Digital Signature and Watermark Methods For Image Authentication using Cryptography Analysis

[1]M.Sreerama Murty, [2] D.Veeraiah, [3]A.Srinivas Rao

[1]Department of Computer Science and Engineering
Sai Spurthi Institute of Technology,Khamamm,Andhra Pradesh,India
sreerammaturi@yahoo.com
[2]Department of Computer Science and Engineering
Sai Spurthi Institute of Technology,Khamamm,Andhra Pradesh,India
veeraiahdvc@gmail.com
[3]Department of Computer Science and Engineering
Sai Spurthi Institute of Technology,Khamamm,Andhra Pradesh,India
srinivas.ada@gmail.com

Abstract

The digital signature and watermarking methods are used for image authentication. Digital signature encodes the signature in a file separate from the original image. Cryptographic algorithms have suggested several advantages over the traditional encryption algorithms such as high security, speed, reasonable computational overheads and computational power. A digital watermark and signature method for image authentication using cryptography analysis is proposed. The digital signature created for the original image and apply watermark. Images are resized before transmission in the network. After digital signature and water marking an image, apply the encryption and decryption process to an image for the authentication. The encryption is used to securely transmit data in open networks for the encryption of an image using public key and decrypt that image using private key.

Keywords: *Digital Signature, Water Marking, Cryptography, Authentication, security*

1. Introduction

1.1 Digital Signature

Digital signature is a sort of Cryptography. Cryptography means keeping communications private. Its mainly used for the converting of the information is encryption and decryption. No one can't access the information without access key.

The main process of the digital signature is similarly as the handwritten signauture.its like paper signature and it having the digital certificate using this verifies the identity.

DOI : 10.5121/sipij.2011.2214

1.2 Watermarking

Watermarking is a sub-discipline of information hiding. It is the process of embedding information into a digital signal in a way that is difficult to remove. It's providing copyright protection for intellectual method that's in digital format.

1.3 Cryptography

The cryptography is providing better mechanisms for information security. In this analysis to provide the public and private keys for recovery the original information. The ability store and transfer sensitive information. By using the different encryption methods for generating public keys, decryption using for private keys.

This method applied to digital signatures and watermarking for to provide high security in transactions.

2. Literature Survey

2. 1 "Digital Signature and Digital Watermark Scheme for Image Authentication"

This paper is investigate the combination of digital signature and watermarking is applied a host image for authentication process. The original images are having the water mark and apply the digital signature on it before the transmission in the internet.

2.2 "A New Algorithm of Encryption and Decryption of Images Using Chaotic Mapping"

The combination of chaotic theory and cryptography forms an important field of information security. In this paper implement encryption and decryption using chaotic mapping applying plain-image.

2.3"Image Encryption Using Block-Based Transformation Algorithm"

Encryption is used to securely transmit data in open networks. In this paper developed for the confidential image data from unauthorized access. The original images was divided into sub images and apply the transformation algorithms for better security.

3. Methodologies

3.1 Digital signature and Watermarking

Digital signature is a sort of Cryptography. Cryptography means keeping communications private. It deals with encryption, decryption and authentication.

3.1.1. Secret key or Symmetric Cryptography

In this processes sender and receiver massages have to know the similarly key for encryption and decryption of a message.

3.1.2 Public key or Asymmetric Cryptography

Asymmetric Cryptography involves two related keys, one of which only the the private key and the other 'public key.

3.1.3 Creation of Digital Signature

The creation of digital signature is done by getting the details from administrator, and the created signature is posted to the signature table and this is used by the certification authority. This is done by the certification authority and creates a personal identification to the person. This is carried out by using the **Digital Signature** Algorithm and the **Secure Hashing** algorithm. This digital signature provides a personalization.

