Copyright Protection of Gray Scale Images by Watermarking Technique Using (N, N) Secret Sharing Scheme

Sushma Yalamanchili
Professor & Head, Department of CSE,V.R.Siddhartha Engineering College, Vijayawada.
Email: sushma_yalamanchili@yahoo.co.in

M.Kameswara Rao
Lecturer, P.B.Siddhartha College, P.G.Centre, Vijayawada.
Email: kamesh.manchiraju@gmail.com

***Abstract*— Since the rise of the Internet one of the most important factors of information technology and communication has been the security of information. A special case of information hiding is digital watermarking. Digital watermarking is the process of embedding information into digital multimedia content such that the information (the watermark) can later be extracted or detected for a variety of purposes including copy prevention and control. Among numerous cryptographic solutions proposed in the past few years, secret sharing schemes have been found sufficiently secure to facilitate distributed trust and shared control in various communication applications.**

In this paper, a new image watermarking algorithm is developed using (n,n) secret sharing scheme for copyright protection. The proposed method embeds the copyright image into original image and is to be shared among n participants. Then the copyright image could be recovered using simple XOR operations without any loss.

Experimental simulations are provided using MATLAB 7.1 to demonstrate the efficient performance of the developed technique in terms of reliability of watermark embedding and extraction. The scheme contains three phases: the copyright image embedding phase, embedded image secret sharing phase, copyright image extraction phase. The experimental results show that the proposed scheme can resist several attacks such as JPEG compression, resize and noise addition.

***Index Terms*— copyright protection, secret sharing, watermarking, steganography.**

I. INTRODUCTION

On the Internet today it is possible to duplicate digital information a million-fold and distribute it over the entire world in seconds. These issues worry creators of intellectual property to the point that they do not even consider to publish on the Internet. To solve the problem of publishing digital images, researchers have come up with digital image watermarking [1]. Digital watermarking is a method of embedding identifying information in an image, in such a manner that it cannot easily be removed .An application of watermarking is copyright control, in which an image owner seeks to prevent illegal copying of the image. A digital watermark is a code that is embedded inside an image. It acts as a digital signature, giving the image a sense of ownership or authenticity. Digital watermarking of an image has also been proposed for the prevention of copying of an image by unauthorized persons.

To a computer, an image is a collection of numbers that constitute different light intensities in different areas of the image [4]. This numeric representation forms a grid and the individual points are referred to as pixels. Most images on the Internet consists of a rectangular map of the image's pixels (represented as bits) where each pixel is located and its colour [5]. Digital colour images are typically stored in 24-bit files and use the RGB colour model, also known as true colour [6]. All colour variations for the pixels of a 24-bit image are derived from three primary colours: red, green and blue, and each primary colour is represented by 8 bits [4].

Secret sharing [2] refers to method for distributing a secret amongst a group of participants, each of which is allocated a share of the secret. The secret can be reconstructed only when the shares are combined together; individual shares are of no use on their own. Secret image sharing is a technique for protecting images that involves the dispersion of the secret image into many shadow images. This endows the method with a higher tolerance against data corruption or loss than other image-protection mechanisms, such as encryption or steganography.

A secret kept in a single information-carrier could be easily lost or damaged. Secret sharing (SS) schemes, called (n, n) schemes, have been proposed since late 1970s. To encode the secret into n pieces ("shadows" or "shares") that the pieces can be distributed to n participants at different locations. The secret can only be reconstructed from n pieces [2].

II. PROPOSED METHOD

Consider an image A of NR ×NC. Each pixel of A can take any one of c different colors or gray-levels. Image A is represented by an integer matrix A:
A = [aij]NR×NC , where i = 1, 2, . . . , NR,
j = 1, 2, . . . , Nc, and aij € {0, 1, . . . , c − 1}.We have c =2 for a binary image, and c =256 for a grayscale image

doi:10.4304/jetwi.2.2.101-105

with one byte per pixel. In a color image with one byte per pixel, the pixel value can be an index to a color table, thus c = 256. In a color image using an RGB model, each pixel has three integers: R (red), G (green) and B (blue). If each R, G or B takes value between 0 and 255, we have c = 256 [2]. The proposed method includes the following steps

Step 1: Consider two images - Original image and the copyright image - represented by integer matrices.

