ISSN:0975-9646

Digital Image Watermarking for Copyright Protection

Shankar Thawkar

Department of Information Technology

Hindustan College of Science and Technology, Mathura (UP), India

Abstract— Digital Watermarking is the process of embedding data called watermark or signature or label or tag into a multimedia object (image or audio or video) so that the watermark can be extracted for ownership verification or authentication. A visible watermark is a secondary translucent image overlaid into the primary image and appears visible to a viewer on a careful inspection. The invisible watermark is embedded in such a way that the modifications made to the pixel value is perceptually not noticed and it can be recovered only with an appropriate decoding mechanism

This paper presents an invisible image watermarking scheme for copyright protection and temper detection. The secret key encryption algorithm is used for embedding the watermark using LSB technique. The verification (the watermark extraction) process uses the same key as in encryption, and hence it can be used for copyright protection of digital media such as images, audio and video. The proposed method able to detect any modification made in the image pixels.

Keywords— **Digital Watermarking, Secret key, Encryption, Decryption, Least Significant Bit.**

I. INTRODUCTION

Digital Watermarking is the process of embedding data called watermark or signature or label or tag into a multimedia object (image or audio or video) so that the watermark can be extracted for ownership verification or authentication. This technology is becoming important due to the popularity of usages of images on web.

In general any watermarking algorithm consist of three parts [1]-

- Watermark
- The encoder
- The decoder

Watermarking techniques can be divided into various categories in various ways [1]. Watermarking techniques can be divided into four categories according to the type of document to be watermarked as follows:

- Text Watermarking
- Image Watermarking
- ·Audio Watermarking
- Video Watermarking

In other way, the digital watermarks can be divided into three different types as follows:

- Visible watermark
- Invisible-Robust watermark
- Invisible-Fragile watermark

In Visible watermarking watermark appears visible to a casual viewer on a careful inspection. The invisible-robust watermark is embedded in such a way that alternations made to the pixel value are perceptually not noticed and it can be recovered only with appropriate decoding mechanism. The invisible-fragile watermark is embedded in such a way that any manipulation or modification of the image would alter or destroy the watermark.

In this paper we used invisible watermarking. The watermark is encoded using secrete Key so that the ownership of the images can be verified using the same key. In such a system, the owner of the image inserts a watermark using a secret key K. In the watermark extraction procedure, the owner uses the same key [3] to prove ownership of the object. This technique is very useful for copyright protection, and it prevent illegal use of the multimedia content without the prior permission of owner. The proposed scheme is also capable of detecting any changes made in the pixel values of the image, this is achieved by inserting the image hash along with the encrypted message digest in the image.

The rest of the paper is organised as follows : In section 2 the proposed scheme is described in detail ; experimental results are presented in section 3 and conclusions are drawn in section 4.

II. PROPOSED SCHME

The basic idea of proposed scheme is to provide Image Integrity and Copyright protection which uses cryptographic functions such as encryption for copyright protection and hash function for Image Integrity. The working of the proposed scheme involve following steps-

A. *Watermark Embedding Algorithm*

The watermark embedding process is stated in the following algorithm-

(1) Consider an image X in which the watermark to be inserted and M be a message (owners information's).

(2) Let H (.) be a cryptographic function such as MD5or SHA-1 [2]. The Message digest is computed as-

$H(M)=(P1,P2,P3\ldots\ldots\ldots\ldots\ldots P_s)$

Where P_i denote the output bits of hash function and s is the size of the hash value that depends upon the type of the hash function such as s=128 for MD5 and s=160 bits for SHA-1.

(3) The Image hash is computed as-

(a) First the Binary image B is crated from the original image X.

(b)Then Image hash is computed using hash function such as MD5 or SHA-1

i.e. $I = H(X)$

(4**)** Then watermark W is generated by encrypting message digest P_s using symmetric key cryptosystem [3] as:

$W= E_K (P_s)$

Where E(.) is an encryption function of the symmetric key system and K is the secrete key.

(5) Embed the watermark bits and Image hash into LSB of original Image X.