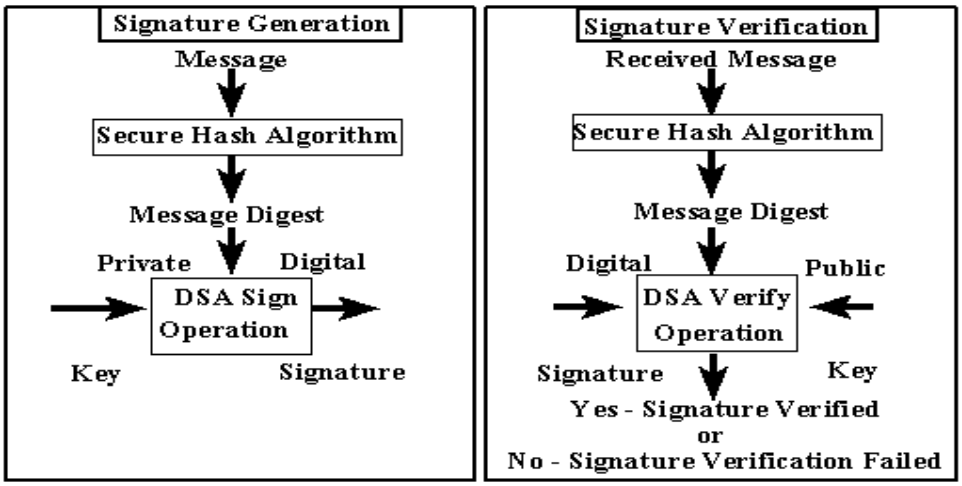

Fig 3.1.1: Using the SHA with the DSA

3.1.4 Digital Signature Algorithm

(i) GLOBAL PUBLIC-KEY COMPONENTS

1. p = a prime number, where $2^{L-1} < p < 2^{L}$ for 512 = < L = <1024 and L a multiple of 64
2. q = a prime divisor of p - 1, where $2^{159} < q < 2^{160}$
3. $g = h^{(p-1)/q} \bmod p$, where h is any integer with $1 < h < p - 1$ such that $h^{(p-1)/q} \bmod P > 1$ (g has order q mod p).

(ii) THE USER'S PRIVATE KEY:

x = a randomly or pseudo randomly generated integer with $0 < x < q$

(iii) USER'S PUBLIC KEY:

$y = g^{x} \bmod p$

(iv) USER'S PER-MESSAGE SECRET NUMBER:

k = a randomly or pseudo randomly generated integer with $0 < k < q$

3.2. Watermarking Digital Signature

Digital image watermarking schemes mainly fall into two broad categories:

3.2.1 Spatial-domain techniques

The spatial –domain techniques consist of two categories, these are

a) Least-Significant Bit (LSB): The given image contains pixels these pixels are indicated by the 8-bit sequence, the watermarks are linked two the last, bit of selected pixels of the original image. its used to hide the information and attackers could not destroy the information.

b) SSM-Modulation-Based Technique: These technique are applied in the water marking algorithms with an linked information and attached to the original image with pseudo noise signal ,its modulated by the watermark.

3.2.2 Frequency-domain techniques

The frequency-domain techniques mainly used for watermarking of the human visual system are better captured by the spectral coefficients.

The transforms are broadly categorized in two ways

(a) Discrete Cosine Transformation (DCT)

(b) Discrete Wavelet Transformation (DWT)

The following figures are explained about Discrete Cosine Transformation and Discrete Wavelet Transformation.

Fig: 3.2.2.1 One Level DWT

Original Image Water Marked Imag

Fig: 3.2.2 .2 Two Level DWT

Original Image Water Marked Image

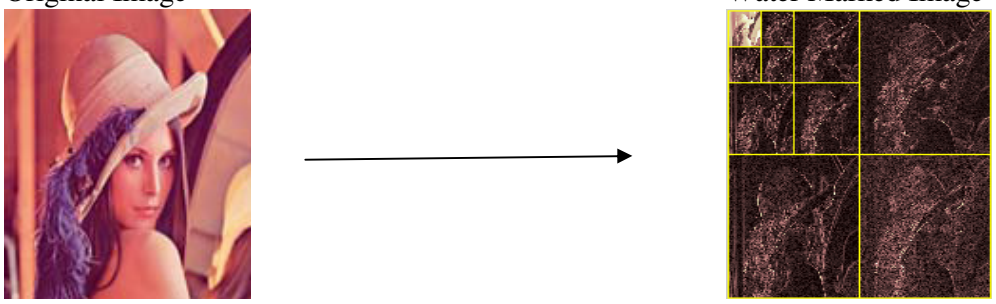

Fig: 3.2.2.4 Three Levels DWT

The above process of 2-D discrete wavelet transforms are divided into three sub images for providing the watermarking for host image.

3.2.3 Authentication using image verification

This is done by authentication verifier, initially he logins with person date of birth and passport/driving license information and extracts the signature, and these details are submitted for the verification process. By this image verification is done and can know the details.

4. Cryptography

An encryption system is also called a cipher, or a cryptosystem. The message consists of plaintext, and cipher text. Denote the plaintext and the cipher text by P and C, respectively. The encryption procedure of a cipher can be described as $C = E_{Ke}(P)$, where Ke is the encryption key and E is the encryption function. Similarly, the decryption procedure is $P = D_{Kd}(C)$, where Kd is the decryption key and D is the decryption function. For public-key ciphers, the encryption key Ke is published, and the decryption key Kd is kept private, for which no additional secret channel is needed for key transfer.

