International Journal of Advanced Computer Research (ISSN (print): 2249-7277 ISSN (online): 2277-7970)
Volume-3 Number-3 Issue-12 September-2013

Key Generation and Verification for Image Authentication

Soheb Munir[1], A.S.Zadgaonkar[2], Manish Shrivastava[3]

Abstract

We present a novel approach using distributed source coding for image authentication. The key idea is to provide a Slepian–Wolf encoded quantized image projection as image authentication data. This can be correctly decoded with the help of an authentic image using as side information. Distributed source coding provides the desired robustness against legitimate variations while detecting illegitimate modification. The decoder incorporating expectation maximization algorithms can authenticate images which have undergone contrast, brightness, and affine warping adjustments. We introduce the image authentication system using distributed source coding from transmitter side to receiver side. We formulate image authentication problem as a hypothesis testing problem. The original image projection is quantized and encoded using chaos based coding, a form of distributed source coding. By correctly choosing the size of the chaos based bit stream, it can be decoded using the legitimate image as side information.

Keywords

Key Generation, Image Authentication, Slepian–Wolf, Encryption

1. Introduction

In today's commercial environment, establishing a framework for the authentication of computer-based information requires a familiarity with concepts and professional skills from both the legal and computer security fields. Combining these two disciplines is not an easy task. Concepts from the information security field often correspond only loosely to concepts from the legal field, even in situations where the terminology is similar. For example, from the information security point of view, "digital signature" means the result of applying to specific information certain specific technical processes described below. Digital certification gives the user a sense of legitimacy and formalizes the process. It ensures that the company that the user is dealing with has a registration with a trusted authority and that the transaction is guaranteed to be done with the intended parties. Now we will define the basic components of Digital Signature i.e. Encryption, Decryption and Hashing.

1.1 Basics Purpose of Encryption

The purpose of this document is to provide a high level overview of encryption, and some of the standard techniques in which it is used to protect information. This includes such topics as encryption types, hashing, email, data transfer, remote access, key management, and securing portable devices like laptops, blackberry's, smart phones etc.
This document does not intend to recommend or promote any particular product or technology. Where specific brands or products are mentioned, they are used as examples only. There are many solutions available, and this makes no attempt to recommend any one solution over another [1].

1.2 Encryption

Encryption is simply defined as the process of transforming information (referred to as plaintext) using an algorithm (called cipher) to make it unreadable to anyone except those possessing special knowledge, usually referred to as a key."

1.3 Asymmetric vs. Symmetric Encryption

"Are there different kinds of encryption? And how do I know if they are truly safe?" There are a few things about encryption that are important to understand. There are many books and other publications on the subject of encryption that go into much more detail, but here are the basic things that everyone should understand [1]:

1.4 Symmetric Encryption

Cryptographic solutions fall into one of two types. Symmetric encryption requires that each party who wants to decipher the encoded message (cipher text) must have the secret key (or password). So if person X wanted to send person Y his grandmother's secret recipe for chocolate chip cookies, he could encrypt the message and use the key to do so. Now for Y to decrypt that message, she would need to know the password (or "key"). This works well when the intended recipients are few or when there are only a small number of secret messages that will be delivered over time. However, the management of secret keys for each message becomes complicated

real fast especially as the number of intended recipients grows. This can become a key management [1,2].

1.5 Asymmetric Encryption

Not long ago, some real smart people from MIT developed a system known as Public Key encryption. Simply described, each person has two keys. One is a secret (or Private) key, and the other is a Public key. Public keys can be stored in a public database for anyone to see. If X wants to send Y a secret message, all he needs to do is to encrypt that message with Y Public key and send her the message. The trick is that only that Y's Private key can decrypt the message. Now Y and X do not need to worry about sending the private keys to anyone, because they only need to know each other's Public keys, and can keep their private keys to themselves. Additionally, X can encrypt a message with his Private Key knowing that anyone can decrypt it with his Public key. Now why would X want to do this? Because anyone who used X's Public key to decrypt the message would know that only X could have encrypted it (remember that X used his Private Key that only he knows). This process is referred to as "Digitally Signing" and it is used to prove the origin of the message. In this manner, a digital signature is much more reliable than a written signature which can often be easily forged [2].

1.6 Hashing

Another clever use of encryption is to create a unique fixed length string of characters from a selected text (such as the entire document). This string is called a HASH. If anything at all changes within that document (or file) then the HASH is completely different. This process is used to verify the INTEGRITY of the file. Using this hashing process, and by comparing the hashes of the original and received messages or files, Y could tell immediately if anything had been altered within the message [1].

