Visual Secret Sharing Based Digital Image Watermarking

B. Surekha [1], Dr. G. N. Swamy [2]

**[1] Associate Professor, Department of ECE, TRR College of Engineering,
Hyderabad, Andhra Pradesh, INDIA - 502 319.**

**[2] Professor, Department of ECE, VR Siddhartha Engineering College,
Vijayawada, Andhra Pradesh, INDIA -520007.**

Abstract

In this paper, a spatial domain image watermarking technique based on Visual Secret Sharing (VSS) and unique statistical properties is proposed. A random looking image is generated during watermark hiding process and is secretly registered with an arbitrator for verification during conflicts. Another random looking image is generated during watermark revelation stage and is combined with the existing one, to recover the watermark. This whole process is done without altering the image to be protected and hence the quality of the cover image is high. When compared with similar existing techniques, the proposed technique has three main advantages: Provides greater convenience in carrying and storing the intermediate images called shares; Provides high security; Reduce tradeoff between spatial and frequency domain techniques in terms of robustness.

Keywords: *Copyright Protection, Digital Watermarking, Secret Sharing, Visual Cryptography.*

1. Introduction

The E-commerce has grown enormously, because of the wide spread databases and web technologies. This has lead to easy availability and forgery of multimedia data. Therefore the data owners are in a need to trace the illegal distribution of their data and to prove their copyrights.

Digital Watermarking is a technique that combines the copyright information with the data (usually image or video) to be copyright protected. Later, when the owner wants to prove his copyrights, he can do it so by extracting the watermark from the watermarked data. Several criteria [1] for example Imperceptibility, Robustness, Security, Capacity and Complexity decide the performance of any watermarking technique.

Traditional watermarking techniques physically embed the watermarks into the cover images and hence fail in resolving the tradeoff between imperceptibility, capacity and robustness. To solve this problem, some researchers used the concept of Visual Secret Sharing (VSS) to hide and judge the ownership rights without altering the cover image. Instead of physically embedding the watermark into the cover image, this approach hides it using random patterns of binary images called shares. This approach is particularly suitable in protecting sensitive images like military, medical and satellite images.

Visual Secret Sharing (VSS) [2] is an image secret sharing scheme introduced by Naor and Shamir in mid 90's. It has the ability to decode the encoded data by Human Visual System (HVS). A *(k, n)* threshold VSS splits a secret image into *n* shares using a codebook such that any *k* out of *n* share images can be used to restore the secret image by stacking one above the other. VSS based watermarking techniques in [3-12] works as follows: Given a grey level cover image and a binary watermark, a feature vector is computed from the cover image. A secret key and a method of comparison 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 basic VSS to create a noise looking binary image, called private share. This share is time-stamped and is registered with a Certified Authority (CA). During copyright verification, a similar process is used to extract another binary image called public share from the claimed image using the same secret key. It is then combined with the private share to judge the copyrights.

The schemes in [3-6] use the above approach to hide watermarks in frequency domain. Though they are robust, watermark hiding in spatial domain [7-12] is much simple. It is to be noted that, even if all the properties of the watermarking are satisfied the 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.

Hwang’s [10] spatial domain technique of watermarking uses Most Significant Bits (MSB’s) as the feature vector. The security of this scheme is analyzed by Hassan et al. in [8] and proved that it leads to higher probability of false alarm and leads to ambiguity in copyright verification. Hsu et al. [7] used the theories and properties of sampling distribution of means (SDM) to reduce the false probability. Zaghloul et al. [11] extended Hwang’s scheme to hide a binary watermark into a color image by using features extracted from histograms of HSV planes of the cover 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. In [12] the results of comparing two pixels that are selected randomly from the cover image are used to determine the feature vector.

In this paper, a spatial domain digital watermark hiding technique based on Visual Secret Sharing (VSS) and unique statistical properties is proposed. A random binary image is generated during watermark hiding process and is secretly registered with an arbitrator for further verification during conflicts. Another random image is generated during watermark revelation process and combined with the existing one, to recover the watermark. This whole process is done without altering the image to be protected and hence the quality of the cover image is high. When compared with similar existing techniques, the proposed technique has three main advantages. 1. Since unique features of the cover image are used, it reduces the chances of false positives there by improving the security of the watermarking scheme 2. Since a modified version of VSS called Multi-Pixel VSS (MPVSS) with no pixel expansion, is used, it is convenient to carry and store the intermediate images called shares. 3. Since the chosen feature vector depends on spatial correlation of pixels, it reduces tradeoff between spatial and frequency domain techniques in terms of robustness against range of attacks.

