Watermarking Scheme for Color Images using Wavelet Transform based Texture Properties and Secret Sharing

Nagaraj V. Dharwadkar and B.B.Amberker

Abstract—In this paper, a new secure watermarking scheme for color image is proposed. It splits the watermark into two shares using (2,2)- threshold Visual Cryptography Scheme (VCS) with Adaptive Order Dithering technique and embeds one share into high textured subband of Luminance channel of the color image. The other share is used as the key and is available only with the super-user or the author of the image. In this scheme only the super-user can reveal the original watermark. The proposed scheme is dynamic in the sense that to maintain the perceptual similarity between the original and the watermarked image the selected subband coefficients are modified by varying the watermark scaling factor. The experimental results demonstrate the effectiveness of the proposed scheme. Further, the proposed scheme is able to resist all common attacks even with strong amplitude.

Keywords-VCS, Dithering, HVS, DWT.

I. INTRODUCTION

N recent years Copyright protection and authentication L of digital data using watermarking is an intense issue of research. The basic principle of digital watermarking technique [1] is to embed an amount of secret information in the functional part of the cover data. This data may be an image, an audio or video. Since mid 1990s this technique has attracted much attention from academic and industrial sector. After the pioneering contribution by I. J. Cox [1], digital watermarking techniques have been widely developed as an effective tool against piracy, illegal alteration of contents or improper use of image. In image watermarking, the major constraint for a watermark embedded into cover image is robustness against manipulations, including different variety of digital and analog processing operations. Other constraints are maintaining the perceptual similarity between original and watermarked image, embedding capacity etc. Human Visual System (HVS) plays important role in watermarking of images to maintain the perceptual similarity between original and watermarked image. HVS has been characterized with several phenomena that permits to adjust the pixel values to yield perception. These phenomena are luminance sensitivity, frequency sensitivity and texture sensitivity. Human visual model is based on the characteristics such as edges and textures, which are incorporated to determine the gain factor in watermarking [2]. The distortion

Nagaraj V. Dharwadkar is full time PhD research scholar in computer Science and Engineering department at National Institute of Technology, Warangal. His research area is Digital image watermarking and Image security. E-mail: nvd@nitw.ac.in.

B.B.Amberker is Professor in the department of computer Science and Engineering at National Institute of Technology, Warangal. E-mail: bba@nitw.ac.in

visibility is very low if the back ground contains texture. In a high texture block, energy is more distributed among the pixels. Therefore, the block having a stronger texture can have a high embedding gain factor.

The classification of watermarking algorithm is done on several view points. One of the viewpoints is based on usage of cover image to decode the watermark. If the cover image is used to decode the watermark then it is known as nonblind or private watermarking algorithm. If the cover image is not used to decode the watermark, then it is known as Blind or public watermarking algorithm. Another view point is based on processing domain such as spatial domain or frequency domain. Many techniques have been proposed in the spatial domain, such as the LSB (Least Significant Bit) insertion. These methods usually have features of less computation and large embedding gain, but they are less robust. The techniques found in frequency domain uses transforms such as Discrete Cosine Transform (DCT), Discrete Fourier Transform (DFT) and Discrete Wavelet Transform (DWT). Generally, a watermark embedded in the frequency domain is more robust than that in the spatial domain. The frequency domain transform techniques are more popular due to the natural framework for incorporating perceptual knowledge into the embedding algorithm which achieves better perceptual quality and robustness [1]. There are many ways to embed the watermark into cover image using DWT. In [3], the watermark is embedded into discrete wavelet subband coefficients of known robustness (usually large coefficients) or into perceptual significant regions such as contours and textures of an image. In [4] the watermark is embedded by selecting larger coefficients and using threshold scheme. Another approach of embedding is to insert the watermark by considering variable strength of each coefficient[5].

Visual cryptography Scheme (VCS) is an emerging cryptography technology, which uses the characteristics of Human Visual System to encrypt and decrypt images without requirement of complex computation [9]. Earlier days the VCS is used in only secret sharing applications, but in the recent years the VCS scheme is also used in protecting the copyrights of the images using watermarking. In the year 2000, Young-Chang [10] proposed an asymmetric Watermarking Scheme based on Visual Cryptography. In this scheme the watermark to be embedded is first split into two shares. One share is embedded into a cover-image to produce a stego-image. The other share is the key to extract the watermark. The stego-image can be transmitted on the internet and the key is held

by the copyright owner of this stego-image. The extraction of watermark is done by superimposing the key over the stego-image. In this method the watermark is embedded in spatial domain and image filtration may reduce the strength of watermark inserted. The watermarked image produced by this algorithm is highly distorted compared to the original cover image. If the cropping is applied in the location where watermark exists, then it is tough to justify the copy rights of the owner. In the year 2006, Shang-Lin Hsieh [11] proposed a method similar to one proposed by [10] but embedding of one share is in frequency domain. Moreover, this method adopts the value of Just Noticeable Distortion features as an embedding scaling factor to embed the share image in the color image.

