Halftone Image Watermarking based on Visual Cryptography

Jaishri Chourasia
MITS,Lakshmangarh

M. B. Potdar
Project Director
BISAG, Gandhinagar

Abdul Jhummarwala
Project Scientist
BISAG, Gandhinagar

Keyur Parmar
SVNIT, Surat

ABSTRACT
In this paper we have proposed digital watermarking scheme for halftone images based on visual cryptography scheme. The scheme does not embed the watermark directly on the halftone image instead watermark will be divided into the parts called as shares. The scheme not only protects the watermark but also provides an effective copyright protection scheme. At the time of watermark embedding verification share is generated and at the time of watermark extraction master share is generated using (2, 2) visual cryptography scheme. Verification share and master share are used to extract the watermark pattern. The experimental results show that the scheme is robust and transparent against various watermarking attack.

General Terms
Cryptography, digital image processing.

Keywords
Digital watermarking, visual cryptography scheme, error diffusion, halftone.

1. INTRODUCTION
Digital watermarking is the process of embedding information, for example a number or text, in digital media, such as images, video or audio. It may be used to verify its authenticity or identity of its owners. In visible digital watermarking, the information is visible in the digital media. In invisible digital watermarking, the information can't be perceived as such, although it may be possible to detect some amount of information, hidden in the digital media [1], [2].

The image watermarking method must satisfy the following requirements [1]:

(1). Transparency: The embedded watermark pattern does not visually spoil the original image and should be perceptually invisible.

(2). Robustness: The watermark pattern is hard to detect and remove in illegal way.

Watermarking is one of the most popular techniques in protecting copyrights in digital media. Watermarking is also important for several imaging applications:

- Trusted Camera
- Legal usage of images
- News reporting
- Commercial image transaction

In each of these applications, it is important to verify that the image has not been manipulated and the image was originated by a specific user. The watermark embedded into the image can be extracted for the purpose of ownership verification and/or authentication. Due to the combination of the computer and communication technology, more and more digital documents are transmitted and exchanged over the internet. It has created an environment that digital information is easy to distribute, duplicate and modify. This has led to need for effective copyright protection technique.

A halftone image is made up of series of dots rather than a continuous tone. These dots can be different in sizes, different colors and sometimes even different shapes. Larger dots are used to represent darker, denser areas of the images, while smaller dots are used for lighter areas. Halftone images are used in newspapers and magazines because it is much more efficient way to print images. Since a halftone image is made up of discreet dots, it requires significantly less ink to print than a continuous tone image. As long as the resolution of the image is high enough, the dots appear as a continuous image to the human eye [3], [4], and [5].

In this paper we have proposed an effective digital watermarking technique for halftone images based on the (2, 2) visual cryptography scheme. Digital watermark is point of attraction for the hackers, to break and use it in an illegal way. It is difficult to verify that particular data has been sent from the intended sender or not i.e. verification of the owner, if the watermark is hacked or cracked and used in illegal way. Watermarking is now days used in newspapers for copyright protection. The proposed visual cryptography based digital watermarking scheme can be applied to newspaper data, which are halftone images just before the last printing procedures. The verification share will be embedded into the newspaper by the copyright holder of the newspaper and verification is done by the newspaper readership corporation, who performs copy control and copy record management using watermark detection. This process will help in the management of the copy usage and copy usage fees and provide unified right management.

The rest of the paper is organized as follows: Section 2 describes the (2, 2) visual cryptography scheme which is used for the generation of the shares of the watermark pattern. Section 3 and 4 describe error diffusion algorithm & the proposed watermarking scheme respectively. Section 5 shows experimental results and section 6 is analysis of the proposed scheme. Finally, section 7 concludes the paper.

2. BRIEF DESCRIPTION OF (2, 2) VISUAL CRYPTOGRAPHY SCHEME
Visual cryptography scheme was introduced by Naor and Shamir [6], [7], [8].which is used to encrypt written material such as printed text, handwritten notes, pictures, etc., in a perfectly secure way which can be decoded directly by the human visual system. In visual secret sharing scheme an

image is broken up into n parts called shares so that only someone with all n shares could decrypt the image, while any n-1 shares revealed no information about the original image. Each share was printed on a separate transparency, and decryption was performed by overlaying the shares. When all n shares were overlaid, the original image would appear.