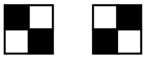
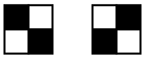
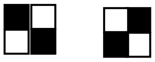
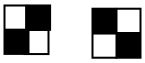
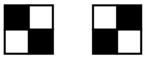
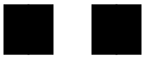
The rest of the paper is organized as follows. Section2 briefly reviews basic Visual Secret Sharing (VSS) in detail, Multi-pixel VSS (MPVSS) and Color Correlation Table (CCT). Section3 describes the proposed watermark hiding and revelation procedures. Simulation results are illustrated in Section4.

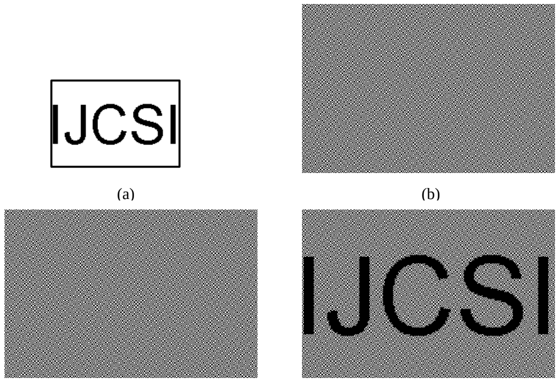
2. Preliminaries

2.1 Basic Visual Secret Sharing (VSS)

The basic VSS splits a binary secret image into two binary noise images called shares. The shares are generated in such a way that for each pixel in the secret image, a code block consisting of four sub-pixels is substituted in each of the shares using a codebook given in Table 1. Each code block has half white and half black sub-pixels, independent of whether the corresponding pixel in the secret image is black or white. 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 a 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 a code block.

Table 1: Codebook of basic VSS

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



(a) (b) (c) (d)

Fig. 1 Example of basic (*2, 2)* VSS
(a) Secret image (b) Share1 (c) Share2 (d) Decoded image

The results of basic VSS are shown in Fig.1. Here, all the pixels are encoded using independent random selection of columns. Thus no information is obtained by observing any group of pixels on each share. To decode the secret image, each of these shares has to be xeroxed onto transparent sheets. Stacking both these sheets will reveal the original secret. When the two shares are stacked one above the other, as in Fig.1.d, the black pixels in the original image remain black and the white pixels turns gray.

Note that in basic VSS, the size of each share is four times the original image. This is because each pixel in the original image is replaced with a code block consisting of four sub-pixels in each share. To reduce the size of each share the proposed watermarking scheme exploits a modified VSS with codebook shown in Table 2. Note that, instead of coding a single pixel each time, MPVSS 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. Each code-block has one white and one black sub-pixel, independent of the pair of pixels in the secret image. 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.

The results of using a modified codebook are shown in Fig. 2. Note that the decoded image in Fig. 2d is exactly same in size and contrast as the original secret image.

Table 2: Codebook used in MPVSS

Pixel	**WW**		**BB**	
Prob.	**50%**	**50%**	**50%**	**50%**
Share1	■□	□■	■□	□■
Share2	■□	□■	□■	■□
Share1 + Share2	■□	□■	■■	■■

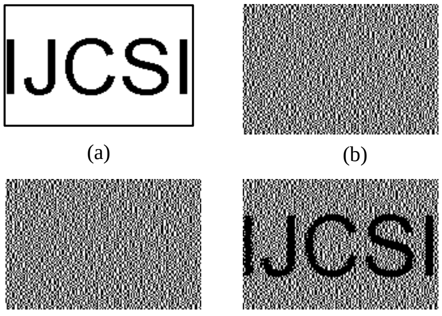


Fig. 2 Example of MPVSS
(a) Secret image (b) Share1 (c) Share2 (d) Decoded image

2.2 Color Correlation Table (CCT)

CCT is extracted from the image by constructing a table consisting of *k* rows and *t* columns, where *k* indicates the total number of colors in the given image and *t* indicates the distance between any two pixels in an image. The distance measure used here is D_8 distance. Hence maximum distance is one less than the number of rows or columns of the given image, whichever is max. The i^{th} entry in j^{th} row indicates the probability of finding a pixel of color c_j at a distance *i* from a pixel of same color in the image. This image feature robustly survives against attacks related to large changes in shape and appearance.

For an image of size $n\times n$ pixels and *k* colors, the size of the SCC table is $k\times n\text{-}1$. The D_8 distance between any two pixels p_1 and p_2 with coordinates (x_1, y_1) and (x_2, y_2) is given by

$$p_1 - p_2 = \max\{|x_1 - x_2|, |y_1 - y_2|\} \tag{1}$$

3. The Proposed Scheme

Unlike traditional watermarking schemes, the proposed scheme doesn't actually embed the watermark into the cover image. Instead, the features of cover image are used to hide a binary watermark by splitting it into two binary noise images: private share and public share. The private share is constructed during watermark hiding phase, and a public share is extracted from the claimed image during watermark extraction phase.