In this paper, we propose a blind watermarking scheme that operates in the frequency domain. The watermark is masked according to the characteristics of the human visual system (HVS), taking into account the texture and the luminance content of the image subbands. We apply wavelet transformation on Luminance channel of color image and get the first level decomposition. From this a subband having high texture energy is selected. On this subband, apply DWT to obtain second level decomposition. From this, again select a subband having high texture energy and then embedd the watermark. After embedding the watermark the texture properties of modified subband coefficients are recalculated to decide the noticeable distortions of image. If the change in texture property is high, then the embedding scaling factor is adjusted until the texture distortion is negligible. Thus, to maintain the perceptual similarity between the original color image and watermarked color image the embedding scaling factor is adjusted dynamically. In this scheme, we use VCS-(2, 2) with Adaptive Order Dither Technique. Note that in our scheme, one of the share is directly embedded into cover image unlike in [11] where the share image is preprocessed using a transform before embedding. The main feature of our scheme compared to the scheme in [11] is that the watermark is not expanded by factor of 2. Experimental results demonstrate that there is high degree of perceptual similarity between original image and watermarked image. Further, the proposed scheme resist different types of attacks.

This paper is organized as follows. Section II briefly reviews the DWT and Texture properties of image using DWT. Section III briefly reviews the (k,n) Visual Cryptography Scheme for gray-scale images using Adaptive order Dithering. Proposed watermark embedding and extraction algorithm is given in Section IV. Results and discussion is given in Section V. Finally the paper is concluded in Section VI.

II. TEXTURE FEATURES EXTRACTION USING DWT

The term "texture" is used to represent the available detail in an image surface. It is characterized by "tone" (which refers to intensity) and "structure" (which refers to spatial relationships). There are two types of textures namely regular and irregular. Regular textures, as seen on a brick wall, can be composed out of a small building-block or primitive. Irregular textures, as seen on an image of clouds or grass, cannot be constructed by using a primitive and require statistical

techniques for their analysis [6]. Texture features typically consist of contrast, uniformity, coarseness and density. There are two basic methods of obtaining texture descriptors, namely, statistical model-based method and transform-based method. The following section briefly reviews the discrete wavelet transform and texture descriptors of image using wavelet transform.

A. Discrete Wavelet Transformation

Discrete Wavelet decomposition of image produces the multi-resolution representation of image. A multi-resolution representation provides a simple hierarchical framework for interpreting the image information. At different resolutions, the details of an image generally characterize different physical structures of the image. At a coarse resolution, these details correspond to the larger structures which provide the image context. The following section briefly reviews about Two Dimensional Wavelet Transformation.

1) Two Dimensional Wavelet Transform: In two dimensions Wavelet transformation, the wavelet representation can be computed with a pyramidal algorithm. The two-dimensional wavelet transform that we describe can be seen as a one-dimensional wavelet transform along the x and y axes. Mathematically the wavelet transform is convolution operation, which is equivalent to pass the pixel values of an image through a lowpass and highpass filters. A separable filter bank to the image is represented as follows:

$$L_n(\vec{b}) = [H_x * [H_y * L_{n-1}] \downarrow 2, 1] \downarrow_{1,2} (\vec{b})$$

$$D_{n1}(\vec{b}) = [H_x * [G_y * L_{n-1}] \downarrow 2, 1] \downarrow_{1,2} (\vec{b})$$

$$D_{n2}(\vec{b}) = [G_x * [H_y * L_{n-1}] \downarrow 2, 1] \downarrow_{1,2} (\vec{b})$$

 $D_{n3}(\vec{b}) = [G_x * [G_u * L_{n-1}] \downarrow 2, 1] \downarrow_{1,2} (\vec{b})$

Where * represents the convolution operator, $\downarrow 2, 1(\downarrow_{1,2})$ represents subsampling along the rows (columns) and $L_o = I(x)$ is the original image. H and G are the lowpass and bandpass filter respectively. L_n is obtained by lowpass filtering and is therefore referred to as low resolution image at scale n. The D_{nl} are obtained by bandpass filtering in a special direction and thus contains the directional detail information at scale n, they are referred to as the detail images. The original image I is thus represented by set of subimages at several scales; $\{\{L_d, D_{nl}\}|l=1,2,3,n=1,2,3,...,d\}$, which is multi-scale representation with depth d of the image I. The image is represented by two dimensional signal function, wavelet transform decomposes the image into four frequency bands, namely, the LL_1 , HL_1 , LH_1 and HH_1 bands. H and L denotes the highpass and lowpass filters respectively. The approximated image LL is obtained by lowpass filtering in both row and column directions. The detailed images, LH, HL and HH contains the high frequency components. To obtain the next coarse level of wavelet coefficients, the subband LL_1 alone is further decomposed and critically sampled. Similarly LL_2 will be used to obtain further decomposition. By decomposing the approximated image at each level into

(1)

u,	HL,	HL,
LH ₂	нн,	HL,
LH	l ₁	нн,

Fig. 1. Layout of individual bands at second level of DWT decomposition

four subimages forms the pyramidal image tree. This results in two-level wavelet decomposition of image as shown in the

Figure 1.

al (1973).

