ISSN:0975-9646

Robust Watermarking Using Secret Key Encryption by Embedding Noise in JPEG Image

P.B.Ranbhare,.S.Kavitha

Abstract: we propose a new approach of designing watermarking on jpeg image using spread spectrum by creating noise on image. It is necessary to choose noise creation scheme for security .Stream cipher encryption algorithm is used in this paper to provide confidentiality for watermark. To make sure that each pixel in the image is contributed for watermarking Five stages of spread spectrum image watermarking is applied. So it is easy to maintain best watermarking on jpeg image. Noising and Embed watermark on compressed encrypted domain. Extract watermark and decompress decrypted domain then denoise algorithm used for getting real image.

Keywords-Noise in JPEG image, Secret key, Denoise, Encryption.

I .INTRODUCTION

In digital media transformation management system multimedia data distributed in different level or different way. Owner can send sensitive digital data to her customer through distributed network In this transformation if unauthorised person or third party can access data then it spoil security or change data transformation so it create major problem for owner as well as customer. So to avoid this we propose Robust Watermarking using secret key on noisy image JPEG.

In this paper we focus on compressed JPEG images encryption algorithm symmetric stream cipher used to encrypt noisy image. Noise creation and encryption both these techniques are useful for maintaining security of multimedia data. Any unauthorized user will not be able to get exact image though he has the secret key since he doesn't know the kind of noise as well as type of noise has been added to image.

There are several techniques of watermarking. For example semi-fragile watermarking where few sub-bands are encrypted and others are plain text. As only few sub-bands are used an attacker can easily decrypt the image. We are using spread spectrum for Robust Watermarking techniques. This technique provides fully compressed encrypted domain for watermarking as opposed to semi-fragile watermarking.

II .EXISTING SYSTEM

In existing system as shown in Fig.1 robust watermarking is carried out using RSA algorithm which is an asymmetric algorithm. It is useful for maintaining security but it is not useful for maintaining capacity. If payload capacity decreases it will have an effect on watermarking.

In RSA scheme encryption is performed on message size of less no of bits then it increases the size of cipher text which will lead to loss in compression efficiency. Increasing message size might help in improving compression efficiency but adversely affect payload capacity where payload capacity is a measure of watermarked signal bits per encrypted message.

By considering above two disadvantages of asymmetric schemes we need such a scheme which maintains compression efficiency as well as payload capacity. Symmetric RC4 stream cipher scheme with homomorphism property is a scheme where we get best trade off between security-compression efficiency and payload capacity.

In Existing system users use compressed encrypted domain for watermarking no doubt it maintain confidentiality and security as well as best image quality.

Architecture of Existing System

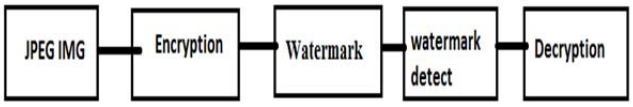

Fig.1 Architecture of Existing System

III .PROPOSED SYSTEM

Architecture of Proposed System.

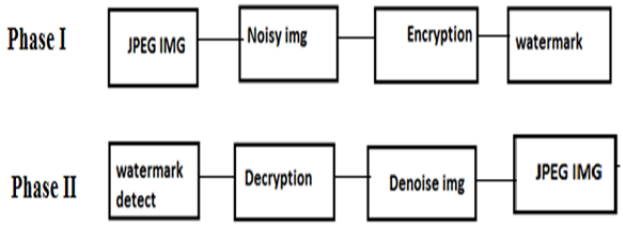

Fig.2 Architecture of Proposed System

The proposed system works on robust watermarking using secret key encryption on noisy jpeg images. In this system input image is jpeg image.jpeg images are itself compressed images. first stage noise creation. This part is different than existing system .It maintain best security of multimedia data transformation because third party might be know secret key but don't know exact noise which is created by owner. After that RC4 stream cipher encryption algorithm applies on noisy jpeg imag.RC4 stream cipher is symmetric algorithm and preferred homomorphic property. Using this algorithm getting ciphertext .RC4 is helpful for maintaining compression efficiency and payload capacity.

I .**Noise Algorithm**

R is real image and we are adding N noise on that we get noise image M.

M=R+N [I]

II .Encryption Algorithm

We are using RC4 encryption algorithm. Noise image M, k is secret key is ciphertext.

C=E(M, k) [II]

Spread spectrum works on ciphertext.This technique is best for watermarking.Watermarking apply on full compressed encrypted domain. It over first phase.on second phase detect watermark and decrypt jpeg image. Then getting noisy image so denoise jpg image and finally obtain real image.

III. Embedding Algorithm

RC4 uses for security. On encrypted data we are applying watermark W.C is encrypted data. Encrypted data with watermark means S.

S=C+W [III]

IV. Decryption Algorithm

After detecting watermark decrypt that image.

M= (D, k) [IV]

V. Denoise Algorithm

We are getting real image R.

R=M-N [V]

IV. EXPERIMENTAL RESULT

I. Noise creation

Real Image img.jpg

II. Encryption

Encrypted Img

III. SPREAD SPECTRUM

Img1.jpg

Img2.jpg

Img3.jpg

Img4.jpg

Img5.jpg

IV. ROBUST WATERMARKING:

Before watermarking.jpg

After watermarked_Image1.jpg

V .CONCLUSION:

In this paper we propose a best technique to robust watermarking using secret key encryption on noisy jpg image. We are using noisy image for encryption only purpose is to maintain best security. as we all know secret key uses both encryption as well as decryption. if hacker can hack key or key know to third party then create problematic security issue. so we are creating noise in real image. Our scheme preserves confidentiality and compression efficiency.

REFERENCE

[1] S. Hwang, K. Yoon,K. Jun, andK. Lee, "Modeling and implementation of digital rights," J. Syst. Softw., vol. 73, no. 3, pp. 533–549, 2004.

[2] A. Sachan, S. Emmanuel, A. Das, and M. S. Kankanhalli , "Privacy preservingmultiparty multilevel DRM architecture," in Proc. 6th IEEE Consumer Communications and Networking Conf., Workshop Digital Rights Management, 2009, pp. 1–5.

[3] T. Thomas, S. Emmanuel, A. Subramanyam, and M. Kankanhalli, "Joint watermarking scheme for multiparty multilevel DRM architecture," IEEE Trans. Inf. Forensics Security, vol. 4, no. 4, pp. 758–767, Dec. 2009.

[4] A. Subramanyam, S. Emmanuel, and M. Kankanhalli, "Compressedencrypted domain JPEG2000 image watermarking," in Proc. IEEE Int. Conf. Multimedia and Expo, 2010, pp. 1315–1320.

[5] H. Wu and D.Ma, "Efficient and secure encryption schemes for JPEG 2000," in Proc. IEEE Int. Conf. Acoustics, Speech and Signal Processing, 2004, vol. 5, pp. 869–872.

[6] M. Deng, T. Bianchi,A. Piva, and B. Preneel, "An efficient buyer-seller watermarking protocol based on composite signal representation," in Proc. 11th ACM Workshop Multimedia and Security, 2009, pp. 9–18.

[7] T. Bianchi, A. Piva, and M. Barni, "Composite signal representation for fast and storage-efficient processing of encrypted signals," IEEE Trans. Inf. Forensics Security, vol. 5, no. 1, pp. 180–187, Mar. 2010.

[8] S. Lian, Z. Liu, R. Zhen, and H. Wang, "Commutative watermarking and encryption for media data," Opt. Eng., vol. 45, pp. 1–3, 2006.