An Overview to the Proposed Technique for Image Authentication Using LDPC Codes

[1]Imran Ali Khan, [2]Bhanu Pratap Singh Sengar
[1,2]Dept. of CSE, All Saint's College of Technology, Bhopal, MP, India

Abstract

Image authentication is important in content delivery via untrusted intermediaries, such as peer-to-peer (P2P) file sharing. Many differently encoded versions of the original image might exist. In addition, intermediaries might tamper with the contents. Distinguishing legitimate diversity from malicious manipulations is the challenge addressed in this dissertation.

We proposed an approach using encryption and LDPC source coding for the image authentication problem. The key idea is to provide a Slepian-Wolf encoded quantized image projection as authentication data which is again encrypted using a secret key cryptography before ready to send. This can be correctly decoded with the help of an authentic image as side information.

Keywords

Image Security, Image digest, image authentication, Digital Image Processing

I. Introduction

In today's world, digital images are being widely used in numerous applications such as military, intelligence, surveillance, digital copyright applications, etc. Among the existing image formats, JPEG is the most widely used formats that store the digital images using digital cameras and software tools [2]. With the increase in use of multimedia type data over the internet. The Image authentication plays an important role in security and communication. Images are being transferred over the Internet and are readily available for access from any part of the world and without introducing an authentication mechanism, it is almost impossible to distinguish if an image is original or being manipulated.

Using cryptographic methods to authenticate image data will result in an unworkable system or unacceptable systems because data authentication is sensitive to single bit change in the original data while image authentication systems need to be mainly content sensitive [5]. This is because images undergo a range of processing including lossy compression that result in changes in bits that are deemed acceptable. Such changes must be tolerable by the authentication system while it is essential for the system to remain sensitive to malicious manipulations. Many organizations are struggling with the issue of photo tampering. For example, digital images, videos, and audio are now routinely introduced as evidence in civil, criminal, and national security cases. In such cases, the integrity of digital evidence is central.

Digital image processing is the technology of applying a number of computer algorithms to process digital images [4]. The outcomes of this process can be either images or a set of representative characteristics or properties of the original images. The applications of digital image processing have been commonly found in robotics/intelligent systems, medical imaging, remote sensing, photography and forensics.

Digital image processing directly deals with an image, which is composed of many image points. These image points, also namely pixels, are of spatial coordinates that indicate the position of the points in the image, and intensity (or gray level) values. A colorful image accompanies higher dimensional information than a gray image, as red, green and blue values are typically used in different combinations to reproduce the colors of the image in the real world.

The main purpose of digital image processing is to allow human beings to obtain an image of high quality or descriptive characteristics of the original image [2]. In addition, unlike the human visual system, which is capable of adapting itself to various circumstances, imaging machines or sensors are reluctant to automatically capture "meaningful" targets. For example, these sensory systems cannot discriminate between a human subject and the background without the implementation of an intelligent algorithm. We shall classify attacks into two types:-

A. Passive Attacks

Passive attacks do no involve any modifications to the contents of an original message. These are further classified into two sub-categories:

1. Release of Message Content

It is quite simple to understand when we send a confidential email message to our friend; we desire that only she/he be able to access it. Otherwise the content of message is released against our wishes to someone else.

2. Traffic Analysis

A passive attacker could try to figure out similarities between messages to come up with some sort of pattern that provide her/him some clues regarding the communication that is taking place. Such attempts of analyzing messages to come up with likely patterns are the work of traffic analysis attack

B. Active Attacks

Active attacks are based on modifications to the contents of an original message in some manner or creation of a false message. These are attacks cannot be prevented easily. These are further classified into three subcategories:-

1. Interruption (Masquerade)

It is caused when an unauthorized entity pretends to be an authorized (another) entity. For Example, an authorized user C might pose as an authorized user A and send a message to user B. User B might be lead to believe that the message indeed came from user A [2,6]. In masquerade attacks, usually some other forms of active attacks are also embedded. As an instance, the attack may involve capturing the user`s authentication sequence (e.g. user ID and password).

2. Modification

Modification refers to the change in message contents.

II. Multimedia Information

In this digital revolution, the explosion of communication networks, and the increasingly growing passion of the general public for new information technologies lead to exponential growth of multimedia document traffic (image, text, audio, video, etc.). This phenomenon is now so important that insuring protection and control of the exchanged data has become a major issue. Indeed, from their digital nature, multimedia documents can be duplicated, modified, transformed, and diffused very easily. In this context, it is important to develop systems for copyright protection, protection against duplication, and authentication of content [6,9]. Watermarking seems to be the alternative solution for reinforcing the security of multimedia documents.