Secret image Sharel Share2 Stacked image

Fig. 2. Sharing and Stacking Scheme of Black and white pixel

Secret Image	Shares		OR		XOR				
() (Whitepitel)	1	0	Г	1	0	1	0	0	0
() (миерин)	1	0	,	1	0	1	0	0	0
(Blackpixel)	1	0	Г	0	1	1	1	1	1
(Diskpus)	1	0	,	0	1	1	1	1	1

Fig. 3. Comparison between OR and XOR based VCS

B. Texture Properties using Wavelet Transformation

The previous discussed two-level discrete wavelet analysis can be applied to input image, which generates the distinguishing frequency layers. It is found that at each resolution level three new feature channels are obtained which are characterized by the given scale depth, horizontal, vertical and the diagonal components. As the micro textures or macro textures have non-uniform pixel value variations, they are statically characterized by the features in approximation and detailed images. Thus the values in the sub-band images or derived features from these subbands uniquely characterize the texture properties [8], which are used to decide the subband for embedding watermark. The representative texture feature vectors are used for analyzing the image for watermarking. The various co-occurrence features such as energy, homogene-

ity and contrast at the output of each channel are calculated.

Following equations are used to calculate feature vector at

each level of decomposed image as suggested by Haralick et

$$Energy_l = \frac{1}{M \times N} \sum_{i=1}^{M} \sum_{j=1}^{N} I_l^2(i,j)$$
 (2)

$$Homogeneity_{l} = \sum_{i=1}^{M} \sum_{j=1}^{N} \frac{1}{1 + (i-j)^{2}} I_{l}(i,j)$$
 (3)

$$Contrast_{l} = \sum_{i=1}^{M} \sum_{j=1}^{N} (i-j)^{2} I_{l}(i,j)$$
 (4)

where, $I_l(i,j)$ denotes an image obtained in l^{th} subband and $l \in \{LL, LH, HL, HH\}$, with resolution of $M \times N$ having been determined by wavelet analysis.

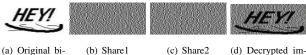
III. VISUAL CRYPTOGRAPHY SCHEME

Naor and Shamir first proposed a (k,n) Visual Cryptography scheme (VCS) to share a secret image [9]. In this scheme, a secret image is hidden into n share images and can be decrypted by superimposing at least k share images but any k-1 shares cannot reveal the secret. The (2,2)-VCS scheme is illustrated to introduce the basic concept of Visual cryptography Scheme. In the encryption process, every secret pixel is turned into two shares, and each share belongs to the corresponding share image. At last two share images are

obtained using (2,2) - VCS. In the decryption process, two corresponding shares are stacked together (using OR operation) to retrieve the secret pixel. The two shares of a white secret pixel are the same while those of a black secret pixel are complementary as shown in Figure 2. Consequently, a white secret pixel is represented by a share with the stacked result of half white sub-pixels, and a black secret pixel is all black. Using this basic VCS Scheme we cannot completely recover the white Secrete pixel, that causes loss in contrast. XOR based VCS scheme where the share images are superimposed using XOR operation, results in perfect reconstruction of both black and white pixels as shown in Figure 3 and by subsampling a 2×2 block into a single pixel, we get decrypted image of same size as original secret image. Figure 4 shows an example of (2,2) - VCS scheme, where the share images are 2×2 times larger than the original secret image.

A. VCS for Gray-scale images

After the introduction of visual cryptography by Naor and Shamir many algorithms for visual cryptography were proposed, but they are limited to binary images only. Visual cryptography for gray level image is seldomly discussed. A (k,n) threshold visual cryptography for gray-level image [12], whose pixels have g gray levels ranging from 0 (representing a white pixel) to g-1 (black pixel) where each pixel is



image

(c) Share2

(d) Decrypted image using OR operation



(e) Decrypted image using XOR operation and Subsample

Fig. 4. Example of (2,2) VCS scheme for binary image

expanded to m subpixels of size $m \geq g(k-1)$ is proposed. Here the size of decoded image is larger than the secret image compared to Naor and Shamir VCS scheme. In order to reduce the size of decrypted image, the Space-Filling Curve Ordered Dither (SFCOD) technique [14] is first used to convert the given gray-level image into binary image, then existing visual cryptography scheme for binary image is applied [13]. Using this technique the reduction of size of decrypted image is achieved but the quality of decrypted image depends on the halftone image and the quality of halftone image depends on the cluster length used for halftone.

