

# Sensitive Digital Image Watermarking for Copyright Protection

B. Surekha<sup>1</sup> and G. N. Swamy<sup>2</sup>  
(Corresponding author: B. Surekha)

Associate Professor, Department of ECE, TRR College of Engineering<sup>1</sup>  
Patancheru, Hyderabad, Andhra Pradesh, INDIA - 502 319.

Professor, Department of ECE, VR Siddhartha Engineering College<sup>2</sup>  
Kanuru, Vijayawada, Andhra Pradesh, INDIA – 520 007

(Email: borrasurekha@gmail.com)

(Received Feb. 1, 2012; revised and accepted June 12, 2012)

## Abstract

In this paper, a watermark hiding scheme for copyright protection of sensitive images is proposed. The concept of visual cryptography is used, so that the original host image is not altered. The proposed scheme aims at improving the security of the related schemes. The scheme also reduces the size of codebook and size of shares, to be used in watermark hiding process. This is achieved by adapting the concept of Pair-Wise Visual Cryptography (PWVC). The simulation results reveal that the proposed scheme has good robustness to a range of image processing attacks.

*Keywords:* Copyright Protection, digital watermarking, discrete wavelet transform, secret sharing, visual cryptography.

## 1 Introduction

The evolution in Internet technology has led to easy access of multimedia data such as text, image, audio and video. However, there are some areas (E-commerce) where the data cannot be arbitrarily copied, distributed and modified. Various schemes have been introduced to address the problem of copyright protection of such data. Digital Image Watermarking is one such technique. It combines the copyright information (in the form of watermark image) with the image to be protected, in such a way, that it is hard to be detected and removed. Later, when the owner wants to prove his copyrights, he can do it so by extracting the watermark from the watermarked image.

The performance of any watermarking technique depends on several criteria [10]: Imperceptibility: refers to the perceptual similarity between the watermarked image and the original image. Robustness: refers to the immunity of the watermark to several attacks, which may happen during transmission or storage phase. Security: refers to the ability of the watermarking scheme to extract the watermark, without any ambiguity, by the right owner. Capacity: refers to the size of the watermark that can be embedded into the host image.

In traditional watermarking techniques, large watermarks demands for a compromise between robustness and imperceptibility. Hence, it is very difficult to satisfy all the performance criteria at a time. This tradeoff can be solved by adapting the concept of Visual Cryptography (VC). A  $t$ -of- $n$  threshold visual cryptography [13] encrypts a secret image into  $n$  random looking images called shares. Note that, the shares are expanded versions of the original secret image. These shares are printed on to transparencies and are distributed to  $n$  participants. A codebook used in generating these shares is designed, in such a way that gathering of any  $t$  out of  $n$  shares can visually recover the secret image and any less than  $t$  number of shares is unable to decode the secret. The secret image is revealed by stacking  $t$  or more number of shares one above the other. The decoding of the secret by the Human Visual System (HVS) is the interesting feature that has attracted the research community in adapting this concept for several applications including watermarking and authentication.

The classification of copyright protection schemes based on VC is done on several view points. One of the viewpoints is based on whether a part of the watermark (public share) is physically embedded into the host image or not. If the public share is physically embedded into the host image then they fall under the category of watermark embedding schemes [1, 3, 6, 12]. These are much similar to traditional watermarking schemes in the way they embed the watermarks and are unable to balance all the performance criteria at a time. The second category schemes are called watermark concealing schemes [2, 4, 5, 7, 8, 9, 11, 14, 15, 17, 18, 19, 20]. This category of schemes doesn't physically embed the watermark into the host image. Since the original image is not altered; these techniques are particularly useful in protecting highly sensitive images (astronomical, military and medical).

Irrespective of the working domain, almost all VC based watermark concealing schemes in the literatures are based on (2, 2) VC and works as follows: Given a host image and a binary watermark, these schemes first compute

a feature vector from the host image. A method of comparison and a secret key is then used to obtain a secret binary matrix from the extracted feature vector. Depending on the color of each pixel in the binary watermark, and the bits in the secret binary matrix a particular code is selected from the code book of (2, 2) VC to create a noise looking binary image, called private share. This share is time-stamped and is confidentially kept secret at a Certified Authority (CA). During copyright verification, a similar process is used to extract another noise looking binary image called public share from the claimed image using the same secret key. It is then combined with the private share to prove the copyrights.

This approach can be extended to embed multiple watermarks into the same host image. In this case, multiple private shares (one for each owner) are to be generated using multiple secret keys and are to be registered with the arbitrator. Since, shares are expanded versions of the original watermark it will be a heavy burden for the CA to store them. Hence, it is important to reduce the size of shares (or pixel expansion) as much as possible.

Another problem with such schemes is that, most of them are not secure always. This is because they don't meet all the security requirements of VC. Further, any watermarking technique becomes meaningless, if it leads to false positives. A false positive is a result of extraction of a watermark from an unauthorized image, which doesn't actually belong to the owner. Since, false positives encourage malicious owners in claiming other unauthorized images, this problem should be avoided. This problem pronounces if the selected feature vector is not unique.