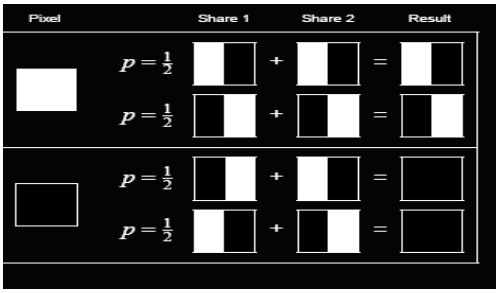


Figure 1: (2, 2) Visual cryptography scheme

To encrypt the secret information using (2, 2) visual cryptography scheme, the secret information is dived into two shares such that each pixel in the original image is replaced with the non-overlapping block of two subpixels. Anyone who holds only one share will not able to reconstruct the secret information as single share does not contain complete secret information. Figure 1 illustrates encoding scheme for (2, 2) visual cryptography which is to be applied on the every pixel of the secret information. If pixel p is white of the secret information then it is replaced with two identical blocks of subpixels. If the pixel p is black of the secret information then it is replaced with two complementary blocks of subpixels. To decrypt the secret information, each share is xeroxed onto the transparency. Superimposition of both transparencies will reveal the secret information.

3. ERROR DIFFUSION ALGORITHM

The host image is converted into the halftone image using error diffusion algorithm. Error diffusion is a type of halftoning in which the quantization residual is distributed to neighboring pixels that have not yet been processed. Its main use is to convert a multilevel image into binary image. As discussed in section I, that these halftone images are used in newspaper & even newspaper itself is a halftone image. Floyd Steinberg algorithm is an error diffusion algorithm approximate the original color depth by diffusing error to the four neighboring pixel. It is faster than other error diffusion algorithms and produces better quality of halftone image. When the following algorithm is applied on host image (I), it generates halftone image (H). In this paper, we use the Floyd-Steinberg Algorithm to get the halftone images [9], [10], and [11].

```
for each y from top to bottom
  for each x from left to right
    oldpixel := pixel[x][y]
    newpixel := find_closest_palette_color(oldpixel)
    pixel[x][y] := newpixel
    quant_error := oldpixel - newpixel
    pixel[x+1][y] := pixel[x+1][y] + 7/16 * quant_error
    pixel[x-1][y+1] := pixel[x-1][y+1] + 3/16 * quant_error
    pixel[x][y+1] := pixel[x][y+1] + 5/16 * quant_error
   pixel[x+1][y+1] := pixel[x+1][y+1] + 1/16 * quant_error
```

For example, to convert 16 bit to 8 bit find_closest_palette_color () may perform just a simple rounding find_closest_palette_color (oldpixel) = oldpixel / 256 * 256.