B. VCS for Gray-scale images Using Adaptive Order Dithering

The reduction in size of decrypted image is archived using (k,n) threshold Visual cryptography scheme for gray level images using SFCOD technique. But the quality of decrypted image depends upon the quality of halftone image. In order to achieve both properties we propose to use Adaptive Order Dither (AOD) technique during halftones and then apply existing VCS scheme for binary image to accomplish the creation of shares. Adaptive order Dither technique does the halftones of gray-level image by using a space-filling curve to perform an adaptive variation of the cluster size and inherits the advantages of the SFCOD and the stochastic screening dithering method [15][16]. The proposed (2,2)-threshold VCS using AOD for the gray-scale watermark can be summarized as follows:

1) Creation of Shares of watermark:: The creation of shares of watermark is achieved using the following steps:

1.Halftoning using AOD: Using AOD halftone technique [15], the gray-scale watermark image I is changed into approximate binary image or halftone image I_{hft} .

$$[I] - Halftoning(AOD) \rightarrow [I_{hft}]$$
 (5)

2.Creation of shares: The method described in Section 3 is used to create the shares by considering the (2,2)-VCS scheme.

$$[I_{hft}] - (2,2) - VCS \rightarrow [S_0, S_1]$$
 (6)

Where, S_0, S_1 are shares of I_{hft} image.

2) Recovering the Watermark:: The original watermark image is reconstructed by stacking binary shares. The stacking (XOR) operation is performed to get recovered watermark image. We used XOR operation for stacking share image to get better decrypted image and subsampling 2×2 block into a single pixel produces a decrypted image with same size as original image.

$$[S_0, S_1] - Stacking(XOR) \rightarrow [I]$$
 (7)

IV. PROPOSED MODEL

The highest energy subband of Luminance channel of the color image is used for embedding the watermark. Before embedding the watermark, the watermark is split into two shares by applying Visual cryptography Scheme (VCS) using Adaptive Order Dither Technique. One of these binary share

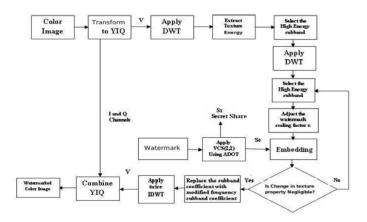


Fig. 5. Watermark Embedding algorithm

is embedded into cover image where as the other share is kept secret. The watermark embedding and extraction algorithms are explained in the following section.

A. Watermark Embedding Algorithm

Figure 5 shows the watermark embedding algorithm. The embedding algorithm uses color image as cover and grayscale image as watermark. The color image is decomposed into Luminance, Intensity and Hue channels. The DWT is applied on the Luminance channel of color image, which produces the frequency subband coefficients. From these subband coefficients the highest texture energy subband is selected. On this subband apply DWT to obtain the second level decomposition. From this again select a subband having high texture energy. Before embedding the watermark into selected subbands, the watermark image is split into two shares by applying (2,2)-VCS scheme using AOD as explained in Section 3. Out of these two shares one share is embedded into selected subband and other share is kept secret. The details of the algorithm is as follows:

Algorithm: Watermark Embedding Algorithm.

Input : Cover (Color) image, Watermark (gray-scale) image. Output : Watermarked color image.

- 1) Read the cover (color) image I of size $N \times N$ and watermark (gray-scale)image W of size $M \times M$
- 2) Decompose the color image into Luminance (Y), Intensity (I) and Hue (Q) channels of size $M \times M$
- 3) Split the watermark by applying (2,2)-VCS using AOD, as explained in Section 3 using equations (7) and (8) which produces two shares (S_0,S_1) , where share S_0 is kept secret and S_1 is used for embedding.
- 4) Apply DWT on Luminance (Y) channel to get subband coefficients $(LL_1, LH_1, HL_1 \text{ and } HH_1)$.
- 5) Extract the texture property *Energy* for each subband coefficient using equations (4)
- Select the subband frequency coefficients (LL₁ or LH₁ or HL₁ or HH₁) which is having high energy.
- 7) Apply the DWT on selected subband to get second level decomposition $(LL_2, LH_2, HL_2 \text{ and } HH_2)$

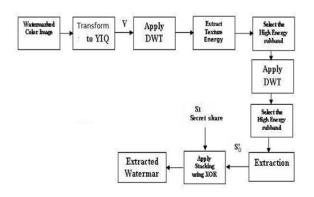


Fig. 6. Watermark Extraction algorithm

- Extract the vector of texture property Energy for each subband of second level decomposition, using equations
 (4)
- 9) Select the subband which is having high energy from second level decomposition (LL_2 ,or LH_2 or HL_2) or HH_2).
- 10) Embed the share S_1 produced in Step 3 into the selected subband coefficients of Step 9 using following steps.

```
\begin{array}{l} \mbox{for } i=1 \mbox{ to } M \mbox{ do} \\ \mbox{for } j=1 \mbox{ to } M \mbox{ do} \\ \mbox{$Y'(i,j)=(|Y(i,j)|+\alpha)S_1(i,j)$} \\ \mbox{end for} \\ \mbox{end for} \end{array}
```

Where Y'(i,j) represents the modified frequency coefficient of subband, Y(i,j) represents the original frequency coefficient of subband, α represents the watermark scaling factor.