One simple spatial domain scheme, which leads to false positives, is Hwang's scheme [9]. This scheme constructs a secret binary matrix from Most Significant Bits (MSB's) of selected pixel values of the host image. The security of this scheme is analyzed by Hassan et al. [5] proved that if 90% of the pixels in the host image have gray-levels greater than 128, then the scheme becomes monotonous, since private share can be revealed without the knowledge of the secret key. To improve the security of the Hwang's scheme, Surekha et al. [15] proposed a similar MSB's based technique, which involves an XOR operation. This scheme offers better security than Hwang's scheme, but with no improvement in robustness. Also, since feature vector is obtained directly from MSB's, both these schemes increase the probability of false alarm and leads to ambiguity in copyright verification. Hence, such schemes can't be used for copyright protection.

To overcome this drawback, Hsu et al. [8] used the theories and properties of sampling distribution of means (SDM) to achieve the required security. Y. C. Hou [7] compared two pixels that are selected randomly from the host image are used to determine the feature vector. Zaghoul et al. [20] extended Hwang's scheme to hide a binary watermark into a color image by using features extracted from histograms of HSV planes of the host images. This histogram which usually describes the color

distribution of an image is easy to be computed but does not include any spatial information, and is therefore liable to false positives.

A robust scheme, which leads to false positives, while working in frequency domain is LTL scheme [11], proposed by Lou et al., This scheme constructs a secret binary matrix by comparing the modified Discrete Wavelet Transform (DWT) coefficients obtained, from two selected sub bands of same level with that of LL sub bands coefficients. The security of this scheme is analyzed by Chen et al. [2]. They proved that for almost all host images, the LL sub band coefficients of DWT are greater than or equal to coefficients in other sub bands. The result is that the scheme becomes monotonous, as verification of watermark purely depends on secret key. This way, the LTL scheme increases the probability of false alarm and leads to ambiguity in copyright verification. Hence, this scheme can't be used for copyright protection. To overcome this drawback, Park et al. [14] used a different threshold for comparison. They have compared the same modified DWT coefficients of LTL's scheme with the average of the coefficients in LL sub band. Though this scheme reduces the probability of false alarm to some extent, it fails in secure verification of watermark. The security of this scheme is analyzed by Xing et al. [19] and has proved that, if someone gains a copy of private share, they can overlay it on a share consisting of all black pixels to extract a trace of the watermark without the need to extract a public share. The result is that the scheme becomes independent of the host image and the secret key. This problem arises due to majority of black sub pixels in their codebook. The scheme also has a drawback that it requires the original watermark, in addition to private share for copyright verification. To enhance the security, Xing proposed a new DWT based scheme that compares modified LL sub band coefficients with the same average that was used in Park's scheme. It results in four different decimal values (0, 1, 2, 3), instead of binary 1's and 0's to be contained in the secret matrix for generation of shares. This doubles the size of the codebook. In addition, the selected feature may not guarantee to result equal probability of occurrences of all the four decimal values. This reduces the security of visual cryptography.

The objectives of this research paper are three fold: (i) to investigate and introduce three new security related performance criteria which are to be satisfied by all VC based watermark concealing schemes. They are column equity, code equity, and color equity. Note that, the schemes that fail to satisfy these criteria may result in ambiguity, while resolving rightful ownership; (ii) propose a novel watermark concealing scheme in DWT domain that satisfies all these criteria; (iii) a modified VC technique called Pair-Wise Visual Cryptography (PWVC) is applied in order to have no pixel expansion while creating the shares. Since the size of share images is same as the original watermark it brings greater convenience for the arbitrator in carrying and storing the private shares.

The rest of the paper is organized as follows. In Section 2, we review some preliminaries related to the proposed watermarking scheme. Section 3 describes the proposed watermark hiding and verification phases. In Section 4, along with simulation results, we draw some comparisons among the proposed scheme and well known VC-based DWT watermarking schemes with respect to security criteria and pixel expansion. Finally, Section 5 concludes the paper.

## 2 Preliminaries

### 2.1 Basic 2-of-2 Visual Cryptography

Visual cryptography [13] is an image secret sharing scheme proposed by Naor and Shamir in mid 90's. A basic version of it is 2-of-2 visual cryptography. It divides a secret image into two random looking images called shares. The procedure for creating the shares is as follows: using a codebook given in Table 1, each pixel in the original secret image is replaced by a block of four pixels called code-block. A white pixel is shared into two identical code blocks. A black pixel is shared into two complementary code-blocks.

While creating the shares, if the given pixel  $p$  in the original image is white, then the encoder randomly chooses one of the first two columns of Table 1 to select the code-block. If the given pixel  $p$  is black, then the encoder randomly chooses one of the last two columns of Table 1, to select the code-block. All the pixels are coded by independent random selection of columns. Therefore no information is gained by observing any group of pixels on each share. Note that, the security of VC lies in the random selection of the columns and the design of code-blocks in the codebook.







Assuming that the VC chooses its first column in the codebook if secret key bit is 0 and second column when secret key bit is 1, a secret key is used as a seed to generate a random binary matrix of size equal to original secret image. The bits in this binary matrix are used as a key for selecting particular columns in the codebook.