Step 2: Decide a value called weight_value between 0 and 1.For invisible watermark weight_value must be near to 0.

Watermark Embedding :

Step 3: Embed the copyright image inside the original image as follows

Embedded image=original image + (resized copyright image * weight_value).

(N,N) Secret Sharing Scheme For the embedded Image :

The output of a (n,n) scheme for embedded images is a set of n distinct NR×NC matrices A1, . . . , An, called shares or shadow images. Each share image has the same number of pixels as the original image A, but every pixel in a share may contain m sub pixels. A can be reconstructed from the set {Ai1, . . . , Aik } and even complete knowledge of k − 1 shares reveals no information about A. The first condition above is called precision, and the second condition is called security [2].

Step 4: Encode the embedded image into n shadows or secrets as follows and

generate n − 1 random matrices B1, . . . , Bn−1,

compute the shadow images as below:

$A1 = B1$,

$A2 = B1 \oplus B2$,

. . . . . .

$An-1 = Bn-2 \oplus Bn-1$,

$An = Bn-1 \oplus A$.

In the generation of the shadow images and in the reconstruction of the secret, Boolean operation XOR (“$\oplus$”) is used. For easy lookup, the truth-table of XOR for binary scalar inputs is given below.

	a=0	a=1
b=0	0	1
b=1	1	0

a $\oplus$ b

For example, when a =125 and b =18, the XOR between these two integers is

$a \oplus b = (125)_{10} \oplus (18)_{10} = (01111101)_2 \oplus (00010010)_2$

$= (01101111)_2 = (111)_{10}$.

Step 5 : Reveal the embedded image from the n shadow images as below:

$A' = A1 \oplus A2 \oplus \cdots \oplus An$.

Because the “$\oplus$” operation is associative and $Bi \oplus Bi$ is a zero matrix for any i, we have

$A = B1 \oplus (B1 \oplus B2) \oplus \cdots \oplus (Bn-2 \oplus Bn-1) \oplus (Bn-1 \oplus A)$

$= (B1 \oplus B1) \oplus \cdots \oplus (Bn-1 \oplus Bn-1) \oplus A = A.$

To demonstrate the computation steps in the revealing process, we give a trivial example for n = 3 and a single-pixel secret image A.

Given: $A = (231)_{10} = (11100111)_2$

Generate: $B1 = (46)_{10} = (00101110)_2$ and

$B2 = (188)_{10} = (10111100)_2$

Compute: $A1 = B1 = (46)_{10} = (00101110)_2$,

$A2 = B1 \oplus B2 = (10010010)_2$, and

$A3 = B2 \oplus A = (01011011)_2$

Reconstruct: $A1 \oplus A2 \oplus A3 = (11100111)_2 = (231)_{10}$.

An example for the proposed (n, n) scheme using a 3 × 3 secret image A is given below:

$$A = \begin{pmatrix} 209 & 214 & 225 \\ 233 & 227 & 228 \\ 222 & 221 & 226 \end{pmatrix}$$

$$B1 = \begin{pmatrix} 136 & 169 & 28 \\ 254 & 128 & 245 \\ 96 & 108 & 49 \end{pmatrix}$$

$$B2 = \begin{pmatrix} 8 & 94 & 65 \\ 218 & 137 & 228 \\ 46 & 71 & 222 \end{pmatrix}$$

,

$$A1 = B1 = \begin{pmatrix} 136 & 169 & 28 \\ 254 & 128 & 245 \\ 96 & 108 & 49 \end{pmatrix}$$