- 11) The value of α is adjusted such that the texture properties of embedded subband are changed by negligible value
- 12) Replace the modified subband coefficients into its initial location and apply twice inverse DWT to get the watermarked Luminance channel.
- 13) Combine the watermarked Luminance (Y) channel with Intensity (I) and Hue (Q) to get watermarked color image.

B. Watermark Extraction Algorithm

Figure 6 shows the watermark extraction algorithm. Extraction algorithm is of type blind extraction which uses only watermarked color image as input. The watermarked color image is decomposed into Luminance, Intensity and Hue channels. The DWT is applied on the Luminance channel of watermarked color image, which produces the frequency subband coefficients. From these subband coefficient the highest texture energy subband is selected. On this subband apply DWT to obtain the second level decomposition. From this again select a subband having high texture energy. The watermark is extracted from these selected subband coefficients. After extracting the watermark, the watermark image is superimposed

with secret share using (2,2)-VCS scheme as explained in Section 3. The output of superimposition produces the extracted watermark. The details of the extraction algorithm is explained below.

Algorithm: Watermark Extraction Algorithm.

Input: Watermarked (Color) image.

Output: Extracted watermark.

- 1) Read the watermarked color image I of size $N \times N$
- 2) Decompose the watermarked color image into Luminance (Y), Intensity (I) and Hue (Q) channels of size $M\times M$
- 3) Apply DWT on Luminance (Y) channel to get subband $(LL_1, LH_1, HL_1 \text{ and } HH_1)$.
- Extract the texture property Energy for each subband coefficients.
- Select the subband frequency coefficients (LL₁ or LH₁ or HL₁ or HH₁) which is having high energy.
- Apply the DWT on selected subband to get second level decomposition subbands(LL₂, LH₂, HL₂ and HH₂)
- 7) Extract the texture property Energy for each subband of second level decomposition.
- 8) Select the subband frequency coefficients which is having high energy from second level (LL_2 ,or LH_2 or HL_2 or HH_2).
- Extract the share S'₁ from selected subband coefficients of Step 9 using following steps.

```
\begin{array}{l} \textbf{for} \ i=1 \ \textbf{to} \ M \ \textbf{do} \\ \textbf{for} \ j=1 \ \textbf{to} \ M \ \textbf{do} \\ \textbf{if} \ \ Y' \gg 0 \ \textbf{then} \\ S_1'(i,j)=1; \\ \textbf{else} \\ S_1'(i,j)=0; \\ \textbf{end} \ \textbf{if} \\ \textbf{end} \ \textbf{for} \\ \end{array}
```

10) Superimpose extracted share S_1' with secret share S_0 using (2,2)-VCS as explained in Section 3, using equation (9) which produces the extracted watermark.

V. RESULTS AND DISCUSSION

To verify the effectiveness of the proposed scheme, a series of experiments were conducted. In these experiments, we used a set of color images of different sizes with 8 bit color representation. Figure 7 shows color images of Bird, Boat, Girl, Rose, Lena, House, Peppers and Tree, which are used in our experiments. The Bird, Boat, Girl, Rose, Lena, House, Peppers and Tree images are of size 575×379 , 256×256 , $256 \times 256,\ 370 \times 278,\ 256 \times 256,\ 256 \times 256,\ 256 \times 256$ and 256×256 respectively. The watermark used is a gray-scale image of size 40×40 . For the extraction of texture features we used biorthogonal wavelets. Figure 8 shows the watermarked color images obtained using our algorithm. Figure 9 shows the watermark used in our algorithm along with the two shares of the watermark obtained by (2,2)-VCS. The extracted share and the watermark produced by stacking of extracted share and secret share also shown in this figure.

In order to measure the distortion occurred by the embedding algorithm we have used Mean Square Error (MSE) and Peak Signal to Noise Ratio (PSNR) between original and watermarked color images. The quality of extracted watermark is measured by calculating the Normalized Correlation (NC) and Standard Correlation (SC) between extracted and original watermark. The MSE, PSNR, NC and SC are calculated using following equations.

Mean Square Error (MSE):

$$MSE = \frac{\sum_{R,G,B} \sum_{i=1}^{M} \sum_{j=1}^{N} \left(I[i,j] - I'[i,j]\right)^{2}}{3MN}$$

Here, M and N are the height and width of image respectively. f(i,j) is the $(i,j)^{th}$ pixel value of the original image and f'(i,j) is the $(i,j)^{th}$ pixel value of watermarked image.