The results of basic 2-of-2 VC are shown in Figure 1. To decode the secret image, each of these shares is to be Xeroxed on transparent sheets. Stacking both these sheets will reveal the original secret. When the two shares are overlaid one above the other, as in Figure 1.d, the black pixels in the original image remain black and the white pixels turns gray.

In addition to satisfying minimal perceptibility, high robustness, high capacity and less complexity, the VC-based watermarking schemes should meet other performance criteria such as minimum pixel expansion and security. Note that there exists tradeoff between pixel expansion and security in VC. While pixel expansion purely depends on the codebook used for VC, the security of VC depends on the random selection of the columns as

well as the design of the codebook.

Table 1: Codebook used in basic 2-of-2 visual cryptography

Pixel	White	Black
Prob.	50% 50%	50% 50%
Share1		
Share2		
Share1 + Share2		

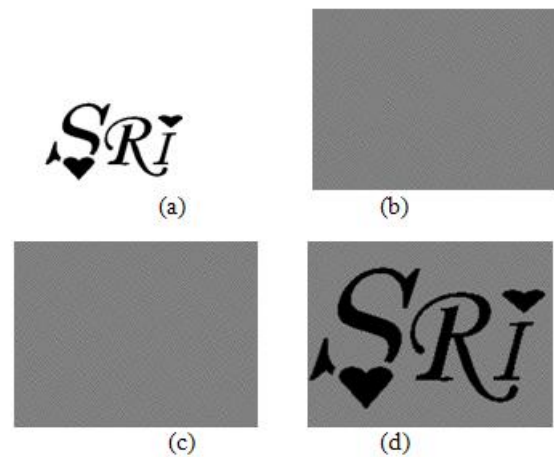


Figure 1: Example of basic 2-of-2 visual cryptography  
 a) secret binary image b) Share-1 c) Share-2  
 d) decoded image

Smaller pixel expansion implies small shares, and hence requires less storage space. Maximum security in VC is achieved when the following three criteria are satisfied by the codebook. They are column equity, code equity, and color equity.

Column Equity: refers to the probability of selecting each column in the codebook of VC, while coding either black or white pixel of the secret image. A 'high' value for column equity indicates that the probability of choosing both the columns is almost equal. If only one column is chosen always to select the codes, for either pixel color, then VC becomes independent of a secret key, thereby leaving a clue about the secret pixels upon observing a group of pixels on either share. This greatly reduces the security of VC, and hence makes it unsuitable for image hiding. Thus to have 'ideal' value for column equity, the secret binary matrix should be chosen in such a way that the probability of occurrences of logical ones and zeros in it

should be same.

**Code Equity:** refers to the similarity of code-blocks used, for coding black and white pixels of the secret image. High code equity indicates that most of the code-blocks used in coding a black pixel are also present in coding a white pixel. If different code-blocks are used for coding black and white pixels, then there is a very good chance for the attackers to predict the secret bit upon observing a group of pixels in individual shares. Thus to have high security for VC, the code equity should have ideal value. For that all the code blocks which are used for coding a black pixel must also repeat in coding a white pixel. This greatly confuses the attacker in predicting the secret bit.

**Color Equity:** refers to distribution of black and white pixels in each code block used in the codebook of VC. High color equity indicates that the probability of distributing black and white pixels in each code block is almost equal. If the probability of distributing one color is much more when compared to the other color, VC becomes independent of the secret key, and leaves a clue about the secret pixels upon observing a group of pixels in each share. Also, if the majority of sub-pixels in all the code blocks are black(white), then it is possible to extract a trace of original secret image by stacking the available share with an image consisting of all white (black) pixels. Again, this greatly reduces the security of VC, and hence makes it unsuitable for image hiding. Thus to have ideal value for color equity the distribution of black and white pixels in each code block should be same.

To achieve high security with VC, the column equity, code equity and color equities should be satisfied.

**2.2 Pair Wise Visual Cryptography (PWVC)**

PWVC [16] technique aims at resolving the tradeoff between color equity and pixel expansion by creating VC shares, which are of same size as the original secret image. Instead of coding a single pixel each time, PWVC technique codes a pair of pixels from the original image, using modified codebook. The procedure is as follows: Given a binary secret image, at any time a pair of pixels can be in one of the four forms WW, BB, WB, BW, where W indicates white pixel and B indicate black pixel. If the given pixel pair in the original image is WW, then the encoder randomly chooses one of the first two columns of Table 2. If the given pixel pair is BB, then the encoder randomly chooses one of the last two columns of Table 2. If the given pixel pair is either WB or BW, then the coding algorithm first checks the count of occurrence of such pairs. If the count is even, then the encoder randomly chooses one of the first two columns of Table 2, otherwise the encoder randomly chooses one of the last two columns of Table 2 Note that, each code-block has one white and one black sub-pixels, independent of the pair of pixels in the secret image. Also, all the codes used for coding a WW pixel pair are also used for coding any other pixel pair. Thus it implies that the codebook used here satisfies both color

equity and code equity.