2. Literature Review

This paper first reviews about the introduction of distributed source coding techniques and low density parity check (LDPC) codes. A new method of distributed source coding for binary sources using low density parity check codes is to be developed. This new scheme for distributed source coding of binary sources using low density parity check codes is developed and implemented in the probability domain as opposed to the log domain presented by Liveris et. al. [3] . The performance of these schemes is analyzed by comparing the bit error rate and symbol error rate for different correlations between two randomly generated binary and non-binary sources respectively. Gallager's [4] low density parity check (LDPC) codes are defined by sparse parity check matrices, usually with a random construction. Such codes have near Shannon limit performance when decoded using an iterative probabilistic decoding algorithm. Low density parity check codes are also shown to be useful for communicating over channels which make insertions and deletions as well as additive (substitution) errors. LDPC codes can also be extended over non binary sources for channel coding by Davey et. al. [5]. These codes were shown to have a 0.6 db improvement in signal to noise ratio for a given bit error rate. The use of LDPC codes for distributed source coding was suggested by Liveris et. al. [3]. They developed distributed source coding scheme for binary sources in the log domain. This paper deals with the development of distributed source coding for non-binary sources using LDPC codes. The first scheme is the implementation of distributed source coding scheme proposed in the paper [6]. The implementation in this dissertation is carried out using Slepian-Wolf coding (LDPC codes) in the probability domain described in [2]. This was necessitated as the development of distributed source coding for binary sources over a log domain could not be directly extended for non-binary sources. Two binary sources with different correlations are considered. One of the sources is assumed to be available at the decoder and is acting as the side information. The other source is compressed and sent to the decoder. The decoder decodes the compressed source by using the side information available to it from the other source.

3. Previous Work on Image Authentication

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 [7, 8]. 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 [2, 9]. 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.

In paper [4] develops authentication techniques based on robust hashing, which is inspired by cryptographic hashing. 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 [10, 11]. These compression-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 [12], zero-mean low-pass Gaussian pseudo-random projection [13, 14], block standard deviations and means [15, 16], column and row projections [17]. 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 such as in [18], keeps the null space a secret. Similar considerations apply to features calculated in a nonlinear manner. Features robust against rotation, cropping, resizing, or translation have been proposed based on the different transform, and pixel statistics.

4. Problem Statement

After studying literatures, we find that the work that does not came into the knowledge of researchers i.e. key points that are further work for our research. Image authentication based on chaos techniques of encryption, decryption and distributed source coding. In the encryption chaos method is used for key generation based on some random no, between [0 1] and decryption also, source coding we will focus on the Slepian-Wolf coding and on the basis distributed source coding. Using above proposed scheme we will try to find out that whether image is tampered or not.

5. Flow Chart of Proposed Method

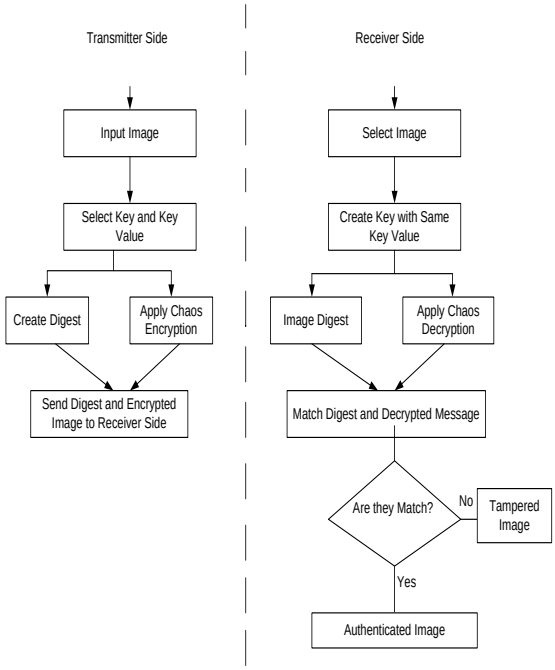

Figure 1: Flowchart

6. Proposed Methodology

Proposed method contains of two parts:

(I) Transmitter Side: It is first part of image authentication algorithm which consist of following:
  (i) Select input image from database
  (ii) Generate secret key with certain key value from interval [0 1]
  (iii) Construct image digest and and Chaos based image encryption
  (iv) Send image digest and encrypted data to receiver

(II) Transmitter Side: It is first part of image authentication algorithm which consist of following:
  (i) Select image from database which we want to check for authentication
  (ii) Create key with same key value from interval [0 1]
  (iii) Construct image digest and and Chaos based image decryption
  (iv) Send image digest and encrypted data to receiver

(v) Match these data if (a) yes: Image is Authenticated (ii) no: Tampered Image

7. Conclusion

In this chapter we describe different literatures related to the field of image authentication. We conclude that various methods given by the researchers in the area of image authentication. In this paper we will describe in brief about the encryption, decryption and hashing also binary low density parity check codes (distributed source coding) is to use for image authentication based on chaos system. An image authentication system proposed in our method is chaos based distributed source coding technique.