(6) Finally obtain the watermark image X_w

Watermark Embedding Scheme is shown in fig.1

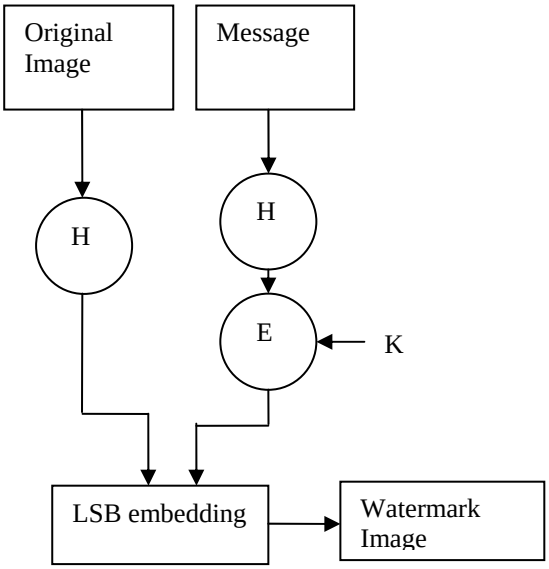

Fig. 1 Watermark Embedding

B. ***Watermark Extraction Algorithm***

The watermark extracting process is stated in the following algorithm-

(1) Extract encrypted Message digest and Image hash from LSB of watermark Image $X_{w.}$

(2) Obtain the hash value using symmetric key algorithm i.e. $P'_{s} = D_K(W')$

Where D(.) is an decryption function and K is the owners secrete key.

(3) Compare P'_s with recomputed hash value of message to prove the ownership of the image.

(4) Similarly the Image hash is recomputed and compare for temper detection.

Watermark extraction and verification process is shown in fig.2.

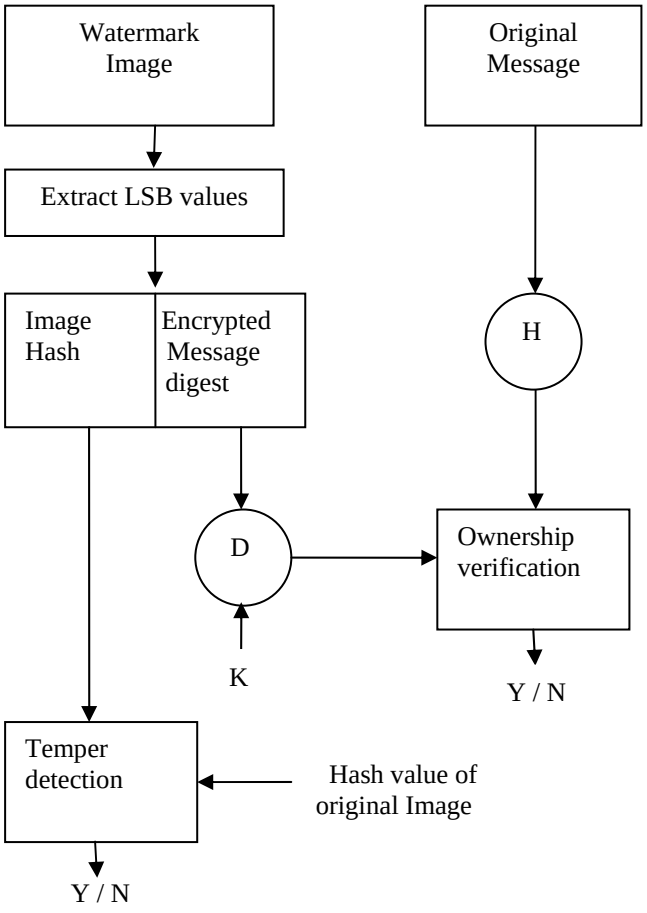

Fig. 2 Watermark extraction

III. IMPLEMENTATION AND EXPERIMENTAL RESULTS

The proposed idea is implemented using Java development kit (JDK1.6). The cryptographic primitives are implemented using JCA. JCA provide a set of classes for the implementation of cryptographic function such as encryption,

decryption and hash. The original image is being watermarked using this proposed scheme (shown in fig. 3 and 4). The proposed algorithm is tested for different payloads.