Table 2: Codebook used in pair-wise visual cryptography

Pixel Pair	WW		BB	
Secret Key bit	0	1	0	1
Share1	■ □	□ ■	■ □	□ ■
Share2	■ □	□ ■	□ ■	■ □
Share1 + Share2	■ □	□ ■	■ ■	■ ■

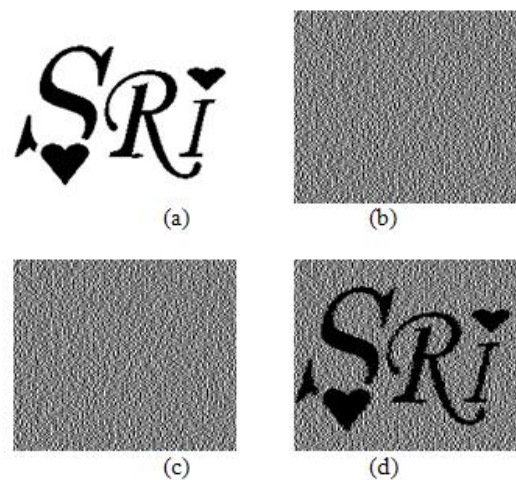


Figure 2: Example of pair-wise visual cryptography  
 a) secret binary image b) Share-1 c) Share-2  
 d) decoded image

The results of PWVC technique are shown in Figure 2.

**3 Proposed Scheme**

There are three types of participants in the proposed model: the owners are the ones who actually own the copyrights of the images to be protected. A Certified Authority (CA) is a trusted third party who resolves the disputes by verifying the rightful ownership. An attacker is the one who modifies the host image with an intention of making watermark unavailable. He can also be a malicious owner who illegally claims the copyrights.

Unlike traditional watermarking schemes, where the watermarks are physically embedded into the host image, the proposed scheme conceals the watermark without altering the host image. In the watermark hiding phase, the owner generates a noise looking image called private share using a secret key and some features extracted from the host image. The watermark and the private share are registered with the arbitrator (CA) secretly. The secret key

is kept secret by the owner and the host image can be published. Once the host images are made available, the attackers may modify and illegally use them. Whenever a dispute regarding rightful owner occurs, the legal owners need to use the same secret key at the arbitrator to extract the public share from the claimed image. The copyrights can then be revealed by overlaying the public share and the private share one above the other. By comparing the extracted watermark and the original watermark, the arbitrator can make a judgment regarding rightful owner. In this way, the legal owners can claim the copyright of the host images.

The procedure for watermark hiding is shown in Figure 3 and the steps are given below:

**Inputs:** Host Image  $I$  of size  $(m \times n)$ , Watermark Image of size  $(r \times c)$ , Secret Key  $S$ , Number of decomposition levels  $k$   
**Outputs:** Private Share of size  $(r \times c)$

**Step 1:** Select the number of wavelet decomposition levels  $k$  such that,  $2^k \geq (m \times n)/(r \times c)$

**Step 2:** A  $k$ -level Discrete Wavelet Transform is performed on the cover image  $I$ . Select  $LL^k$  sub band image for feature extraction.

**Step 3:** Calculate average gray level of the  $LL^k$  sub band image. Let it be  $LL_{avg}$ .

**Step 4:** A secret key  $S$  is used as a seed to select  $r \times c$  random pixel locations with in  $LL^k$  sub band image. Let  $R_i(x,y)$  be the  $i^{th}$  random location.

**Step 5:** For each  $R_i(x,y)$ , select a  $7 \times 7$  size sub image area centered at location  $R_i(x,y)$ , and find its average.

**Step 6:** Construct a feature image  $F$  of size  $r \times c$ , such that the entries in the matrix are the sample averages obtained in the above step.

**Step 7:** Construct a binary matrix  $B$ , using the following comparison:

$$B(x,y) = \begin{cases} 1, & \text{if } F(x,y) \geq LL_{avg} \\ 0, & \text{if } F(x,y) < LL_{avg} \end{cases} \quad (1)$$

**Step 8:** Use the bits in matrix  $B$  as secret key bits to select columns in Table 2 (PWVC scheme) for generating the private share (Share-2).

Finally, the watermark and the private share are time-stamped and are confidentially registered at Certified Authority (CA). The secret key  $S$  and the number of decomposition levels  $k$  are kept secret. During verification of the copyright, the owner should provide the same Secret key  $k$  to the Certified Authority, to retrieve a second share called public share. When this share is overlaid on the private share, the watermark can be revealed.

The procedure for watermark extraction is shown in Figure 4 and the steps are given below:

**Inputs:** Claimed image  $I'$  of size  $(m \times n)$ , private share of size  $(r \times c)$ , Secret Key  $S$ , Number of decomposition levels  $k$

**Outputs:** Watermark of size  $(r \times c)$

**Step 1:** A  $k$ -level Discrete Wavelet Transform is performed on the cover image  $I'$ . Select  $LL^k$  sub band image for feature extraction.