Peak signal to noise ratio (PSNR):

$$PSNR = \log \frac{(2^n - 1)^2}{MSE}$$

Where n is the number of bits used for color representation. **Normalized Correlation (NC)**:

$$NC = \frac{\sum_{i=1}^{M} \sum_{j=1}^{N} (I[i,j]I'[i,j])}{\sum_{i=1}^{M} \sum_{j=1}^{N} (I[i,j])^{2}}$$

Where I(i, j) is the original image and I'(i, j) is the modified image, M is height of the image and N is width of the image. **Standard Correlation (SC) :**

$$SC = \frac{\sum_{i=1}^{M} \sum_{j=1}^{N} (I[i,j] - I') (J[i,j] - J')}{\sqrt{\sum_{i=1}^{M} \sum_{j=1}^{N} (I[i,j] - I')} \sqrt{\sum_{i=1}^{M} \sum_{j=1}^{N} (J[i,j] - J')}}$$

Here, I(i,j) is original watermark, J(i,j) is extracted watermark, I^\prime is the mean of original watermark and J^\prime is mean of extracted watermark

Table I shows the values of MSE and PSNR between the original and watermarked images and the value of watermark scaling factor α used in embedding algorithm. The watermark scaling factor α is dynamically adjusted and fixed for each image such that the texture quality of image is changed by a negligible value.

Table II shows the values of texture energy for different images at different levels of DWT decompositions for both original images and watermarked images, where V_1 , V_2 represents the vertical subbands at first and second level decomposition, H_1 , H_2 represents the horizontal subbands at first and second level decomposition and D_1 , D_2 represents the diagonal subbands at first and second level decomposition. From this table it can seen that texture properties are modified by negligible values. Table III shows the values of NC and SC between the original and extracted watermark for a set of color images. The results shows that the extracted watermark is highly correlated to the original watermark.

A. Effects of Attacks on watermarking algorithm

Now, we discuss different attacks on watermarked color image such as blurring, adding salt and pepper noise, sharpening, Gaussian filtering and cropping. Figure 10 shows the set of extracted watermark from the image, when the watermarked image is under different types of attacks.

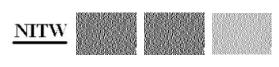


Fig. 7. A set of color images used for embedding watermark



Fig. 8. A set of watermarked color images

1) Effect of Blurring on Watermarked Image: Special type of circular averaging filter is applied on the watermarked color image to analyze the effect of Blurring. The circular averaging (pillbox) filter is applied, which filters the watermarked image within the square matrix of side $2\times(DiskRadius)+1$. The disk radius is varied from 0.5 to 1.5 and the effect of blurring is analyzed on extraction algorithm. Performance of algorithm is decided by calculating NC and SC between extracted watermark and original watermark. Figure 11 shows the effect of blurring on watermarked images in terms of NC and SC



(a) Original (b) Secrete (c) Share used (d) I watermark Share for embedding Share

NITW

(e) Extracted share superimposed with secret share to produce the watermark

Fig. 9. Watermark used in our algorithm



(a) Blurring (b) Salt and (c) Sharpening (d) 30 percentwith Disk pepper Noise with sharpness age of Cropradius of 1.1 with density of 0.8 ping 0.005



(e) Gaussian filtering of image

Fig. 10. Extracted watermark from different types of attacked color images

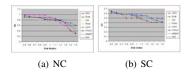


Fig. 11. Effect of Blurring on watermarked images in terms of NC and SC between original and extracted watermark

between original and extracted watermark. The Blurring is applied on set of images by varying the disk radius from 0.5 to 1.5. It is found that the correlation between the extracted and the original watermark is nearly 0.5 at disk radius of 1.3. Thus the watermark algorithm is highly robust against blurring attack.

- 2) Effect of salt and pepper noise on Watermarked Image: The salt and pepper noise is added to the watermarked image I with the noise density d. This affects approximately $d \times$ (size(I)) pixels. The performance of the extraction algorithm is analyzed by increasing the density of noise starting from 0.001 up to 0.100. The extracted watermark and the original watermark are compared in terms of NC and SC. Figure 12 shows the effect of salt and pepper noise on watermarked images in terms of NC and SC between original and extracted watermark. The salt and pepper noise is added to a set of watermarked images by increasing the noise density from 0.001 to 0.100. From these experimental results it is found that the correlation between the extracted and the original watermark is nearly 0.5 at noise density of 0.005. Thus the watermark algorithm is highly robust against the attack of adding salt and pepper noise to the watermarked image.
- 3) Effect of Sharpening on Watermarked Image: A special type of 2D un-sharp contrast enhancement filter is applied on the watermarked color image. The un-sharp contrast enhancement filter enhances edges, and other high frequency com-