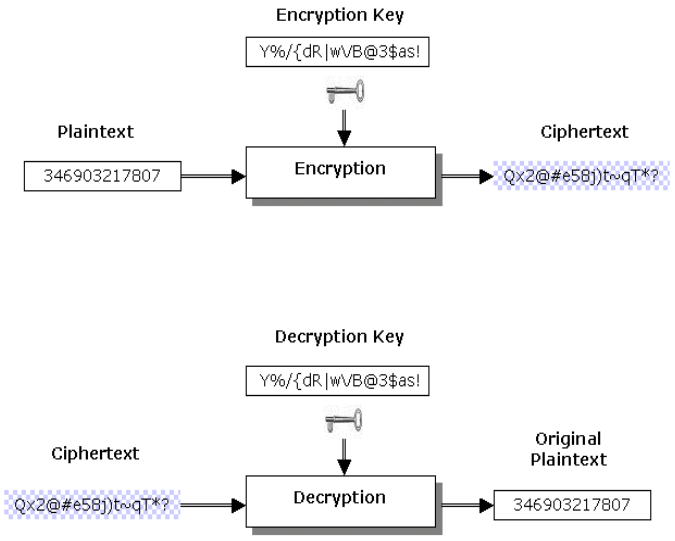

Fig: 4.1 Encryption and Decryption

5. Experimental Results

5.1 Water Marking

The given picture shows the watermarking in the bottom at left corner

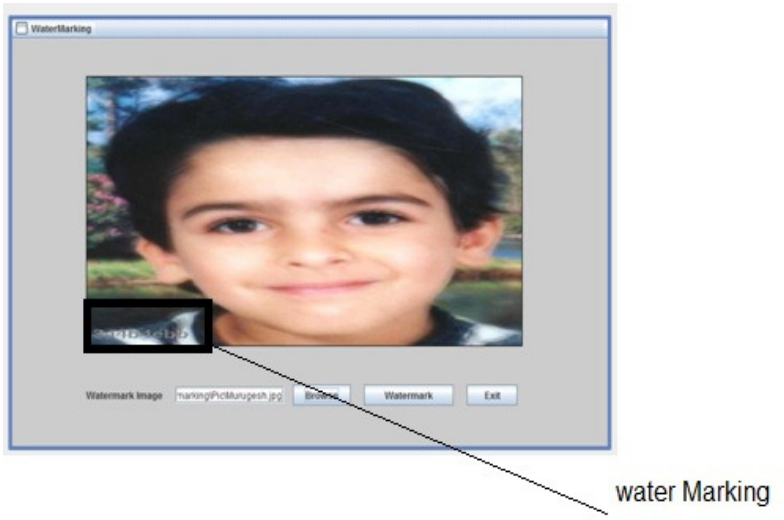

Figure 5.1.1 watermarking

5.2 Watermarking as digital signature

The given picture shows the watermarking with digital signature in the bottom at left corner

Fig 5.2.1 watermarking as digital signature

5.3 Encryption for image

The given picture shows the encryption for image

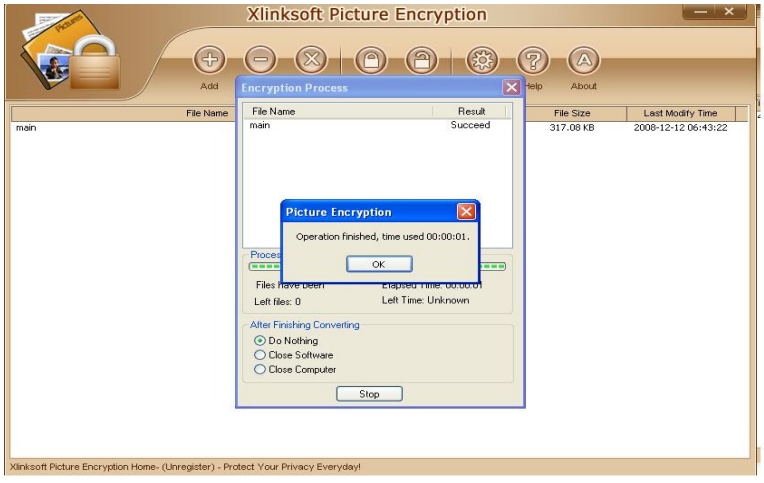

Fig: 5.3.1 Encryption

5.4 Decryption for image

The given picture shows the decryption for image

Fig: 5.4.1 Decryption

6. Conclusion

Digital signature and watermark are two techniques used for copyright protection and authentication, respectively. In this paper a digital signature and watermark methods are used cryptography analysis proposed for image security. Experiments show our scheme is robust to reasonable compression rate while preserving good image quality, and capable to authentication.

7. Future Work

Future work will be focused on more robust signature extraction method and possible ways to recover the illegally modified image without the original image.

References

[1] G.L. Friedman, "The Trustworthy Digital Camera: Restoring Credibility to the Photographic image", IEEE Transaction on Consumer Electronics, Vol. 39, No.4, 1993, pp. 905-910.

