ISSN 2250-3153

Robust Digital Signature for Image Authentication

Debkamal Mohapatra, Brijesh Mishra

Abstract- Robust digital signature verifies the originality of an image by detecting malicious manipulations. Its goal is different from that of image watermarking, which embeds into the image a signature surviving most manipulations. In this paper, we present an effective technique for image authentication which can prevent malicious manipulations but allow JPEG lossy compression. The authentication signature is based on the invariance of the relationships between discrete cosine transform (DCT) coefficient at the same position in separate blocks of an image.

Index Terms- Digital signature, Authentication, JPEG, Discrete cosine transform

I. INTRODUCTION

Due to the presence of powerful multimedia tools, the age of "seeing is believing" no longer exists. Therefore, it has led to reduction in credibility of multimedia data such as photos, audio or video clips, printed documents. To ensure trust-worthiness, multimedia authentication techniques are being developed to protect multimedia data by verifying the information integrity, the alleged source of data, and the reality of data. This distinguishes from other generic message authentication in its unique requirements of integrity. Multimedia data are generally compressed and quality enhanced. Thus, accepting lossy compressed multimedia and some content-preserving filtering is an essential requirement in many applications. [3]

II. PRINCIPLE AND WORKING

RDS is an encrypted form of the feature codes of the multimedia data. When a user needs to authenticate the received data, he should decrypt this signature and compare the feature codes to their corresponding values in the signature. If the derived feature codes match the range space of the original feature codes after acceptable manipulations, this multimedia data is said to be "authentic." How to extract (short) feature codes that are invariant to acceptable manipulations but sensitive to malicious changes is the main challenge of RDS. We found that some strictly quantitative invariants and predictable properties can be extracted when multimedia data is transcoded by quantization based compressions. For instance, because all DCT coefficient matrices of images are divided by the same quantization table in the JPEG compression process, the relationship between two DCT coefficients of the same coordinate position should remain the same after the quantization process.

Furthermore, due to the rounding effect after quantization, the relationship of the two may be the same or become equal. In other words, if one coefficient Fp(n) in the position n of block p is larger than the other coefficient Fq(n) in the position n of block q, then after compression, their relationship, Fp _(n) ≥ Fq _(n), where

Fp _(n) = Integer Round (Fp(n)/Q) • Q and Fq _(n) = Integer Round (Fq(n)/Q) • Q, is guaranteed. It can be summarized as Theorem 1: [2]

Theorem 1:

- if Fp(n) > Fq(n) then Fp_(n) ≥ Fq_(n),
- if Fp(n) < Fq(n) then Fp_(n) ≤ Fq_(n),
- if Fp(n) = Fq(n) then Fp_(n) = Fq_(n).

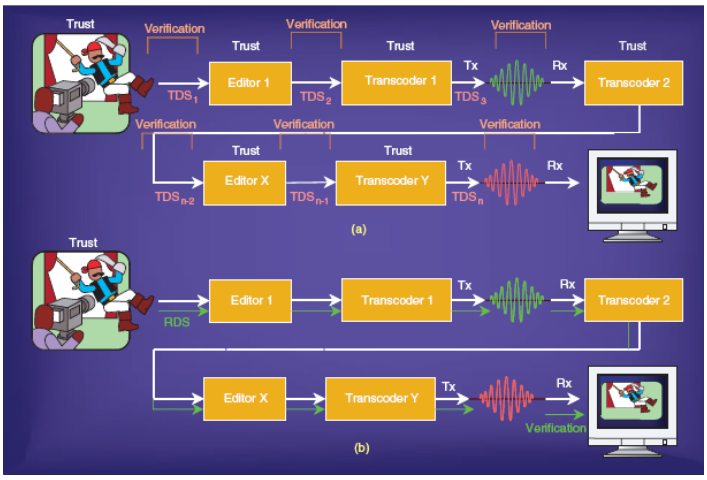

Fig 1 : Multimedia authentication: (a) using traditional digital signatures (TDS)—trust all parties and verify multiple digital signatures; (b) using robust digital signatures (RDS)—trust only the original signer and verify a single signature.

Given a signature derived from the original image and a JPEG compressed image bitstream, for authentication, at the first step, we have to decrypt the signature and reconstruct DCT coefficients. Because the feature codes decrypted from the signature record the relationship of the difference values and *zero*, they indicate the sign of the difference of DCT coefficients, despite the changes of the coefficients incurred by lossy JPEG compression. If these constraints are not satisfied, we can claim that this image has been manipulated by another method.