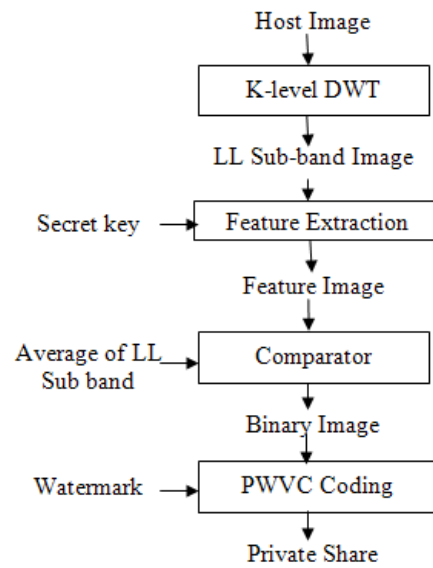


Figure 3: Proposed Watermark Hiding Scheme

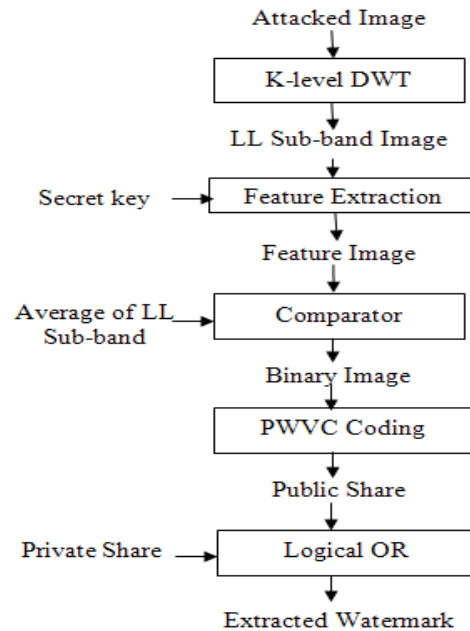


Figure 4: Proposed Watermark Extraction Scheme

**Step 2:** Calculate average gray level of the  $LL^k$  sub band image. Let it be  $LL_{avg}$ .

**Step 3:** A secret key  $S$  is used as a seed to select  $r \times c$  random pixel locations with in  $LL^k$  sub band image. Let  $R_i(x,y)$  be the  $i^{th}$  random location.

**Step 4:** For each  $R_i(x,y)$ , select a  $7 \times 7$  size sub image area centered at location  $R_i(x,y)$ , and find its average.

**Step 5:** Construct a feature image  $F$  of size  $r \times c$ , such that the entries in the matrix are the sample averages obtained in the above step.

**Step 6:** Construct a binary matrix  $B$ , using the following comparison:

$$B(x,y) = \begin{cases} 1, & \text{if } F(x,y) \geq LL_{avg} \\ 0, & \text{if } F(x,y) < LL_{avg} \end{cases} \quad (2)$$



*Step 7:* Use the bits in matrix  $B$  as secret key bits to select public share (Share-1). Note that, the code block assignment for public share corresponding to each secret bit is independent of the pixel pair colors in the watermark image.

*Step 8:* Perform bitwise logical OR operation on the public share and the private share to extract the watermark.

Note that, in the above watermark hiding algorithm, the host image remains unaltered. Hence, the scheme has maximum imperceptibility. Since PWVC technique is used in creating shares, the size of shares is same as the watermark image size. The security of the proposed scheme lies in the generation of secret binary matrix  $B$ , and the design of the codebook used in creating public share and the private share. Here, each entry in the secret binary matrix is obtained by comparing an average of 49 randomly selected coefficients in  $LL$  sub band image, with that of average value of all the coefficients in the same  $LL$  sub band image.

According to the central limit theorem, even if the coefficients of  $LL$  sub band image are not normally distributed, the sampling distribution of averages will approximate a normal distribution, provided the sample size is sufficiently large. The result is that the probability of the number of sample averages which are greater than or equal to the  $LL_{avg}$  is almost equal to the number of sample averages which are less than  $LL_{avg}$ . Since the probability of occurrence of logical ones and zeros in binary matrix is almost same, the probability of choosing both the columns for assigning a code block is also same. Hence the property of column equity satisfies in the proposed scheme. In this way, the proposed scheme improves the security.

## 4 Experimental Results

In this section we give three types of simulation results to evaluate the performance of the proposed VC based watermark concealing scheme. The first type of simulation is done to hide and extract a binary watermark into a gray level watermark using the algorithms mentioned in the previous section. The watermark is extracted by assuming that the host image is not attacked. The second category results were obtained by inputting different attacked images as host images to the watermark extraction algorithm. These results are useful in evaluating the robustness of the proposed scheme to common attacks. Third type of simulations helps in analyzing the performance of the proposed scheme for any test image. In the first type of simulations, a standard gray level cover image Boat, of size  $512 \times 512$  (Figure 5(a)) is chosen as a test image and a binary image of size  $100 \times 100$  is chosen as a watermark (Figure 5(b)). The number of decomposition levels chosen is two. The software chosen is MATLAB 7.5. When the host image and the watermark, along with a secret key, are given as inputs to the watermark hiding algorithm, the result is a private share of size  $100 \times 100$ , which are shown in Figure 5(d) When the host image and private shares are

columns in Table 2 (PWVC scheme) for generating a given as inputs to watermark extraction algorithm, the result is a public share of size  $100 \times 100$  (Figure 5(e)). When a logical OR operation is performed on the public share and the private share the watermark shown in Figure 5(f) is obtained. Although some contrast loss occurs, the extracted watermark can be clearly identified. Note that, the private share, the public share and the extracted watermark size is same as that of the original watermark.