3.1 Watermark Hiding Phase

The process of hiding the watermark in the Intensity component *I* of the cover image is given below.

Inputs: Original Cover image of size (m×n), Binary watermark of size (w×h)
Outputs: Private share of size (w×h)

Step1: Construct a resized image from the original cover image by continuously decimating the given cover image by 2 until it fits to the watermark image size.
Step2: Construct an CCt table *T* from the resized cover image.
Step3: Calculate average of the CCT table. Let it be T_{avg}.
Step4: A secret key *K* is used as a seed to select $30\times w\times h$ random entries from the table *T*.
Step5: For each pixel in the binary watermark, a set of 30 random entries are chosen consecutively and its average is calculated.

Step6: Construct a feature matrix F of size $w\times h$, such that the entries in the matrix are the sample averages obtained in the above step.
Step7: Construct a secret binary matrix S, using the following comparison:

$$S(x,y)=\begin{cases}1, & if \quad F(x,y)\geq T_{avg}\\ 0, & if \quad F(x,y)<T_{avg}\end{cases} \tag{2}$$

Step8: Use the bits in matrix S as secret key bits to select columns in Table 2 (MPVSS Scheme) for generating the Private Share (Share2).

Finally, the private share is time-stamped and is confidentially kept secret at a Certified Authority (CA). During verification of copyrights, the owner should provide the same secret key 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.

3.2 Watermark Extraction Phase

The process of extracting the watermark from the Intensity component I' of the claimed image is given below.

Inputs: Cover image I' of size (m×n), Private Share of size (w×h)
Outputs: Extracted Watermark of size (w×h)

Step1: The procedure to create secret binary matrix S is same as in hiding phase.
Step2: Use the bits in matrix S as secret key bits to select columns in Table 2 (MPVSS Scheme) for generating the Public Share (Share1). 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.
Step3: Finally, the watermark can be revealed by performing bitwise logical OR operation on the public share and the private share.

The proposed scheme can be extended to hide to gray-level or color watermarks. They are first transformed into bi-level halftone images and then embedded into the cover images using the same procedure.

4. Simulation Results

To verify the effectiveness of the proposed watermarking scheme a sequence of simulations were performed using MATLAB Image Processing Toolbox. Fig.3 (a) shows the gray level test image (of size 512×512 pixels) which was selected as cover image. The binary watermark image to be hidden into the cover image is of size 100×150 and is shown in Fig. 3(b). Given the cover image shown in Fig. 3(a) the resultant private share, public share and the extracted watermark of the proposed watermarking scheme are shown in Fig.4.a-c. Note that the size of all these images is same as the original watermark.

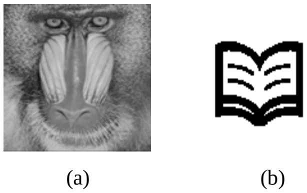


Fig. 3 Test images used in simulations
(a) Baboon (512×512) (b) Watermark (100×150)

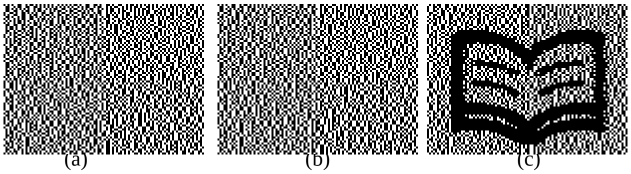


Fig. 4 Results of simulations
(a) Private share (b) Public share (c) Extracted watermark (100×150)

Peak Signal to Noise Ratio *(PNSR)* and Normalized Correlation *(NC)* are used to evaluate the performance of the proposed watermarking scheme. *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:

$$PSNR=10\times\log\frac{255^2}{MSE} \tag{3}$$

$$MSE=\frac{1}{m\times n}\sum_{i=1}^{m}\sum_{j=1}^{n}(H_{i,j}-H'_{i,j})^2 \tag{4}$$

Where $H_{i,j}$ denotes pixel color of original cover image and $H'_{i,j}$ denotes a pixel color of attacked watermarked image, and $m\times n$ denotes the image size.

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

$$NC=\frac{\sum_{i=1}^{w}\sum_{j=1}^{h}\overline{(B_{i,j}\oplus B'_{i,j})}}{w\times h} \tag{5}$$

Where $B_{i,j}$ denotes pixel color of original watermark image and $B'_{i,j}$ denotes a pixel color of extracted watermark image.

