International journal of Advances in Electronics Engineering
Vol:1 Issue:1 ISSN 2278 - 215X

Digital Watermarking with Visual Cryptography in Spatial Domain

Roop Singh
Deptt. Of Electronics
MITS
Gwalior (M.P), India
E-mail: ***roop_solanki@hotmail.com***

Rekha Gupta
Deptt. Of Electronics
MITS
Gwalior (M.P), India
E-mail: rekha652003@yahoo.com

***Abstract*-In this paper, concept of visual cryptography is extended to digital watermarking scheme based on least significant bit (LSB) algorithm. An image which has to be transmitted (watermark) is split into two sheet-images using visual secret sharing algorithm. Then, one sheet -image are embedded into the host images before transmission and second sheet –image is held by the owner At the receiving end, user extracts the sheet -images from the watermarked image and stacks the two sheet- images directly without any leakage of information about the original image. Experimental results show that by using visual cryptography, a significant improvement in peak signal to noise ratio and normalized cross correlation values can be obtained.**

Keyword- Digital image Watermarking, Visual Cryptography, spatial domain, Least Significant Bit (LSB).

I. Introduction

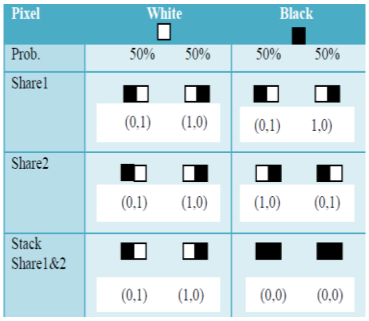
In recent years, with the popularization of Internet, information security has become a challenging topic for researchers [1]. With the continued rise of sharing over Internet, it is getting increasingly more difficult to prevent copyright infringement of digital media. [2]. Digital watermarking refers to techniques used to protect digital data by imperceptibly embedding information (watermark) into the original data in such a way that it always remains present. For the watermarking method to be effective, it should be imperceptible and robust to various image processing attacks. Current digital image watermarking techniques can be grouped in to two major classes: spatial domain and frequency domain techniques. [3], [4]. in spatial domain technique , the watermark embedding is achieved by directly modifying the pixel values of the host image. The most commonly used method in the spatial domain technique is the least significant bit (LSB). [5], [6]. Spatial domain methods are less complex as no transform is used, but are not robust against attacks. In this paper, digital watermarking technique is proposed, to embed binary watermark into digital image based on the concept of visual cryptography (VC). Visual Cryptography (VC) was first introduced by Moni Naor and Adi Shamir at Euro crypt in 1994 [7]. Also known as visual secret sharing (VSS) technique which allows visual information (pictures, text, etc.) to be encrypted (creating sheets) in such a way that the decryption can be performed by human visual system (HSV) without computer. Visual cryptographic techniques can solve the problem of unauthorized access to the information. However, it is unable to prevent an authorized user from illegally replicating the decrypted content [8], [9].

II. Steps of (2,2) visual cryptography

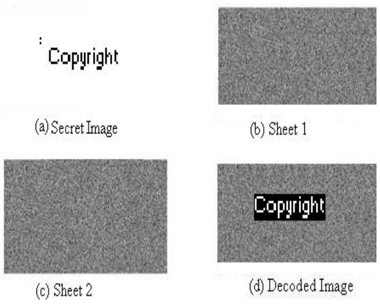
- To encode a black- and –white secret image (Binary or watermark image) using (2, 2) VC scheme, the secret image is divided into two sheets.
- Anyone who holds only one sheet will not be able to reveal any information about the secret image.
- Whereas one sheet reveals no information about the original image.
- A secret image is encrypted into two different sheet-images that reveal the secret image when they are overlaid.
- To decode the secret image, two sheets are stacked together.
- Separately, these two sheets are random noise.

Encoding of one pixel in a (2, 2) VC is illustrated in table 1. A white pixel is shared into two identical blocks of sub-pixels. A black pixel is shared into two complementary blocks of sub-pixels. White creating the sheet-images, if the given pixel p in the original image is white, and then the encoder randomly chooses one of the first two columns of table 1. If the given pixel p is black, then the encoder randomly chooses one of the last columns of table 1. Each block has half white and half black sub-pixels, independent of whether the corresponding pixel in the secret image is black or white. All the pixels in the original image are encrypted similarly using independent random selection of columns. The result of basic (2, 2) VC scheme are shown in fig.1. When the two sheet-images are stacked together, as in fig.1.(d) , the black pixels in the original image remain black and the white pixels become gray. Although some contrast loss occurs, the decoded image can be clear clearly identified [7], [9].