The parameters used to evaluate the performance of the proposed scheme are Peak Signal to Noise Ratio (PSNR) and Normalized Correlation (NC). PSNR is used to evaluate the similarity of original and attacked gray level images. It is defined in terms of Mean Square Error (MSE) as follows:

$$PSNR = 10 \times \log \frac{255^2}{MSE} \quad (3)$$

$$MSE = \frac{1}{m \times n} \sum_{i=1}^m \sum_{j=1}^n (c_{i,j} - c'_{i,j})^2 \quad (4)$$

Where  $c_{i,j}$  denotes pixel color of original host image and  $c'_{i,j}$  denotes a pixel color of attacked host image, and  $m \times n$  denotes the host image size.

Normalized Correlation (NC) is used to measure the similarity between the original and extracted watermark. It is defined as follows:

$$NC = \frac{\sum_{i=1}^r \sum_{j=1}^c (w_{i,j} \oplus w'_{i,j})}{r \times c} \times 100\% \quad (5)$$

Where  $w_{i,j}$  denotes pixel color of extracted watermark image from the original host image when it is not altered and  $w'_{i,j}$  denotes a pixel color of extracted watermark image when the host image is altered, and  $r \times c$  denotes the watermark size.

In the second type of simulations, the boat image is subjected to several common attacks using Matlab software (shown in Figure 6). The corresponding PSNR values are given in Table.3. Each of these attacked images is individually given as inputs to the watermark extraction algorithm and the corresponding public shares are obtained. When these are stacked with the same private share obtained during watermark hiding phase (Figure 5.d). The result is a set of extracted watermark images which are shown in Figure 6, with different NC values, which are given in Table 3.

Third type of simulations helps in analyzing the performance of the proposed scheme for any host image with respect to robustness. Two other benchmark images (Lena and Mandrill) of same size (shown in Figure 7.) are selected as cover images and the simulations of the above two categories is performed. All the test images are downloaded from the website: <http://images.google.co.in> with search words Lena, mandrill, boat of size:  $512 \times 512$ . The resultant PSNR and NC values are listed in Table 3.

Results in Table 3 shows that the proposed algorithm has

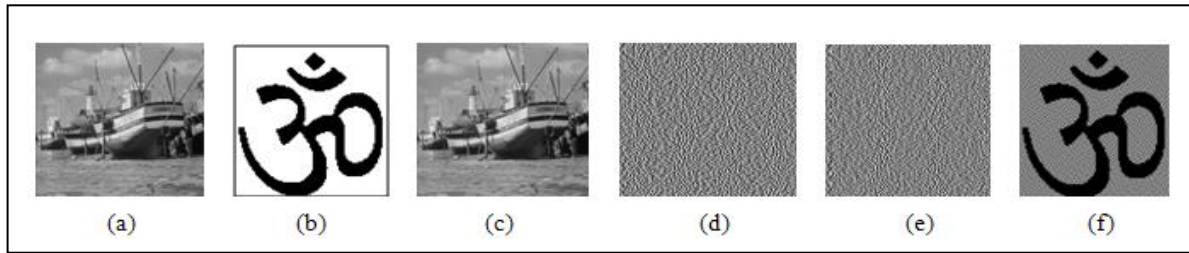


Figure 5: Simulation results of proposed watermark hiding and extraction algorithms  
 a) Host image (512x512) b) Watermark (100x100) c) Host image after generating private share (512x512)  
 d) Private share (100x100) e) Public share (100x100) f) Extracted watermark (100x100)

good robustness against JPEG compression, sharpening, median filtering, wiener filtering, scaling, noise adding, blurring, intensity adjustments, and jitter attacks. It is noticed that the scheme results in satisfactory robustness to cropping, translation and rotations attacks.

The effectiveness comparison of the proposed scheme with some known DWT and VC based copyright protection schemes in the literature are given in Table 4. The comparison is mainly focused on the following properties: pixel expansion, column equity, code equity, color equity and the security. From the results in Table 4, it is clear that only the proposed scheme satisfies all the security related criteria mentioned in Section 2.1 without any pixel expansion.

### 5 Conclusions

In this paper, three new security related performance criteria which are to be satisfied by all watermark concealing schemes based on VC are introduced. They are column equity, code equity, and color equity. A novel watermark concealing scheme is proposed to improve these criteria. In addition, a modified VC technique called PWVC technique is applied in order to have no pixel expansion while creating the shares. The simulation results reveal that the proposed scheme has good robustness to a range of image processing attacks. When compared with the popular DWT and VC-based copyright protection schemes in the literature, the advantages of the proposed scheme are as follows: First, the proposed scheme meets all the security requirements of VC and hence offers better security; second, the scheme requires less memory space to store private shares, thereby reducing the overhead on CA.