,

$$A2 = B1 \oplus B2 = \begin{pmatrix} 128 & 247 & 93 \\ 36 & 9 & 17 \\ 78 & 43 & 239 \end{pmatrix}$$

,

$$A3 = B2 \oplus A = \begin{pmatrix} 217 & 136 & 160 \\ 51 & 106 & 0 \\ 240 & 154 & 60 \end{pmatrix}$$

, and

$$A1 \oplus A2 \oplus A3 = \begin{pmatrix} 209 & 214 & 225 \\ 233 & 227 & 228 \\ 222 & 221 & 226 \end{pmatrix} = A$$

Watermark Extraction :

Step 6 : Extract the copyright image inside the embedded image as follows

copyright image =(Original image – embedded image)/weight_value.

III. Experimental Results On Gray Scale Images

The simulations were conducted on Intel machine with 2.4 GHz processor and 512 MB of RAM. MATLAB 7.1 was used for implementation of proposed scheme and

image processing operations respectively. Applying the proposed method on tree path image as original image and college logo image as copyright image under (n,n) scheme with $n = 3$.

Figure 1 (a) Original image

Figure 1 (b) Copyright Image

Figure 1(c) Embedded Image

Fig. 1 shows the original image in part (a), copyright image in part (b) and the embedded image (Original image + Copyright Image) in part(c) .

(n,n) Secret sharing scheme

A (n,n) secret sharing scheme encodes a secret image into n share images, which demonstrate randomly noisy patterns and hide the information about the secret image, are distributed to n recipients. The secret image can easily be decrypted by XOR operation of the n share images in an arbitrary order without complicated arithmetic.

Figure 2(a)Embedded Image

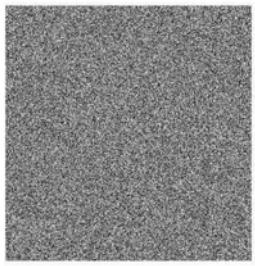

Figure 2(b)shadow image1

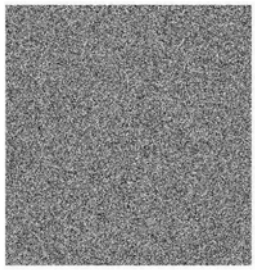

Figure 2(c) Shadow image 2

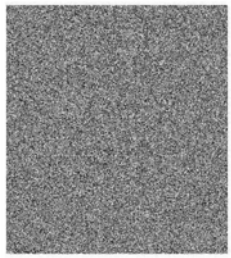

Figure 2(d) Shadow image 3

Figure 2 (e) Reconstructed Embedded image using 3 shadows

Fig. 2(a) shows the embedded image in part (a), shadow images in part(b-d)and the reconstructed embedded image using the 3 shadow images in part(e).

Strength of the (n,n) Scheme

The reconstruction phase of our algorithm computes n shadow images using XOR operation. the proposed (n, n) scheme reconstructs the secret image exactly, and it satisfies the security condition. That is, when fewer than n shadows are used, the original secret image A will not be revealed.

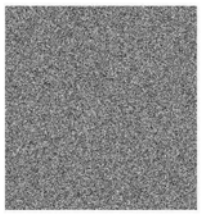

Figure 3(a)Reconstructed image using shadow image 1 and shadow image 2

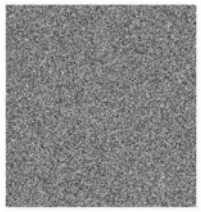

Figure 3(b)Reconstructed image using shadow image 1 and shadow image 3

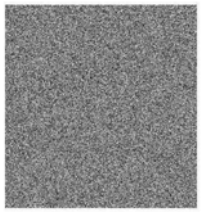

Figure 3(c)Reconstructed image using shadow image 2 and shadow image 3

Fig 3 shows the Reconstructed image using shadow images 2(a) and 2(b) in part(a) Reconstructed image using shadow images 2(a) and 2(c) in part(b) and Reconstructed image using shadow images 2(a) and 2(c) in part(c).