The quality of the watermark image against the embedding payload is tested in terms of three parameters: Histograms, Peak Signal to Noise Ratio (PSNR) and Mean Square Error (MSE). Larger is the PSNR better is the quality of image and smaller is the MSE better is quality of image. The MSE is obtain using following formula-

$$MSE = \left(\frac{1}{X * Y}\right) \sum_{x=1}^{X} \sum_{y=1}^{Y} [I(x,y) - I'(x,y)]^2$$

Where X, Y are the dimensions of the original and watermarked image respectively.

The PSNR values are obtain using following formula-

$$PSNR = 10 \log_{10} \frac{MAX^2}{MSE}$$

Where MSE is the mean square error and MAX is maximum pixel value of image..In general watermark images with PSNR value 30dB are acceptable.

If we look the histograms of watermark images with payload 2kb, 5kb, 10kb and 14kb (as shown in fig. 5 to 9) and histogram of original image, we find that both are almost same. The experimental results with respect to Peak Signal to Noise Ratio and Mean Square Error are shown in table1. It is clear from the results that the PSNR value is greater than the acceptable values i.e. 30dB and MSE values are also in acceptable range.

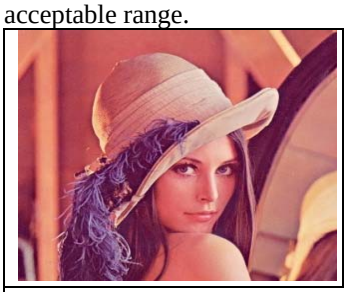

Fig.3: Original Image

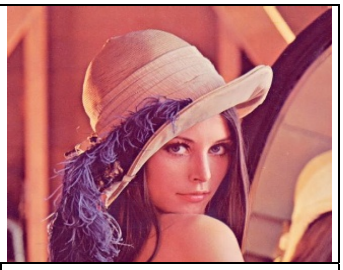

Fig.4: Watermark Image

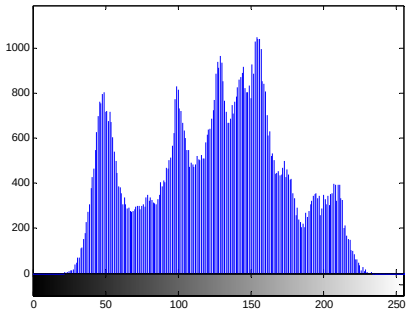

Fig. 5 : Histogram of Original Image

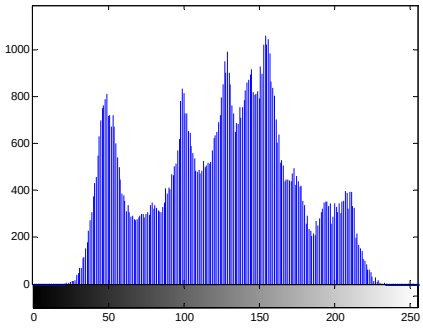

Fig.5 : Histogram of Watermark Image with 2kb of payload

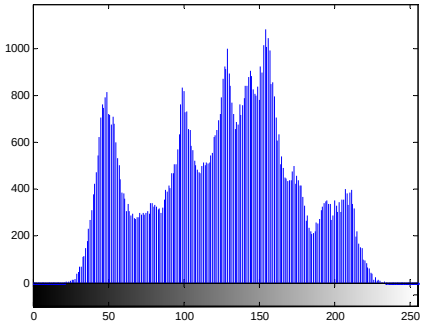

Fig.6: Histogram of Watermark Image with 5kb of payload

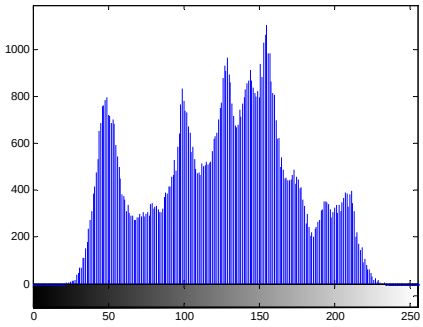

Fig.7 : Histogram of Watermark Image with 10kb of payload

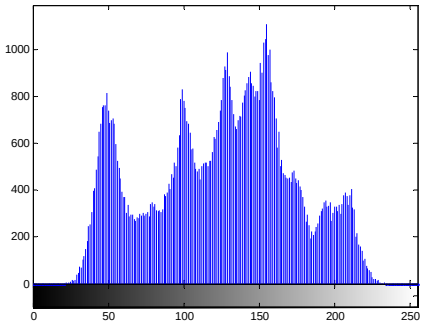

Fig.5 : Histogram of Watermarkl Image with 14kb of payload

Embedding capacity in KB	Mean Square Error(MSE)	Peak Signal to Noise Ratio(PSNR)
2kb	2.85e-002	63.6 dB
5kb	6.92e-002	59.7dB
10kb	1.33e-001	56.9dB
14kb	1.85e-001	55.5 dB

Table 1 : PSNR and MSE values

IV. CONCLUSION

The Digital Watermarking technology is becoming important due to the popularity of usages of images on web. In invisible watermarking technique the watermark is embedded in such a way that the modifications made to the pixel value is perceptually not noticed and it can be recovered only with an appropriate decoding mechanism. This paper presented invisible watermarking scheme for copyright protection of images. The watermark is generated by encrypting the message digest using symmetric key algorithm. Then the generated watermark along with the image hash is embedded into LSB of original image.