4. THE PROPOSED WATERMARKING SCHEME

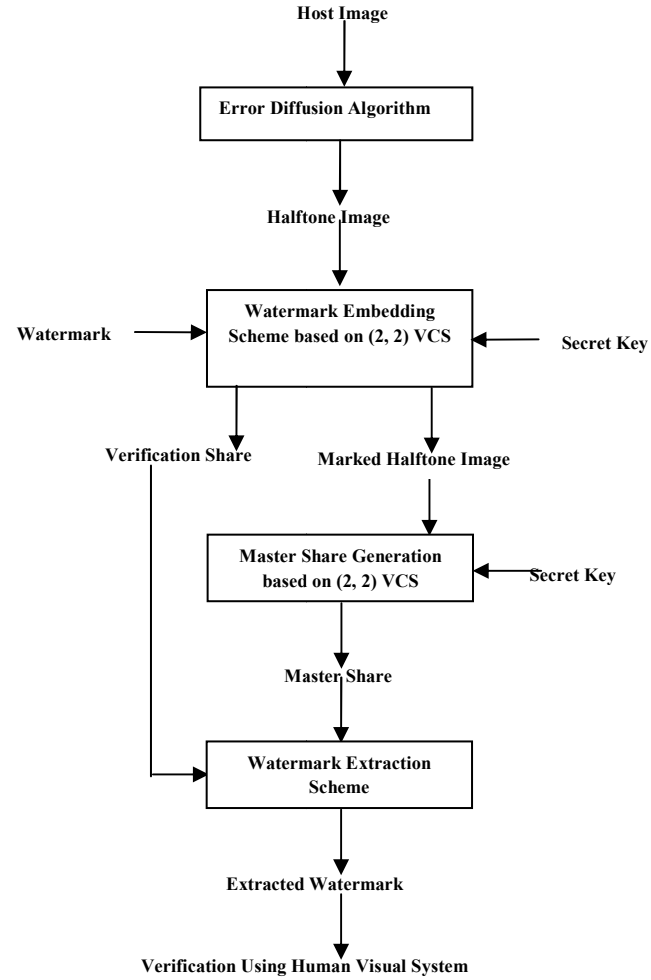


Figure2: Proposed watermarking scheme

The figure 2 shows the proposed watermarking scheme. A binary watermark (W) of size P×Q is to be embedded over the halftone image (I) of the X×Y. The scheme does not embed the watermark directly over the image instead it divides the watermark into the shares called as shares using (2, 2) visual cryptography scheme. At the time of watermark embedding verification share (V) is generated using the original halftone image and master share is generated just before the watermark extraction process. The watermark embedding process is performed using a secret key 'K', original halftone image (I) and original watermark pattern (W). Just before the watermark extraction process the master share (S) is generated using marked image (M) and secret key 'K'. Using verification share (V) and master share (S) the watermark pattern is extracted and the verification can be performed by the human visual system.

4.1 Watermark Embedding Scheme

At the time of watermark embedding process a random number 'K' is selected as a secret key. The secret could be same or different for different halftone images and it must be kept secretly. The embedding phase includes following steps:

Input: Secret key (K), halftone image (I) of size X×Y.

Output: Marked image (M) of size X×Y.

Step1. Select a random number K as the secret key of the halftone image (I). For each image different secret key is used to generate different verification share of the watermark pattern.

Step2. Use 'K' as the seed to generate P×Q random numbers over the interval [1, h]; where h= X×Y. Let R_i is i^{th} random number. The random numbers are generated to implement the concept of visual cryptography to generate the shares.

Step3. Random numbers generated in the step 4 are converted into the binary values and a binary matrix Z of size P×Q is created such that the elements of the matrix Z are the least significant bit of the R_i; i^{th} random number.

Step4. To generate the verification share pixel pair values, watermark pattern W and the binary value of matrix Z is taken and using these i^{th} pair (V_{i1}, V_{i2}) of the verification share (V) is created based on the information given in the table 1.

Step5. All the pair values are assembled to generate the verification share (V) of size P×2Q of the watermark pattern (W).

4.2 Watermark Extraction and Verification scheme

To verify that the image has been sent from the intended sender the watermark pattern is to be extracted from the marked image and before this a master share is generated from the marked image using secret key of the sender. This includes following steps:

Input: Marked image (M) of size X×Y, watermark pattern W of size P×Q, verification share (V) of size P×2Q.

Output: Master share (S) of size P×2Q, extracted watermark pattern (W') of the size P×Q.

Step1. Use secret key 'K' as a seed to generate P×Q random numbers over the interval [1, h]; where h=X×Y. Let Ri is ith random number.

Step2. Random numbers are converted into binary values and binary matrix Z' of size P×Q is created such that the elements of the matrix Z' are the least significant bit of the Ri; ith random number.

Step3. Assign the ith pair (Si1, Si2) of the master share (M) based on the information given in the table 2.

Step4. Assemble all the pair values to construct the master share (S) of size P×2Q. This share is required for the extraction of the watermark pattern.

Step5. To extract the watermark pattern compare verification share (V) and master share (S). If the ith pair (Vi1, Vi2) of V is equal to the ith pair (Si1, Si2) of S then assign the ith element value of the extracted watermark pattern 1 else assign 0. If through human visual system W' can be recognized as W, then it is exact image which has been sent.

Table 1: The rules for generation of verification share

Color of the i^{th} pixel in watermark pattern W_i	i^{th} element in binary matrix Z_i	Pair of bits (V_{i1}, V_{i2}) to be assigned in verification share (V)
Black	1	(0, 1)
Black	0	(1, 0)
White	1	(1, 0)
White	0	(0,1)

Table 2: The rules for generation of master share

i^{th} element in binary matrix Z'_i	Pair of bits (S_{i1}, S_{i2}) to be assigned in master share (S)
1	(1, 0)
0	(0, 1)

5. EXPERIMENTAL RESULTS

This section presents some experimental results concerning the proposed scheme. The figure 3 shows the original image of size 512×512. The proposed scheme is tested on the halftone image of the size 512×512 which is shown in the figure 4. The marked image is shown in the figure 5 is of size 512×512 and watermark pattern to be embedded is of size 68×69 shown in the figure 6. Figure 7 and figure 8 show the verification and master share. Figure 9 shows the extracted watermark pattern. All experiments are implemented in MATLAB Image Processing toolbox