III. HARDWARE ARCHITECTURE

- A Computer not essential with the server configuration.
- RAM Configuration of minimum 1GB
- CPU of minimum 2.9 GHZ.

IV. SOFTWARE ARCHITECTURE

- Front End : MATLAB 2007

V. OPERATION

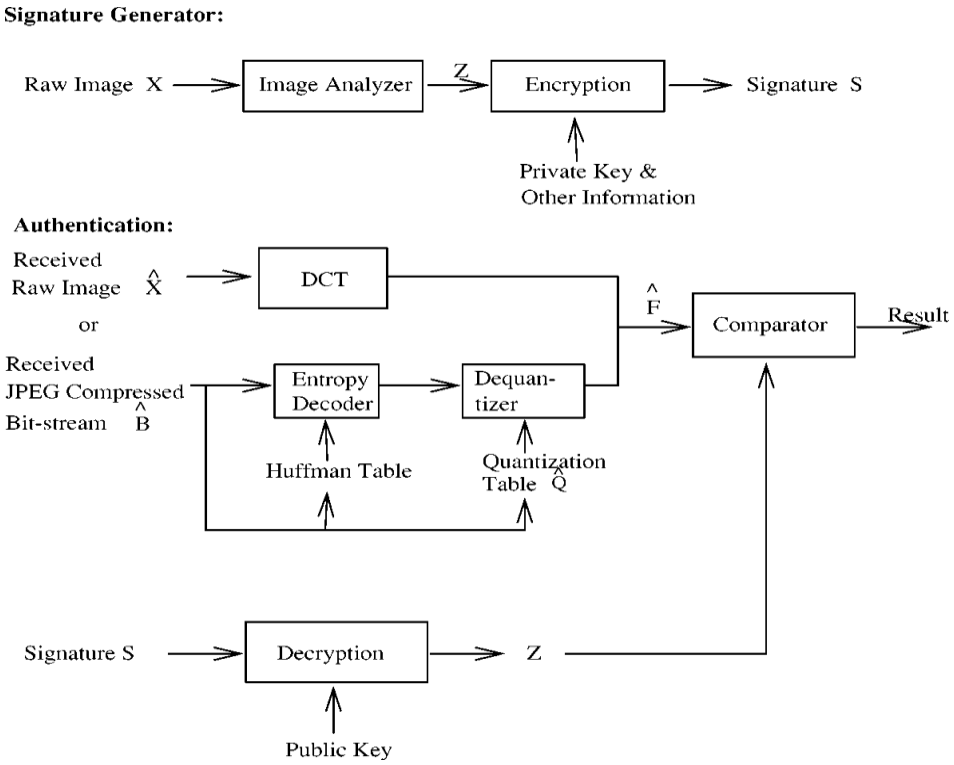

Fig 2 : Signature Generation and Authentication Process

VI. ADVANTAGES

Detecting of malicious manipulations and allowing JPEG compression is its biggest advantage. Restoration of the image to its original authentic state using the signature can be done. In future, This technique can also be applied to video authentication as well. With watermarking embedded in the image we can obtain a better quality correction from modified image.

VII. CONCLUSION

The software was developed according to the plan we had. After its development, the software was tested and was able to detect manipulations in an image and was also able to distinguish between JPEG compression and other manipulations. It was also able to restore the image perfectly to its original state.

ACKNOWLEDGMENT

This project was very helpful in giving us a great insight about authentication of image from malicious manipulations and also learned about the use of DCT coefficients in these. We are very grateful to Mr. Sanjeeb kumar ghosh who provided us with the helpful information in the development of ROBUST DIGITAL SIGNATURE FOR IMAGE AUTHENTICATION.

REFERENCES

[1] S. Bhattacharjee and M. Kutter, "Compression tolerant image authentication," in Proc. IEEE Int. Conf. Image Processing, Chicago, IL, Oct.1998.

[2] Ching – Yung Lin and Shih-Fu Chang, " Circuits And Systems ", IEEE Trans on Image Signature/Authentication, Vol. 1, No. 3, Feb 2001.

[3] William Stallings, "Network Security and Cryptography", Prentice – Hall of India publishers, 3rd Edition, New Delhi, 2005

AUTHORS

First Author – Debkamal Mohapatra, Electronics & Telecommunication Engineer., Email id: debkamal.mohapatra@gmail.com
Second Author – Brijesh Mishra, Electronics & Telecommunication Engineer. Email id: brijesh027@gmail.com