III. Literature Survey

In year 2010, E Kee et. al. proposed a method [29] that describes how to exploit the formation and storage of an embedded image thumbnail for image authentication. The creation of a thumbnail is modelled with a series of filtering operations, contrast adjustment, and compression. We automatically estimate these model parameters and show that these parameters differ significantly between camera manufacturers and photo-editing software. We also describe how this signature can be combined with encoding information from the underlying full resolution image to further refine the signature's distinctiveness.

Past approaches for image authentication fall into three groups: forensics, watermarking, and robust hashing. In digital forensics, the user verifies the authenticity of an image solely by checking the received content [8- 9]. Unfortunately, without any information from the original, one cannot completely confirm the integrity of the received content because content unrelated to the original may pass forensic checking. Another option for image authentication is watermarking. A semi-fragile watermark is embedded into the host signal waveform without perceptual distortion [10-11]. Users can confirm authenticity by extracting the watermark from the received content. The system design should ensure that the watermark survives lossy compression, but that it breaks as a result of malicious manipulations. Unfortunately, watermarking authentication is not backward compatible with previously encoded contents; i.e., unmarked content cannot be authenticated later. Embedded watermarks might also increase the bit rate required when compressing a media file.

Similarly Yao et. al. [12] developed an authentication techniques based on robust hashing, which is inspired by cryptographic hashing [13]. In this technique, the user checks the integrity of the received content using a small amount of data derived from the original content. Many hash-based image authentication systems achieve robustness against lossy compression by using compression-invariant features, such as [14-15]. These compressions-inspired features are designed for particular compression schemes but fail under other coding schemes or common image processing. Robustness is increased using more sophisticated features, such as block-based histograms [16], zero-mean low-pass Gaussian pseudo-random projection [17-18], block standard deviations and means [17-18], column and row projections [19], and transform coefficients [20-21]. Any fixed projection has the weakness that an attacker who knows the null space of the projection can alter the image without affecting the authentication data. Using pseudo-random projections or tiling's, such as in [22], keeps the null space a secret. Similar considerations apply to features calculated in a nonlinear manner. Features robust against rotation, cropping, resizing, or translation has been proposed based on the Radon transform [23- 24], the Fourier transform [25], and pixel statistics along radii [25- 26]. Other methods include features important to the human visual system [28].

Quantization and compression of authentication data have not been studied in depth. Most approaches use coarse quantization. For example, Fridrich et al. Use 1-bit quantization for random projection coefficients and the relation-based approaches can be considered as 1-bit quantization of coefficients differences. The first to consider error-correcting coding in reducing the image authentication data size were Venkatesan et al. [21]. The idea is to project the binary feature vectors of both images into syndrome bits of an error-correcting code and directly compare the syndrome bits to decide the authenticity.

The approach of Sun et al. uses systematic Hamming codes to obtain the parity check bits of the binary feature vectors as the authentication data [30]. These parity check bits are concatenated with the binary feature vector of the received image to correct the errors introduced by image processing, such as compression. Our novel ideas make further improvements with the knowledge of distributed source coding and statistical methods. Inspired by our approach, Tagliasacchi et al. Proposed using Wyner–Ziv coding and compressive sensing for image authentication by exploiting additional assumptions on the sparsity of tampering.

Therefore, after analyzing all the above research work, it is found that still this research area has a wide space of simple and effective techniques for image authentication. Hence, in this dissertation work we proposed a mechanism for image authentication based on the encoding-decoding scheme of low density parity check methods along with the proper use of cryptology. The proposed methodology ensures that the image received at receiver side is original and un-tampered.

IV. Problem Definition

The Objective of this proposed work is to implement a robust technique that works for the authentication of images that can recognize as small as possible changes in the altered image in comparison with the original image. Using the manipulation tools that are available on the internet it is easy to tamper the digital images without any trace. Therefore, verification of originality of images has become a challenging task. The early research in image forensics introduced digital watermarking and robust hashing in the original image for authentication.

V. Proposed Work

The proposed technique uses image authentication system using distributed source coding. The authentication data consists of a Slepian–Wolf as in figure1 encoded quantized pseudorandom projection of the original image, a random seed, and a signature of the image projection. The target image is modeled as an output of the two-state lossy channel. The user projects the target image using the same projection to yield the side information and tries to decode the Slepian–Wolf bit stream using the side information. If the decoding fails, i.e., the hash value of the reconstructed image projection does not match the signature, the verification decoder claims it is tampered; otherwise, the reconstructed image projection along with the side information is examined using hypothesis testing.