[2] J. Cox, J. Killian, F.T. Leighton, and T. Shamoon, "Secure Spread Spectrum Watermarking for Multimedia", IEEE Transactions on Image Processing, Vol.6, No. 12, 1997, pp.1673-1678.

[3] C.-Y. Lin and S.-F. Chang, "A Robust Image Authentication Method Distinguishing JPEG Compression from Malicious Manipulation", IEEE Transaction on Circuits and Systems of Video Technology, Vol. 11, No. 2, 2001, pp.153-168.

[4] J. Fridrich, "Robust Bit Extraction from Images", in Proceedings of IEEE International Conference on Multimedia Computing and Systems (ICMCS'99), Vol. 2, 1999, pp. 536-540.

[5] S.S.Maniccam, N.G. Bourbakis, "Lossless image compression and encryption using SCAN", Pattern Recognition 34 (2001), 1229-1245

[6] Chin-Chen Chang, Min-Shian Hwang, Tung-Shou Chen, "A new encription algorithm for image cryptosystems", The Journal of Systems and Software 58 (2001), 83-91

[7] Jiun-In Guo, Jui-Cheng Yen, "A new mirror-like image encryption algorithm and its VLSI architecture", Department of Electronics Engineering National Lien-Ho College of Technology and Commerce, Miaoli, Taiwan, Republic of China

[8] Jui-Cheng Yen, Jiun-In Guo, "A new chaotic image encryption algorithm",Department of Electronics Engineering National Lien-HoCollege of Technology and Commerce, Miaoli, Taiwan, Republic of China, E-mail: jcyen@mail.lctc.edu.tw

[9] Shuqun Zhang and Mohammed A. Karim, "Color image encryption using double random phase encoding", MICROWAVE AND OPTICALTECHNOLOGY LETTERS Vol. 21, No. 5, June 5 1999, 318-322

[10] Young-Chang Hou, "Visual cryptography for color images", PatternRecognition 36 (2003), www.elsevier.com/locate/patcog, 1619-1629

[11] C. Yen and J. I. Guo, "A new image encryption algorithm and its VLSI architecture." in Proceedings of IEEE workshop on signal processing systems, pp. 430–437, 1999.

[12] M. V. Droogenbroech, R. Benedett, "Techniques for a selective encryption of uncompressed and compressed images," In ACIVS'02, Ghent, Belgium. Proceedings of Advanced Concepts for Intelligent Vision Systems,2002.

[13] S. Changgui, B. Bharat, "An efficient MPEG videoencryption algorithm, " Proc e edings of the symposium on reliable distributed systems, 2002, page(s):708,711.

[14] A. Mitra, , Y V. Subba Rao, and S. R. M. Prasnna, "A new image encryption approach using combinational permutation techniques," Journal of computer Science, vol. 1, no. 1, p.127, 2006, Available:http://www.enformatika.org

[15] A. Sinha, K. Singh, "Image enc rypt ion by us ing f r a c t iona l Fo ur i e r t r ans fo rm and J igs aw t ransform in image bi t planes,"Source: optical engineering, spie-int society optical engineering, vol. 44, no. 5 , 2005, pp.15-18.

[16] M. Sonka, V. Hlavac. and R. Boyle, "Digital image processing," in: image Processing, Analysis, and Machine Vision, 1998, 2nd ed. http://www.pws.com

[17] D. Feldman, "A brief introduction to: information theory, excess entropy and computational mechanics," college of the atlantic 105 eden street, bar harbor, me 04609, 2002, http://hornacek.coa.edu/ computer society Press, 1998, pp. 381-386.

Acknowledgements

The Grateful thanks to authors for their helping and valuable comments that have developing of this paper.

Authors

M.Sreerama Murthy Recived M.Tech in Computer Science and Engineering from University College of Engineering, JNTU, Kakinada.B.Tech in Information Technology from Sai Spurthi Institute of Technology (JNTU,Hyderabad). And now presently working as Assistant Professor Sai Spurthi Institute of Technology,Khammam.His research interests includes Mobile Computing,Image Processing,DataMining ,Computer Networks and Embedded Systems.

D. Veeraiah Recived M.Tech in Computer Scince and Engineering from Anurag Engineering Coolge (JNTUH),B.Tech in Information Technology from Mother Teresa Institute of Science and Technology(JNTU,Hyderabad). And now presently working as Assoc. Professor Sai Spurthi Institute of Technology,Khammam.His research interests includes Image Processing,Computer Networks,Mobile Computing,Compiler Design.

A.Srinivas Rao Recived M.Tech in Computer Scince and Engineering from Anurag Engineering College (JNTUH),B.Tech in Information Technology from Mother Teresa Institute of Science and Technology(JNTU,Hyderabad). And now presently working as Assoc. Professor Sai Spurthi Institute of Technology,Khammam.His research interests includes Mobile Computing,Image Processing,Computer Networks,Compiler Design