References

[1] W. Stallings, Cryptography and Network Security, Prentice Hall, New Jersey, 2006.
[2] B. Schneier , "Applied Cryptography," New York:Wiley, 1996.
[3] L. Xie, G.R. Arce, R.F. Graveman, "Approximate Image Message Authentication Codes", IEEE Trans. Multimedia, pp. 242-252, 2001.
[4] R.G.Gallager, "Low density parity check codes". PhD thesis, MIT, Cambridge, Mass., September 1960.
[5] Matthew. C. Davey and D.J.C. Mackay. "Low density parity check codes over GF(q)". IEEE Commum. Lett., vol. 2, pp.165-167, June 1998.
[6] Y.C. Lin, "Image Authentication Using Distributed Source Coding," Ph.D. dissertation, Stanford University, Stanford, CA, 2010.
[7] M. Johnson, K. Ramachandran, "Dither–based secure image hashing using distributed coding", Proc. IEEE Int. Conf. Image Processing. 2003, Vol. 2. pp. 751-754.
[8] M. Schneider, S. Chang, "A robust content based digital signature for image authentication", ICIP. 1996, pp. 227- 230.
[9] A.D. Liveris, Z.Xiong and C.N.Georghiades. "Compression of binary sources with side information at the decoder using LDPC codes". IEEE Commum. Lett., vol. 6, pp.440-442,2002 .
[10] Matthew. C. Davey and D.J.C. Mackay. "Low density parity check codes over GF(q)". IEEE Commum. Lett., vol. 2, pp.165-167, June 1998.
[11] J. Fridrich, "Robust bit extraction from images," in *Int. Conf. Multimedia Computing and Syst.*, Jul. 1999, vol. 2, pp. 536-540.
[12] J. Fridrich and M. Goljan, "Robust hash functions for digital watermarking," in *Int. Conf. Inf. Technol: Coding and Computing*, 2000, pp. 178-183.
[13] C. Kailasanathan and R. C. Naini, "Image authentication surviving acceptable modifications using statistical measures and k-mean segmentation," in *Workshop on Nonlinear Signal and Image Process.*, Jun. 2001.
[14] D.C. Lou and J.L. Liu, "Fault resilient and compression tolerant digital signature for image authentication," *IEEE Trans. Consumer Electronics*, vol. 46, no. 1, pp. 31-39, Feb. 2000.
[15] L. Xie, G. R. Arce, and R. F. Graveman, "Approximate image message authentication codes," *IEEE Trans. Multimedia*, vol. 3, no. 2, pp. 242-252, Jun. 2001.
[16] R.Venkatesan, S.-M.Koon, M. H. Jakubowski, and P. Moulin, "Robust image hashing," in *Proc. IEEE Int. Conf. Image Process.*, 2000, vol. 3, pp. 664-666.
[17] F. Lefebvre, J. Czyz, and B. Macq, "A robust soft hash algorithm for digital image signature," in *Int. Conf. Multimedia and Expo*, Baltimore, MD, 2003.
[18] Z. Tang, S.Wang, X. Zhang, and 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.

Dr. Manish Shrivastava completed his B.E. degree from UIT-RGPV (Formerly Government Engineering College at Bhopal) in 1993 in Computer Technology and M.Tech [Digital Communication] & Ph.D. [Optical Communication] from MANIT at Bhopal (India). He is currently a Director of PG Education & Research Center at LNCT – Bhopal. He is also Chief Editor of National Journal of Engineering Science & Management. In the past, he has done research on Optical Communications, Networking and Compilers. His current research primarily focuses on Design of Wireless Communication System to scale millions of users.

These research works have led to over 100 papers in journals (International & National) and conferences (International & National). Dr. Shrivastava has also produced a considerable volume of software. In all he has twenty years experience in the field of software development (Five years) and academics & research (Fifteen Years). Initially he had started his carrier with Software companies after completing his graduation. He left software industry in 1998 & switched to academics and has been working with reputed private engineering colleges since last fifteen years.

He has software testing & development and teaching & research experience of more than 20 years. He is Life member of CSI, IETE and Member of IEEE Photonic Society USA.