmitted to the receiver securely. Here the digital signature is obtained by using secure hash algorithm (SHA-1) [16] and is encrypted by using ElGamal algorithm [17]. The receiver can receive the image and encrypted form of the digital signature. After receiving the image and signature, is to be decrypted by using ElGamal decryption procedure and the signature is verified. If the calculated signature is matches with the received signature then the receiver ensures that the original image has been received otherwise the image is corrupted. The algorithm of ElGamal cryptosystem and flowcharts for sending and receiving images along with signature are depicted below.

ElGamal Cryptosystem:

The ElGamal cryptosystem consists three phases: key generation, encryption and decryption.

Key Generation

1. Select a large prime p
2. Chose a generator g from the multiplicative Group z_p^*.
3. Select a random integer a, such that $1 \le a \le p-2$.
4. Compute $g^a \bmod p$.
5. Public key is (p, g, g^a),
6. Private Key is a.

Encryption:

Input: Public key elements: (p, g, g^a).

1. Represent the message as integer m in the range [0... p-1].
2. Select random integer k, $1 \le k \le p-2$.
3. Compute $c1 = g^k \bmod p$ and $c2 = m \times (g^a)^k$.
4. Cipher text c= (c1, c2)

Decryption:

Input: a, c1, c2, p

1. Calculate $(c_1^{-a})^{-1} * c_2 \bmod p$

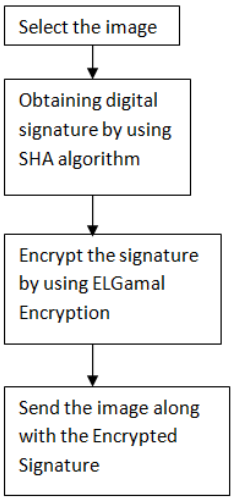

Fig.1 Flowchart for image-signature encryption

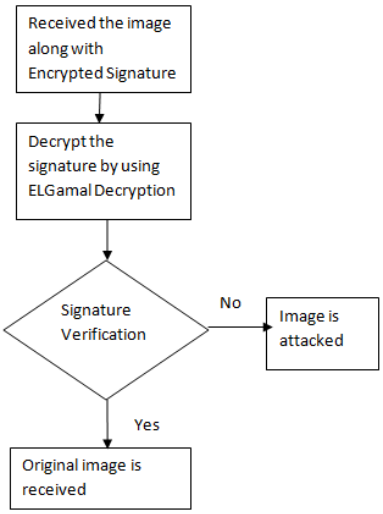

Fig.2 Flowchart for image-signature verification

V. CONCLUSION

In this paper, a 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. The authentication of the image is obtained by using secure hash algorithm and to encrypt the signature the ElGamal algorithm is used. Because the proposed scheme does not require any computational overhead, it is especially suited for wireless authentication systems and other real-time applications.

VI. REFERENCES

[1] Barros J, Rodrigues M.R.D: (2006). Secrecy capacity of wireless channel. Seattle, Information Theory: Proc. IEEE Int. Symp.

[2] Ye s, Sun Q, Chang E.C. (2004). 'Edge directed filter based error. Concealment for wavelet-based images'. Singapore: Proc. IEEE Int. Conf. Image Processing.

[3] Fridrishj, Baldozaa, Simredr.J. April (1998). 'Robust digital watermaking based on key dependent basis functions '.vol. 1525,IH, Portland, OR, USA: Proc.int.Comnf.LNCS,143-157.

[4] Swaminathan A., Mao Y., Wu M. (2006). 'Robust and secure image Hashing'. IEEE Trans. Inf. Forensics Sec. 1 (2), 215-229.

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

[6] Lu C.S, Liao H.M. (2003). 'Structural digital signature for image authentication: an incidental distortion resistant scheme'. IEEE Trans. on Multimed. 5 (2), 161-173.

[7] Martinian E. Wornell G.W. Chen B. (2005). 'Authentication with distortion criteria'. IEEE Trans. Inf. Theory. 3 (2), 1-22.

[8] Peter M., Uhl M (2000). 'Watermark security via wavelet filter parameterization'. 2nd ed. USA: Proc. Int. Conf. ICASSP. 35-40.

[9] Ginesu G., Giusto D.D., Onali T.. (2006). 'Mutual image based authentication framework with JPEG2000 in wireless environment'.EURASIP J. Wirel. Commun. Netw., 2006,. 2 (2), 1-14.

[10] Schneider M., Chang S.-F. (1996). 'A content based digital signature for image authentication'. Proc. IEEE Int. Conf. Image Processing.

[11] Anthony T, Ho S, Yong L.G: (2004). 'Image content authentication using pinned sine transform'. 14th ed. hyd: EURASIP J. Appl. Signal Process. 2174 2184 .

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

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

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

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

[16] http://csrc.nist.gov/publications/fips/fips180-4/fips-180-4.pdf

[17] Taher ElGamal.A public key cryptosystem and a signature scheme based on discrete logarithms. In Proceedings of CRYPTO 84 on Advances in cryptology, pages 10-18.Springer-Verlag New York Inc. 1985