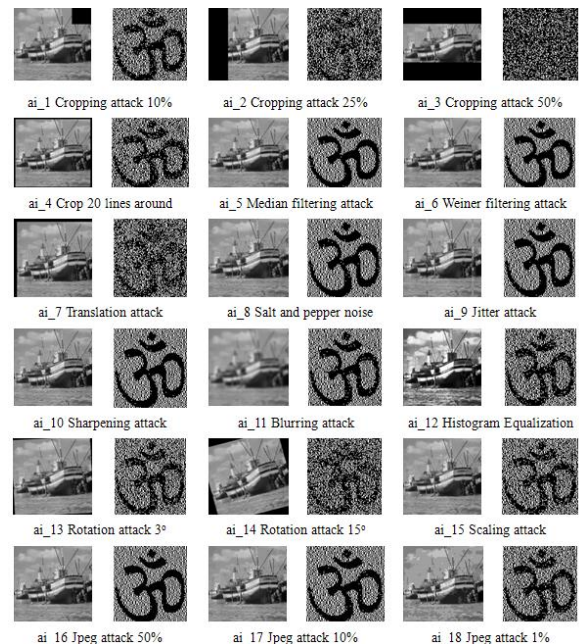


Figure 6: Attacked images and corresponding watermarks

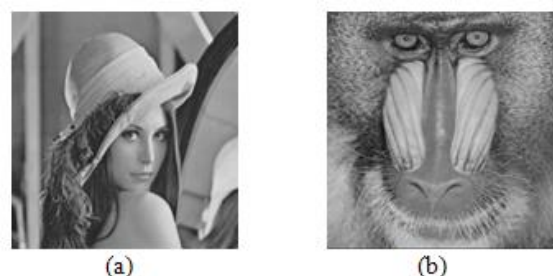


Figure 7: Test images a) Lena (512x512) b) Mandrill (512x512)

### References

[1] C. C. Chang and J. C. Chuang, "An image intellectual property protection scheme for gray-level images using visual secret sharing strategy," *Pattern Recognition Letters*, vol. 23, pp.931-941, 2002.  
 [2] T. H. Chen, C. C. Chang, C. S. Wu, and D. C. Lou, "On the security of a copyright protection scheme

based on visual cryptography," *Computer Standards & Interfaces*, vol. 31, no.1, pp. 1-5, 2009.  
 [3] N. V. Dharwadkar and B. B. Amberker, "Watermarking scheme for color images using wavelet transform based texture properties and secret sharing," *International Journal of Information and Communication Engineering*, vol. 6, no. 2, pp. 94-101, 2010.

Table 3: Test results for robustness against several attacks

Attacks	Boat		Mandrill		Lena	
	PSNR (dB)	NC (%)	PSNR (dB)	NC (%)	PSNR (dB)	NC (%)
Cropping (10%)	36.11	93.82	36.11	92.63	36.21	96.36
Cropping (25%)	30.19	83.20	30.19	81.07	30.25	90.51
Cropping (50%)	27.13	73.10	27.14	77.36	27.20	80.98
Jitter	41.74	99.51	41.26	98.44	41.40	98.57
Blurring	30.52	97.51	29.12	97.11	32.64	98.44
Sharpening	29.61	99.34	28.29	98.88	32.54	99.36
Histogram Equalization	26.97	93.55	27.57	99.20	41.94	98.17
Median Filter 3*3	36.42	99.69	31.69	99.29	40.71	99.82
Wiener Filter 5*5	34.84	99.72	30.77	99.50	39.95	99.84
Salt & Pepper Noise	44.08	99.25	44.10	99.11	38.05	98.34
Ccw_Rotation_3°	29.59	92.09	28.69	92.11	30.68	93.24
Ccw_Rotation_15°	27.89	85.26	27.63	80.79	27.94	80.65
Scale_0.5	33.60	99.16	30.99	98.80	36.81	99.37
JPEG_80	39.44	99.93	35.78	99.92	42.81	99.96
JPEG_50	36.77	99.85	32.69	99.80	40.21	99.79
JPEG_10	32.93	99.09	30.42	99.05	35.36	98.84
JPEG_1	30.09	95.19	29.33	96.51	30.81	98.25
Crop_10 lines around	35.10	92.83	35.07	91.21	35.10	94.70
Translate_20 lines	28.13	85.25	27.74	83.24	27.93	82.24
Mixed attack (blur + sharp + JPEG)	30.55	97.70	29.14	97.24	32.70	98.46

Table 4 Comparison of effectiveness between existing schemes

Criteria/Scheme	Ours	[11]	[14]	[18]	[4]	[16]
Pixel Expansion	no	2	no	4	4	2
Column Equity	yes	no	yes	yes	yes	yes
Code Equity	yes	yes	no	yes	yes	yes
Color Equity	yes	no	no	yes	yes	no
Security	yes	no	no	yes	yes	no