Watermark extraction process

Figure 4(a) Embedded image

Figure 4(b)Extracted copyright image

Fig 4 shows the embedded image in part (a) and the extracted copyright image in part (b)

Attacks on the Proposed Method

Our experiments show that for group of attacks like JPEG compression, resizing, adding noise the proposed method can be able to extract the copyright image with less loss in the quality.

Figure 5(a) Resized Embedded Image

Figure 5(b)Extracted Copyright image when the embedded image is resized

Fig 5 shows the Resized embedded image in part(a) and the extracted copyright image when the embedded image is resized in part(b)

Figure 6(a) Compressed Embedded Image

Figure 6(b)Extracted Copyright image when the embedded image is Compressed

Fig 6 shows the compressed embedded image in part (a) and the extracted copyright image when the embedded image is compressed in part (b)

Figure 7(a) Embedded Image with added noise

Figure 7(b)Extracted Copyright image when the embedded image is added with noise

Fig 7 shows the embedded image with added noise in part (a) and the extracted copyright image when the embedded image is added with noise in part (b)

IV. PSNR MEASUREMENT

One commonly used measure to evaluate the imperceptibility of the watermarked image is the peak signal to noise ratio (PSNR) which is given by

PSNR = 10 * log10((255)^2 / mean_square_error)

Where

OriginalImage_x_size = size(OriginalImage, 2);
OriginalImage_y_size = size(OriginalImage, 1);
CopyrightImage_x_size = size(CopyrightImage, 2);
CopyrightImage_y_size = size(CopyrightImage, 1);
mean_square_error = sum(sum(sum((CopyrightImage – Extracted CopyrightImage).^2))) / double(CopyrightImage_x_size * CopyrightImage_y_size * 3);

TABLE I.
PSNR VALUES

Type of Operation on Image	PSNR
Original Embedded Image	32.6737
After resizing embedded Image	29.0508
After compressing the Embedded image to a .jpg	28.4083
After adding random noise to the Embedded image	33.4338

Table I illustrates PSNR values between the Original Copyright Image and the Extracted Copyright Image taken from various operations

V. CONCLUSIONS

We have demonstrated a new watermarking technique that uses (n,n) secret sharing scheme to embed a copyright image into original image . This technique works well with images of all sizes. This technique provides two layers of security. In the first step, a copyright image is embedded into original image for copyright protection. Also, the embedded image is shared among n participants where all the n shares must be used to reconstruct the embedded image. This makes the system more secure. The method can with stand attacks like JPEG compression, resize and adding noise with less loss in quality of the image. Further this work can be extended by calculating the hash value of the image and encrypt the hash value using either symmetric key or public key and embed the hash value inside the image so that at the receivers end the authentication and integrity of the image can be verified by recalculating the hash and verifying it. Similarly digital signatures can be generated for images and can be verified. Also (k,n) threshold secret sharing schemes can be implemented for much security.

VI. REFERENCES

[1] Adrian Perrig Andrew Willmott, ”Digital Image Watermarking in the Real World" Extended Abstract, March 9, 1998.

[2] DaoshunWang, Lei Zhang, Ning Ma, Xiaobo Li,“Two secret sharing schemes based on Boolean operations”, Science Direct –Pattern Recognition 2007.

[3] A. Shamir, “How to share a secret”, Commun. Assoc. Comput. Mach. 22 (11) (1979) 612–613.

[4]Johnson, N.F. & Jajodia, S., “Exploring Steganography: Seeing the Unseen”, Computer Journal, February 1998 .

[5]“Reference guide: Graphics Technical Options and Decisions”, http://www.devx.com/projectcool/Article/1997

[6] Owens, M., “A discussion of covert channels and steganography”, SANS Institute, 2002.