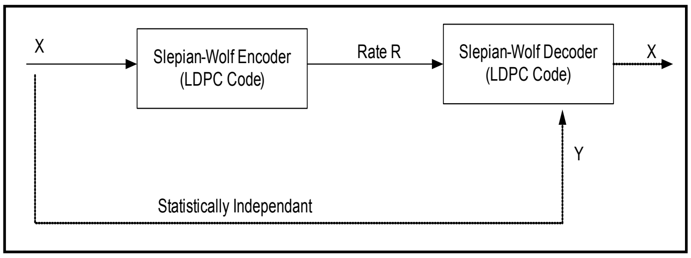

Fig. 1: Simple Image Authentication System

In the proposed approach for the image authentication, there is usage of an image encryption using secret key as depicted in the fig. 2. Therefore, in the proposed research the message digest (size 60x60 pixels) will be encrypted at the sender side and then sent to the receiver.

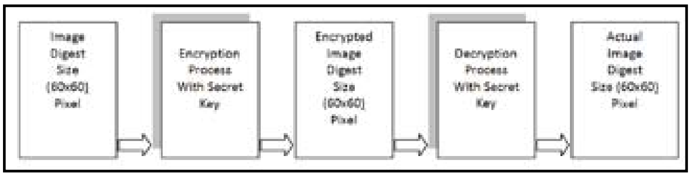
Image Digest Size (60x60) Pixel
Encryption Process With Secret Key
Encrypted Image Digest Size (60x60) Pixel
Decryption Process With Secret Key
Actual Image Digest Size (60x60) Pixel

Fig. 2: Encryption Process with Secret Key

VI. Conclusion

In this paper, we analyses the previous work done in the same domain and proposes a novel image authentication scheme that distinguishes legitimate encoding variations of an image from tampered versions based on distributed source coding and statistical methods. A two-state lossy channel model represents the statistical dependency between the original and the target images. Tampering degradations are captured by using a statistical image model, and legitimate compression noise is assumed to be additive white Gaussian noise.

References

[1] J. Fridrich, D. Soukal, J. Luk´aˇs,"Detection of copy move forgery in digital images," in Proceedings of Digital Forensic Research Workshop, 2003 August.

[2] A. Popescu and H. Farid,"Exposing digital forgeries by detecting duplicated image regions", Tech. Rep. TR2004-515, Department of Computer Science, Dartmouth College, 2004.

[3] Z. Lin, R. Wang, X. Tang, H.-V. Shum,"Detecting doctored images using camera response normality and consistency", in Computer Vision and Pattern Recognition, (San Diego, CA), 2005.

[4] M. Johnson, H. Farid,"Exposing digital forgeries in complex lighting environments", IEEE Transactions on Information Forensics and Security 3(2), 2007, pp. 450–461.

[5] J. Luk´aˇs, J. Fridrich, M. Goljan, "Digital camera identification from sensor noise", IEEE Transactions on Information Security and Forensics 1(2), 2006, pp. 205–214.

[6] Gallager, R. G.,"Low Density Parity Check Codes, Monograph", M.I.T. Press, 1963.

[7] H. Farid,"Image forgery detection", IEEE Signal Process. Mag., Vol. 26, No. 2, Mar 2009, pp. 16–25.

[8] A. Popescu, H. Farid,"Exposing digital forgeries in color filter array interpolated images", IEEE Trans. Signal Process., Vol. 53, No. 10, Oct. 2005, pp. 3948–3959.

[9] I. J. Cox, J. Kilian, T. Leighton, and T. Shamoon,"Secure sprectrum watermarking for images, audio and video", in Proc. I Conf. Image Process., Lausanne, Switzerland, 1996, Sep.

[10] R. B. Wolfgang, E. J. Delp,"A watermark for digital images", in Proc. IEEE Int. Conf. Image Process., Lausanne, Switzerland,1996, Sep.

[11] Yao-Chung Lin, David Varodayan,"Image Authentication Using Distributed Source Coding", In IEEE Transactions on Image Processing, Vol. 21, No. 1, January 2012, pp. 273-283

[12] W. Diffie, M. E. Hellman,"New directions in cryptography", IEEE Trans. Inf. Theory, Vol. IT-22, No. 6, Jan. 1976, pp. 644–654.