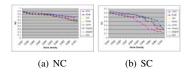


Fig. 12. Effect of salt and pepper noise on watermarked images in terms of NC and SC between original and extracted watermark

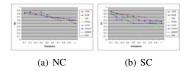


Fig. 13. Effect of sharpening on watermarked image in terms of NC and SC between original and extracted watermark

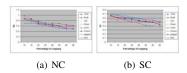


Fig. 14. Effect of cropping on watermarked image in terms of NC and SC between original and extracted watermark

ponents in an image, by subtracting a smoothed ("un-sharp") version of an image from the original image. The sharpness parameter is varied from 0.1 to 1 and the performance of extraction algorithm is analyzed by calculating NC and SC between the original watermark and the extracted watermark. Figure 13 shows the effect of sharpening on watermarked images in terms of NC and SC between original and extracted watermark. The 2D contrast enhancement filter is applied on the set of watermarked images by increasing the sharpness parameter from 0.1 to 1. From these experimental results it is found that sharpenning of the watermarked image of upto to 0.8 sharpness parameter, the extraction algorithm produces the highly corelated watermark with the original.

- 4) Cropping of Watermarked Image: The watermarked image is cropped in terms of percentage of the image size. The cropping is started at 10 percentage and continued in the intervals of 5 percentage up to 50 percentage. The effect of cropping on the extraction algorithm is analyzed by comparing the extracted watermark and the original watermark in terms of NC and SC. Figure 14 shows the effect of cropping on watermarked images in terms of NC and SC between original and extracted watermark. The cropping is applied on a set of watermarked images by increasing the cropping from 10 to 50 percentage. From the experimental results it is found that extraction algorithm produces the highly correlated watermark up to 50 percentage of cropping.
- 5) Gaussian filters on Watermarked Image: Two dimensional Gaussian filter is applied on the watermarked images with standard deviation sigma (positive) varying from 0.1 to 1. The effect of Gaussian filter is analyzed by calculating NC and SC between the extracted and the original watermark. Figure 15 shows the effect of Gaussian filter on watermarked images in terms of NC and SC between original and extracted watermark. The Gaussian filter is applied on a set of watermarked images by increasing the standard deviation from 0.1 to 1. From the experimental results it is found that the extraction algorithm produces the highly correlated watermark at standard deviation of 0.6.

VI. CONCLUSION

In this paper we used the texture properties of color image to select the subband coefficient of image to embed the

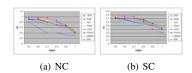


Fig. 15. Effect of Gaussian filter on watermarked image in terms of NC and SC between original and extracted watermark

TADIE

The watermark scaling factor α used for different images and $MSE,\,PSNR$ between original and Watermarked color images

Color Image	α	MSE	PSNR
Bird	0.048	0.2	55.12
Boat	0.096	0.98	48.21
Girl	0.058	1.39	46.70
Rose	0.056	0.54	50.78
Lena	0.046	0.11	57.71
House	0.086	2.54	44.07
Peppers	0.058	0.26	54.05
Tree	0.060	1.40	46.65

watermark. This method dynamically selects the DWT based frequency coefficients subband for embedding the watermark. Application of (2,2)-VCS using AOD for splitting the watermark and XOR operation in superimposition produces the less distorted and same size watermark. The experimental results shows that our scheme is robust and withstand many attacks. Further, the proposed scheme can be enhanced for multiusers using (k,n)-VCS in which n key shares are distributed to n users such that the knowledge of k or more shares are required to recover the watermark.

REFERENCES

- I.J. Cox, M.L. Miller and J. A. Bloom, J. Fridrich, T. Kalker, Digital Watermarking and Steganography, Second edition, Morgan Kaufmann Publishers, 2008.
- [2] Ching-Tang Hsieh, Yeh-Kuang Wu, Digital Image Multiresolution Watermark Based on Human Visual System Using Error Correcting Code, Tamkang Journal of Science and Engineering, Vol. 4, No. 3, 2001, pp. 201-208.

TABLE II
ENERGY VALUE OF ORIGINAL AND WATERMARKED COLOR IMAGES FOR
DIFFERENT SUBBANDS

Image	V_1	V_2	H_1	H_2	D_1	D_2
Original Bird image	16.39	4.97	30.12	14.4	0.65	3.14
Watermarked Bird image	16.39	4.98	31.16	15.40	0.65	3.14
Original Boat image	49.14	23.53	60.03	15.62	7.0	6.05
Watermarked Boat image	49.14	24.34	64.84	15.61	7.01	6.05
Original Girl image	8.5	3.1	6.87	1.12	0.19	0.67
Watermarked Girl image	10.3	4.45	6.85	1.13	0.19	0.67
Original Rose image	15.06	3.21	9.34	1.48	0.46	0.33
Watermarked Rose image	16.01	4.39	9.36	1.48	0.46	0.33
Original Lena image	39.8	11.82	14.64	13.67	3.53	3.86
Watermarked Lena image	40.08	11.81	14.65	14.47	3.53	3.86
Original House image	5.61	1.34	20.8	7.15	0.32	0.43
Watermarked House image	5.62	1.34	19.85	8.42	0.32	0.43
Original Peppers image	23.51	6.53	23.3	8.73	3.07	1.84
Watermarked Peppers image	24.82	6.54	23.31	9.49	3.07	1.83
Original Tree image	21.95	10.17	63.99	17.62	2.6	2.81
Watermarked Tree image	21.96	10.17	65.23	18.45	2.6	2.82