Table I. Pixel expansion in a **(2, 2) VSS** scheme



Pixel	White □		Black ■	
Prob.	50%	50%	50%	50%
Share1	■□ (0,1)	□■ (1,0)	■□ (0,1)	□■ 1,0)
Share2	■□ (0,1)	□■ (1,0)	□■ (1,0)	■□ (0,1)
Stack Share1&2	■□ (0,1)	□■ (1,0)	■■ (0,0)	■■ (0,0)



(a) Secret Image

(b) Sheet 1

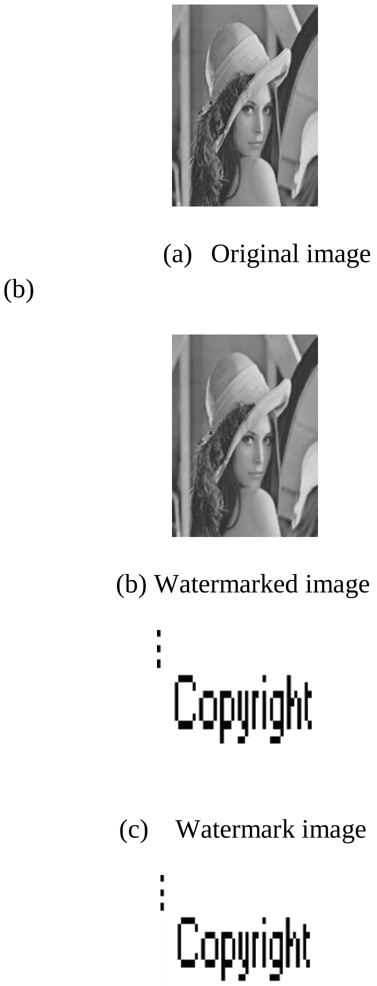
(c) Sheet 2

(d) Decoded Image

Figure 1. Working of (2, 2) visual cryptography

III. WATERMARK EMBEDDING AND EXTRACTION BASED ON LSB

Suppose that the host image Lena is of size 512 x 512 grey level images and another watermark image Copyright is of size 256 x256 Binary image. In spatial domain, the pixel values of original image are modified according to the pixel values of watermark image. To extract the watermark reverse operation of watermark embedding is performed.



(a) Original image

(b)

(b) Watermarked image

(c) Watermark image

(c) Extracted watermark image

Figure 2. Watermarking in spatial domain

IV. Proposed watermarking scheme

In this paper a new visual cryptography scheme is proposed which increase the contrast of the stacked sheet. Then LSB technique is used to embed the generated sheets into host image to improve the peak signal to noise ratio (PSNR) values and normalized cross correlation (NC) values.

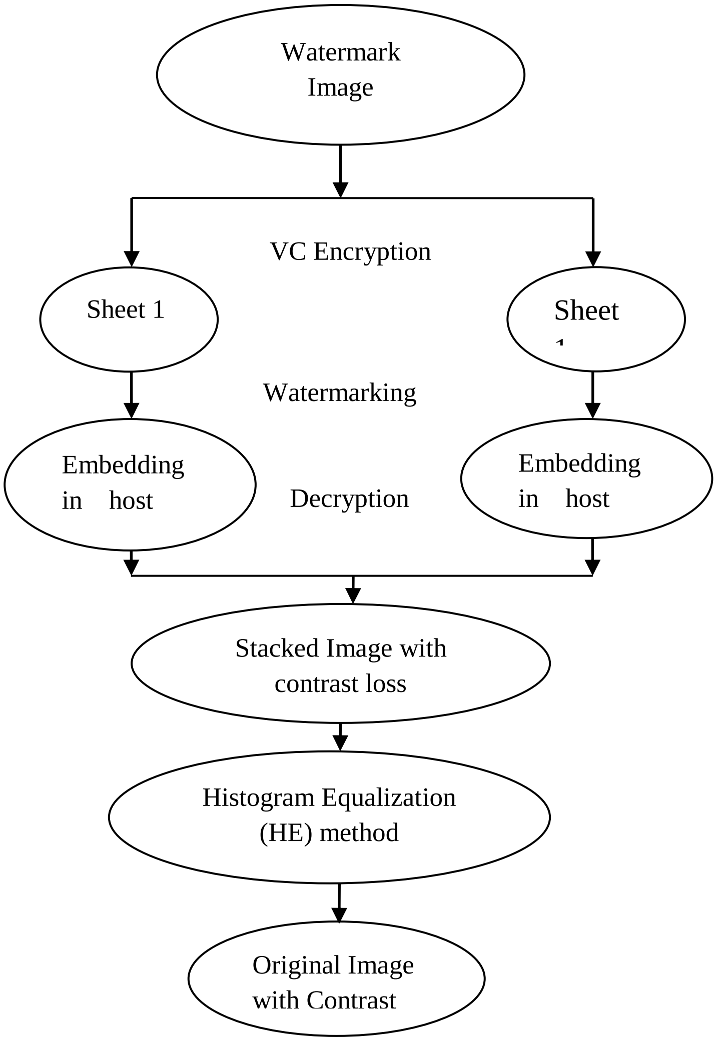


Figure 3. Flow graph of proposed scheme

V. Merits and demerits of proposed scheme

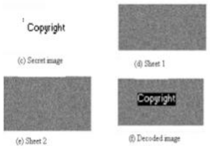
Proposed scheme provides a high level security for copyright protection by improving both the PSNR values and NC values. This scheme also has drawbacks as the original image is completely contrasted.