[13] C.-Y. Lin, S.-F. Chang,"Generating robust digital signature for image/video authentication", in ACM Multimedia: Multimedia and Security Workshop, Bristol, U.K., Sep. 1998, pp. 49–54.

[14] M. Schlauweg, D. Pröfrock, E. Müller, "JPEG2000-based secure image authentication", in Workshop on Multimedia and Security, 2006, Geneva, Switzerland, pp. 62–67.

[15] M. Schneider, S.-F. Chang,"A robust content based digital signature for image authentication", in Proc. IEEE Int. Conf. Image Process., Vol. 3, Sep. 1996, pp. 227–230.

[16] J. Fridrich, "Robust bit extraction from images", in Int. Conf. Multimedia Computing and Syst., Vol. 2, Jul. 1999, pp. 536–540.

[17] D.-C. Lou, J.-L. Liu,"Fault resilient and compression tolerant digital signature for image authentication", IEEE Trans. Consumer Electronics, Vol. 46, No. 1, Feb. 2000, pp. 31–39.

[18] L. Xie, G. R. Arce, R. F. Graveman,"Approximate image message authentication codes", IEEE Trans. Multimedia, Vol. 3, No. 2, Jun. 2001, pp. 242–252.

[19] R.-X. Zhan, K. Y. Chau, Z.-M. Lu, B.-B. Liu, W. H. Ip, "Robust image hashing for image authentication based on DCT-DWT composite domain", in Proc. IEEE Int. Conf. Intelligent Syst. Design and Application, Vol. 2, 2008, Nov. pp. 119–122.

[20] H. Zhang, H. Zhang, Q. Li, and X. Niu,"Predigest Watson's visual model as perceptual hashing method", in Int. Conf. Convergence and Hybrid Inf. Technol., 2008, Nov, Vol. 2, pp. 617–620.

[21] R.Venkatesan, S.-M.Koon,M.H. Jakubowski, P.Moulin, "Robust image hashing", Proc. IEEE Int. Conf. Image Process., Vol. 3, 2000, pp. 664–666.

[22] F. Lefebvre, J. Czyz, B. Macq,"A robust soft hash algorithm for digital image signature", in Int. Conf.Multimedia and Expo, 2003, Baltimore, MD.

[23] H.-L. Zhang, C.-Q. Xiong, G.-Z. Geng,"Content based image hashing robust to geometric transformations", in Proc. Int. Symp. Electronic Commerce and Security, 2009, May, Vol. 2, pp. 105–108.

[24] A. Swaminathan, Y. Mao, M. Wu,"Robust and secure image hashing", IEEE Trans. Inf. Forensics and Security, Vol. 1, No. 2, Jun. 2006, pp. 215–230.

[25] C. De Roover, C. DeVleeschouwer, F. Lefebvre, B.Macq, "Robust video hashing based on radial projections of key frames", IEEE Trans. Signal Process., Vol. 53, No. 10, Oct. 2005, pp. 4020–4037.

[26] Z. Tang, S.Wang, X. Zhang, W.Wei,"Perceptual similarity metric resilient to rotation for application in robust image hashing", in Proc. Int. Conf. Multimedia and Ubiquitous Eng., Jun. 2009, pp. 183–188, 2009.

[27] V. Monga, B. L. Evans,"Perceptual image hashing via feature points: Performance evaluation and tradeoffs", IEEE Trans. Image Process., Vol. 15, No. 11, Nov. 2006, pp. 3452–3465.

[28] M. Schlauweg, E. Müller,"Gaussian scale-space features for semi-fragile image authentication", in Proc. Picture Coding Symp., May 2009, pp. 1–4.

[29] E Kee, H Farid,"Digital Image Authentication from Thumbnails", in SPIE Symposium on Electronic Imaging,

San Jose, CA, 2010.

[30] M. Tagliasacchi, G. Valenzise, S. Tubaro,"Hash-based identification of sparse image tampering", IEEE Trans. Image Process., Vol. 18, No. 11, pp. 2491–2504, Nov. 2009.

Author is pursuing M.Tech. (Computer Science and Engineering) from All Saints' College of Technology, Bhopal. He has done Bachelor of Engineering (Computer Science and Engineering) from All Saints' College of Technology in 2007, Bhopal. His research interest in Image processing, Image Authentication, Distributed Source Coding. He is professional member of various national and international bodies.