Figure 3: Original Image

Figure 4: Halftone Image

Figure 5: Marked Halftone Image

Figure 6: Original Watermark

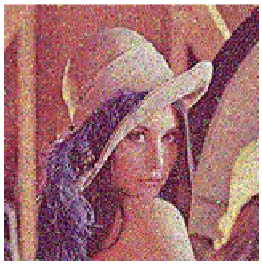
Figure 7: Verification Share

Figure 8: Master Share

Figure 9: Extracted Watermark

To test the robustness of the proposed scheme several watermarking attacks have been applied such as noise, sharpening, blurring, average filter, jpeg compression, image flipping attack etc.

5.1 Noise Attack



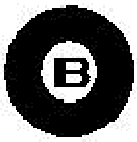


Figure 10: (a) Salt & Pepper attack on Figure 5
(b) Extracted watermark

5.2 Sharpening Attack

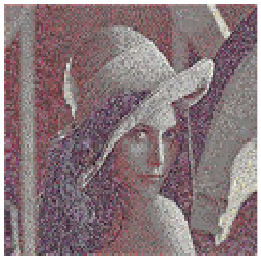


Figure 11: (a) Sharpening attack on Figure 5
(b) Extracted watermark

5.3 Blurring Attack

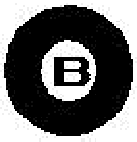


Figure 12: (a) Blurring attack on Figure 5
(b) Extracted watermark

5.4 Averaging Filter Attack

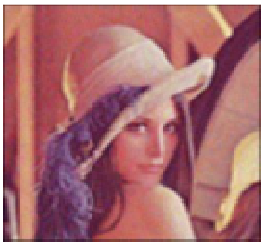
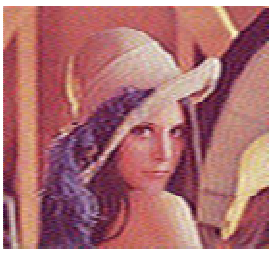


Figure 13: (a) Averaging filter attack on Figure 5
(b) Extracted watermark

5.5 JPEG compression attack



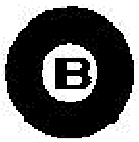
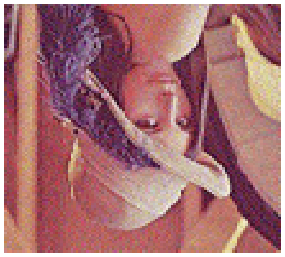


Figure 14: (a) JPEG Compression attack on Figure 5
(b) Extracted watermark

5.6 Image Flipping attack



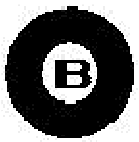


Figure 15: (a) Image flipping attack on Figure 5
(b) Extracted watermark

6. ANALYSIS OF THE PROPOSED SCHEME

This section shows results regarding the Peak Signal To Noise Ratio (PSNR) and Normalized Cross Correlation (NC) to evaluate the proposed watermarking scheme.

6.1 Peak Signal To Noise Ratio (PSNR)

PSNR is the ratio for indicating the quality measure of the image. Higher PSNR means reconstruction is of higher quality. It is defined via the Mean Square Error (MSE) calculated as:

$$MSE = \frac{1}{3*m*n}\sum_{i=0}^{m-1}\sum_{j=0}^{n-1}[f(x,y) - F(x,y)]^2 \quad (1)$$

The PSNR is defined as

$$PSNR = 10 * log_{10}\left(\frac{MAX_I^2}{MSE}\right) \quad (2)$$

Where MAX_I is the maximum pixel value of the image. When the pixel is represented by 8bits/sample, MAX_I is 255.

6.2 Normalized Cross Correlation (NC)

NC is used to measure the similarity between the original watermark and extracted watermark and defined as:

$$\rho(w, W) = \frac{\sum_{i=1}^{n} w_i W_i}{\sqrt{\sum_{i=1}^{n} w_i^2}\sqrt{\sum_{i=0}^{n} W_i^2}} \quad (3)$$

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

Proposed watermarking scheme is based on visual cryptography, which not only protects the watermark for illegal access but also provide an effective copyright protection scheme. This can be verified by the PSNR and NC values as shown in the figure 15 and table 3. The advantage of the scheme is that using different secret key each time different verification share can be generated which enhances the reliability to the system.