The verification process uses the same key as in encryption and hence it can be used for the copyright protection of the images. During the verification process the received hash is compared with the recomputed hash to prove the ownership. Similarly the image hash is compared with the recomputed image hash for detecting any modifications made in the image pixels. This technique provides high capacity and minimum computations. Further we can improve this method by embedding the watermark into DCT coefficients.

REFERENCES

1] Mohanty, Ramakrishnan "A Dual Watermarking Technique for Images "http://citeseer.ist.psu.edu/mohanty99dual.html

[2] R. L. Rivest, "The MD5 message digest algorithm." Internet RFC 1321, April 1992.

[3] R.L. Rivest, A. Shamir, and L. Adleman, "A method for obtaining digital signatures and public key cryptosystems," Communications of the ACM, vol. 21, pp. 120{126, February 1978.

[4] W. Diffie and M. E. Hellman, "New directions in cryptography," IEEE Transactions on Information Theory, vol. 67, pp. 644{654, November 1976.

[5] I.J.Cox et. al., "Secure spread Spectrum Watermarking of Images, Audio and Video", Proc IEEE 1996 International Conf on Image Processing, 1996, Vol 3, pp 243-246

[6] Kefa Rabah "*Steganography-The Art of hiding* **"**http://www.ansinet.org/fulltext/itj/itj33245-69.pdf

[7] Dr. Kenny Hunt "*A Java Framework for Experimentation with Steganography*" http://portal.acm.org

[8] Chen, T.H. Hong, Wang S.H. " A Robust Wavelet based watermarking scheme using Quantization and Human visual system", Pakistan journal of Information and Technology, 2(3):213-230,2003 :ISSN 1682-6027.

[9] Katzenbeisser, S. and Petitcolas, F.A.P., (2000). Information hiding techniques for steganography and digital watermarking. Artech House Publishers.

[10] Nagra, J., Thomborson, C. and Collberg, C. (2002), a functional taxonomy for software watermarking, in M. Oudshoorn, ed., `Proc. 25th Australasian Computer Science Conference 2002', ACS, pp.177-186.

[11] Bhatnagar, G. and Raman, B. (2008), A new robust reference watermarking scheme based on DWT-SVD, Elsevier B.V. All rights reserved.

[12] Luo, H, Chu, S. H. and Lu, Z. M. (2008), Self Embedding Watermarking Using Half-toning Technique, Circuits Syst Signal Process (2008) 27: 155–170

[13] Yang, W. C., Wen, C. Y. and Chen, C. H., (2008), Applying Public-Key Watermarking Techniques in Forensic Imaging to Preserve the Authenticity of the Evidence. Springer-Verlag Berlin Heidelberg 2008.