VI. Watermarking with visual cryptography

In this paper, Original image Lena is of size 512 x 512 grey level images and another watermark image Copyright is of size 256 x256 Binary image is used for test the proposed scheme.

(a) Original image

(b)Watermarked image



(c) Secret image

(d) Sheet 1

(e) Sheet 2

(f) Decoded image

Figure 4. Simulation results of proposed scheme

VII. Simulation results

In this section, some results regarding the PSNR and NC are presented to evaluate the proposed watermarking scheme.

(a) Peak Signal To Noise Ratio (PSNR)

Peak signal to noise ratio are used to measure the quality of the watermarked image [10]. The PSNR in decibels (dB) is given by

$$PSNR = 20\ log_{10}\left(\frac{255}{\sqrt{MSE}}\right) \qquad (1)$$

Where,

$$MSE = \frac{\sum[f(x,y) - F(x,y)]^2}{N^2} \qquad (2)$$

f(x, y) denotes the original image and F(x, y) denotes the watermarked image. $N\ X\ N$ is the image size.

(b) Normalized Cross Correlation (NC)

Normalized cross correlation is used to measure the similarity between the original watermark and extracted watermark. [11], [12]. NC is given as

$$\rho(\mathrm{w}, \hat{\mathrm{w}}) = \frac{\sum_{i=1}^{N} \mathrm{w}_i \hat{\mathrm{w}}_i}{\sqrt{\sum_{i=1}^{N} \mathrm{w}_i{}^2}\sqrt{\sum_{i=1}^{N} \hat{\mathrm{w}}_i{}^2}} \qquad (3)$$

Where, N is the number of pixels in watermark, w and ŵ are original and extracted watermarks respectively.

VIII. Comparison of both watermarking (LSB without cryptography and with cryptography) scheme

Image & size	*MSE*		*PSNR*	
	LSB	*VC*	*LSB*	*VC*
Lena(512x512)	0.44	0.02	51.67	63.95
Cameraman(256x256)	0.45	0.02	51.56	63.91

IX. Conclusion

It has been found that simple VC suffers from contrast loss. Histogram Equalization is applied to the VC algorithm which increases contrast of an image. Proposed VC watermarking provides a gain of 20% gain in PSNR as compared to the LSB watermarking scheme.

X. Acknowledgement

The author would like to acknowledge the contribution of Dr. Rekha Gupta (Guide and mentor) for her tireless efforts during this research work. The author is greatly indebted to her. Also the author remembers his colleagues for their kind help.

References

[1] Pan Shengmin1, Zhang Chunhong, "Digital Watermarking Based on Discrete Cosine Transformation," International Forum on Information Technology and Applications, 2010.

[2] Heather Wood,"Invisible digital watermarking in the spatial and dct domains for color images."

[3] V. Venkata Rama Prasad and Rama Kurupati, "Secure Image Watermarking in Frequency Domain using Arnold Scrambling and Filtering," ISSN 0973-6107 Vol. 3. Number 2, pp. 236–244, 2010.

[4] Chun-Hsien Chou and Kuo-Cheng Liu, "A Perceptually Tuned Watermarking Scheme for Color Images," VOL. 19, NO. 11, Novemember 2010.

[5] Wang Na, Wang Yunjin, Li Xia, "A Novel robust watermarking algorithm based on DWT and DCT," 2009.

[6] X. Wu and Z.-H. Guan, "A novel digital watermark algorithm based on chaotic maps," vol. 365, pp. 403-406, 2007.

[7] B Surekha, Dr. GN Swamy, Dr. K Srinivasa Rao, "A Multiple Watermarking Technique for Images based on Visual Cryptography", Vol. 1 ,No. 11, 2010

[8] Ching-Sheng Hsu and Shu-Fen Tu, "Digital Watermarking Scheme with Visual Cryptography", vol.1, 19-21 March, 2008.

[9] Debasish Jena, Sanjay Kumar Jena," A novel Visual Cryptography Scheme," 978-0-7695-3516-6/08 $25.00 © 2008 IEEE.

[10] Akram M. Zeki and Azizah A. Manaf, "A Novel Digital Watermarking Technique based on ISB(Intermediate Significant Bit)", International Journal of Information and Communication Engineering 5:7 2009.

[11] Mei Jiansheng, Li Sukang1 and Tan Xiaomei, "A digital watermarking based on DWT and DCT", *pp. 104-107, May 22-24, 2009.*

[12] Mahasweta J.Joshi, Prof. Zankhana H.Shah, Keyur N.Brahmbhatt, "Watermarking in DCT-DWT domain", Vol. 2 (2), 2011