- [4] R. Fu and W. Jin, "A wavelet-based method of zero-watermark utilizing visual cryptography," *The 2010 International Conference on Multimedia Technology (ICMT)*, pp. 1-4, 2010.
- [5] M. A. Hassan and M. A. Khalili, "Self watermarking based on visual cryptography," *World Academy of Science, Engineering and Technology*, vol. 8, pp. 159-162, 2005.
- [6] Y. C. Hou and P. M. Chen, "An asymmetric watermarking scheme based on visual cryptography," *Fifth Signal Processing Conference*, vol. 2, pp. 992-995, 2000.
- [7] Y. C. Hou and P. H. Huang, "Image protection based on visual cryptography and statistical property," *IEEE Statistical Signal Processing Workshop (SSP)*, pp. 481-484, 2011.
- [8] C. S. Hsu and Y. C. Hou, "A visual cryptography and statistics based method for ownership identification of digital images," *World Academy of Science, Engineering and Technology*, vol. 2, pp. 172-175, 2005.
- [9] R. Hwang, "Digital image copyright protection scheme based on visual cryptography," *Tamkang Journal of Science and Engineering*, vol. 3, no. 2, pp. 97-106, 2002.
- [10] F. Li and S. Wang, "New efficient proxy blind signature scheme using verifiable self-certified public key," *International Journal of Network Security*, vol. 4, no. 2, pp. 193-200, 2007.
- [11] D. C. Lou, H. K. Tso, and J. L. Liu, "A copyright protection scheme for digital images using visual cryptography technique," *Computer Standards and Interfaces*, vol. 29, pp. 125-131, 2007.
- [12] D. Mathivadhani and C. Meena, "Biometric based authentication using wavelets and visual cryptography," *IEEE International Conference on Recent Trends in Information Technology*, pp. 291-295, June 3-5, 2011.
- [13] N. Naor and A. Shamir, "Visual cryptography," *Advances in cryptology- Eurocrypt '94*, LNCS 950, pp. 1-12, 1995.
- [14] G. D. Park, E. I. Yoon, and K. Y. Yoo, "A new copyright protection scheme with visual cryptography," *The Second International Conference on Future Generation Communication and Networking Symposia*, pp. 60-63, 2008.



- [15] B. Surekha, G. N. Swamy, and K. S. Rao, "A multiple watermarking technique for images based on visual cryptography," *International Journal of Computer Applications*, vol. 1, no. 11, pp. 78-82, 2010.
- [16] S. F. Tu and Y. C. Hou, "On the design of visual cryptographic methods with smooth-looking decoded images of invariant size for gray level images," *Imaging Science Journal*, vol. 55, no. 2, pp. 90-101, 2007.
- [17] M. S. Wang and W. C. Chen, "Digital image copyright protection scheme based on visual cryptography and singular value decomposition," *Optical Engineering*, vol. 46, no. 6, pp. 1-8, 2007.
- [18] M. S. Wang and W. C. Chen, "a hybrid dwt-svd copyright protection scheme based on k-means clustering and visual cryptography," *Computer Standards and Interfaces*, vol. 31, no. 4, pp. 757-762, 2009.
- [19] Y. B Xing and J. H. He, "A new robust copyright Protection scheme for digital image based on Visual Cryptography," *The 2010 International Conference on Wavelet Analysis and Pattern Recognition*, pp. 6-11, Qingdao, 2010.
- [20] R. I. Zaghoul and E. F. Al-Rawashdeh, "HSV image watermarking scheme based on visual cryptography," *World Academy of Science, Engineering and Technology*, vol. 44, pp. 482-485, 2008.
- B. Surekha** received B. Tech degree in Electronics and Communication Engineering from Nagarjuna University (INDIA) in 2003, M.Tech degree in Digital Electronics and Communication Systems from Jawaharlal Nehru Technological University (INDIA) in 2007. Currently she is a research scholar in the department of Electronics and Communication Engineering at JNTUH (INDIA). From 2003 to 2005 she worked as Assistant Professor in ECE Department of PVP Siddhartha Institute of Technology (VIJAYAWADA). In 2007 she was lecturer in KS Institute of Technology (BANGALORE). Since 2008 she is working as Associate Professor in the Department of Electronics and Communication Engineering, TRR College of Engineering (HYDERABAD). Her areas of interest are Image Processing, Cryptography and Copyright Protection. She has published 8 research papers. She is a member of IETE, ISTE.
- G. N. Swamy** received B. Tech degree in Electronics and Communication Engineering from Nagarjuna University (INDIA) in 1991, M.Tech degree in Microwaves from BHU Varanasi University (INDIA) in 1993 and the Ph.D. degree in Signal Processing from Andhra University (INDIA) in 2006. From 1993 to 2006 he was Assistant Professor in ECE Department of VR Siddhartha Engineering College (VIJAYAWADA); from 2007 to 2011 he was Professor and Head of the Department in ECE Department of Gudlavalleru Engineering College (GUDLAVALLERU). Since 2012 he is working as a Professor in the Department of Electronics and Communication Engineering, VR Siddhartha Engineering College (VIJAYAWADA). His research interests include Electronic Devices, Microwaves, Signal Processing, Image Processing and Cryptography. He has several publications to his credit. He is actively associated with national professional bodies like IETE and ISTE, INDIA.