TABLE III
NC AND SC BETWEEN EXTRACTED AND ORIGINAL WATERMARK FROM
DIFFERENT COLOR IMAGES

Color Image	NC	SC
Bird	0.97	0.87
Boat	0.95	0.88
Girl	0.88	0.89
Rose	0.89	0.89
Lena	0.89	0.85
House	0.86	0.88
Peppers	0.88	0.85
Tree	0.89	0.84

- [3] Cox, I. Robust watermarking, ENCRYPT Summer School on Multimedia Security, Salzburg, Austria, Sept. 22, 2005.
- [4] Podilchuk, C., Zeng, W.,Image-Adaptive Watermarking Using Visual Models, IEEE Journal on Selected Areas in Communications, Issue 16, vol.4, 1998, pp. 525-539.
- [5] Barni, M., Bartolini, F., Piva, A Improved wavelet-based watermarking through pixel-wise masking, IEEE Transaction, Image Processing, Issue 10, vol. 5, 2001, pp. 783-791.
- [6] J. R. Smith and S. F. Chang., Automated Binary Texture Feature Sets for Image Retrieval, International Proceedings, International Conference on Acoustics, Speech, and Signal Processing, 1996, pp. 2241-2246.
- [7] Mallat,S., A theory for multiresolution signal decomposition: the wavelet representation, IEEE Transaction. Pattern Analysis and Machine Intelligence, vol.11, No.7, 1989, pp. 674-693.
- [8] S. Arivazhagan, L. Ganesan, Texture classification using wavelet transform, Elsevier, Pattern Recognitation letter.24, 2003, pp.1513-1521.
- [9] M. Naor, A. Shamir, Visual cryptography, Advances in Cryptology, Eurocrypt 94, Lecture Notes in Computer Science, Vol. 950, 1995, pp. 1-12.
- [10] Young-Chang Hou, Pei-Min Chen, An Asymmetric Watermarking Scheme based on Visual Cryptography, IEEE Proceedings of ICSP, 2000, pp. 992-995.
- [11] Shang-Lin Hsieh, I-Ju Tsai, Bin-Yuan Huang, and Jh-Jie Jian, Protecting Copyrights of Color Images using a Watermarking Scheme Based on Secret Sharing and Wavelet Transform, Journal of Multimedia, vol. 3, No. 4, 2008, pp. 42-49.
- [12] Verheul, Van Tilborg, Construction and Properties of k out of n visual secret sharing scheme Designs, Codes and Cryptography, Vol. 11, 1997, pp. 179-196.
- [13] C. Lin, T.H. Tsai, Visual cryptography for gray-level images by dithering techniques, Pattern Recognition Letters 24, 2003, pp. 349-358.
- [14] Yuefeng Zhang, Space-Filling Curve Ordered Dither, Elsevier, Computer & Graphics Journal, Vol. 22, No. 4, 1998, pp. 559-563.
- [15] Yuefeng Zhang, Adaptive Ordered Dither, Graphical, Models and Image Processing, Vol. 59, No. 1, 1997, pp. 49-53.
- [16] L.Velho and J.Gomes, Stochastic screening dithering with adaptive clustering, Proceedings of SIGGRAPH-95, ACM Computer Graphics, Annual Conference Series, 1995, pp. 273-276.

Nagaraj V. Dharwadkar:



He obtained B.E. in Computer Science and Engineering in 2000 and M.Tech. in Computer Science and Engineering in the year 2006. He is Assistant Professor in Computer Science and Engineering department at B.L.D.E.A's college of Engg. & Tech. Bijapur, Karnataka. Presently he is pursuing full time PhD in the Department of Computer Science and Engineering at National Institute of Technology, Warangal. His research area is Digital Image Watermarking and Visual Cryptography. E-mail: nvd@nitw.ac.in

B.B.Amberker:



He obtained Ph.D from the Department of Computer Science and Automation, IISc., Bangalore, India. He is presently working as Professor in the Department of Computer Science and Engineering at National Institute of Technology, Warangal, AP, India. His research areas of interest are Computational Number Theory and Cryptography, Authentication Schemes, Secure Group Communication, Image watermarking and image security. Email: bba@nitw.ac.in.