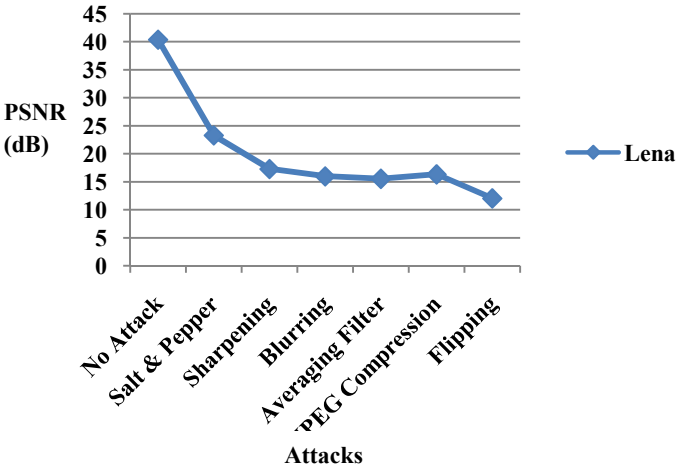


Figure 16: PSNR between original halftone image and marked image after attacks

Table 3: Normalized Cross Correlation between Original and Extracted Watermark

Attack	Correlation (%)
No Attack	99.75
Salt & Pepper Noise	98.62
Sharpening	98.34
Blurring	97.48
Averaging Filter	98.52
JPEG Compression	98.33
Flipping	98.67

7. CONCLUSION

We have proposed digital watermarking scheme for halftone images using visual cryptography scheme, which embed the watermark without affecting the quality of the host image. The scheme is robust against various watermarking attacks such as noise, sharpening, blurring, averaging filter and JPEG compression etc. The scheme is based on visual cryptography and watermark is embedded as a share, which does not reveal complete information about the original watermark, hence it will reduce the chances of watermarking hacking and modification. The key point of the scheme is the secret key; if it is kept secretly then it would be impossible to detect the watermark. The scheme does not depend on the transformations which are used in frequency and spatial domain watermarking scheme. These characteristics prove that the proposed watermarking scheme is robust and transparent.

8. ACKNOWLEDGEMENT

This work was supported by BISAG, Gandhinagar (Gujarat), India, Mr. Nisheeth Saxena & Mr. P. K. Bishnoi, MITS, Lakshmangarh (Rajasthan).

9. REFERENCES

[1] Chunlin Song, Sud Sudirman and Madjid Merabti, “Robust Digital Image Watermarking using Region Adaptive Embedding Technique”, IEEE, pp. 378-382, 2010.

[2] Y-C Hou, P-M Chen, "An Asymmetric Watermarking Scheme based on Visual Cryptography", In Proceedings of ICSP, Vol. 2, pp. 992 -995, (2000).

[3] Ming Sun Fu. Oscar C. Au, “Joint Visual Cryptography and Watermarking”, IEEE International Conference on Multimedia and Expo, pp-975-978 (2004).

[4] Wei Qiao, Hongdong Yin, Huaqing Liang, “A Kind of Visual Cryptography Scheme For Color Images Based on Halftone Technique” In proceeding of IEEE, pp. 393-395, (2009).

[5] Nitty Sarah Alex, L. Jani Anbarasi, “Enhanced Image Secret Sharing via Error Diffusion in Halftone Visual Cryptography” In proceeding if IEEE, pp. 393-397, (2011).

[6] A. Shamir,. “How to Share a secret”,Communications of the ACM, vol. 22, pp.612-613, 1996.

[7] M. Naor, and A. Shamir, “Visual Cryptography”, Advances in Cryptology – Eurocrypt’94 Proceeding, LNCS Vol. 950, Springer-Verlag, pp. 1-12, 1995..

[8] M. Naor and A. Shamir, “Visual Cryptography II:Improving the Contrast Via the Cover Base”,Cambridge Workshop on Protocols, 1996.

[9] Hao Luo, Faxin Yu, “Data Hiding in Image Size Invariant Visual Cryptography” In proceeding of IEEE, pp. 273-276, (2008).

[10] N. Krishna Prakash, Prof. S. Govindaraju, “Visual Secret Sharing Schemes for Color Images using Halftoning”, In proceeding of International Conference on Computational Intelligence and Multimedia Applications, IEEE, pp. 174-178, (2007).

[11] Zhi Zhou,Gonalzo R. Arce and Giovanni Di Crescenzo, “Halftone Visual Cryptography”, IEEE Transactions On Image Processing, Vol. 15, NO. 8, pp. 2441-2453, 2006.