To check attack resilience of the proposed scheme, some common image processing attacks were performed on the three cover images. The corresponding PSNR and NC values are listed in Table 3. The JPEG compression attack is performed by compressing the image with a quality factor 10. The blurring, sharpening and median filtering of the images were done with a window of size 3×3. The salt and pepper noise image is obtained by replacing 20% of pixels in the cover image with black and white pixels. The scaling of an image is done by first reducing the original cover image size from 512×512 pixels to 256×256 pixels, and then zoomed to its original size by means of pixel replication. The cropped image is obtained by cropping 10% of the original cover image at top right corner. To test the robustness against rotation attack the original cover image is rotated 15^o in counter clock wise direction. The speckle noise image is obtained by adding speckle noise with a variance of 0.5 to the cover image. From Table 3 it is clear that the proposed scheme results in good NC values for several common attacks.

5. Conclusions

In this paper, a spatial domain digital watermark hiding technique based on Visual Secret Sharing (VSS) and unique statistical properties is proposed. When compared with similar existing techniques, the proposed technique has three main advantages. 1. Since unique features of the cover image are used, it reduces the chances of false positives there by improving the security of the watermarking scheme 2. Since a modified version of VSS called Multi-Pixel VSS (MPVSS) with no pixel expansion, is used, it is convenient to carry and store the intermediate images called shares. 3. Since the chosen feature vector depends on spatial correlation of pixels, it reduces tradeoff between spatial and frequency domain techniques in terms of robustness against range of attacks.

References

[1] R. J. Anderson, Ed., “Information hiding”, in First International Workshop, LNCS, Springer, 1996, Vol. 1174, pp. 1-7.

[2] M. Naor, and A. Shamir., “Visual cryptography,” in Workshop on the theory and application of cryptographic techniques, 1995, Vol. 950, pp. 1-12.

[3] D. C Lou, H. K Too, and J. L. Iiu, “A copyright protection scheme for digital images using visual cryptography technique,” Computer Standards & Interfaces, vol. 29, No. 1, 2007, pp. 125-131.

[4] G. D. Park, E. I. Yoon, and K. Y. Yoo, “A new copyright protection scheme with visual cryptography,” in The Second International Conference on Future Generation Communication and Networking Symposia, 2008, pp. 60-63.

[5] T. H. Chen, C. C Chang, CS. Wu, and D.-C Lou, “On the security of a copyright protection scheme based on visual cryptography,” Computer Standards & Interfaces, Vol. 31, No.1, 2009, pp. 1-5.

[6] Y. Xing, and J. H He, “A new robust copyright protection scheme for digital images based on visual cryptography,” The 2010 International Conference on Wavelet Analysis and Pattern Recognition, Qingdao, 2010, pp. 6-11.

[7] C. S Hsu, and Y. C Hou, “A visual cryptography and statistics based method for ownership identification of digitalimages,” World Academy of Science, Engineering and Technology, Vol. 2, 2005, pp.172-175.

[8] M. A. Hassan, and M. A. Khalili, “Self watermarking based on visual cryptography”, World Academy of Science, Engineering and Technology, Vol. 8, 2005, pp. 159-162.

[9] 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, 2007, pp 1-8.

[10] R. Hwang, “A digital image copyright protection scheme based on visual cryptography,” Tamkang Journal of science and Engineering, Vol.3, No.2, 2002, pp. 97-106.

[11] R I. Zaghloul, and Enas F. Al-Rawashdeh, “HSV image watermarking scheme based on visual cryptography”, World Academy of Science, Engineering and Technology, Vol. 44, 2008, pp. 482-485.

[12] Y. C Hou, and P. H Huang, “Image protection based on visual cryptography and statistical property”, IEEE statistical signal processing workshop (SSP), 2011, pp.481-484.

Ms B Surekha received the 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 5 research papers. She is a member of IETE, ISTE.

Dr GN Swamy received the B. Tech degree in Electronics and Communication Engineering from Nagarjuna University (INDIA) in 1991, M.Tech degree in Microwaves from BHU Varanasi University (INDIA) in1993 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 at national and international level. He is actively associated with national professional bodies like IETE and ISTE, INDIA.

Table 3 Simulation results of proposed watermarking scheme

Attacks	***Boat***		***Baboon***		***Lena***	
	PSNR(dB)	***NC***	***PSNR (dB)***	***NC***	***PSNR(dB)***	***NC***
JPEG (QF=10%)	32.93	0.9004	30.42	0.9334	35.36	0.9132
Blurring (3×3)	30.52	0.9644	29.12	0.9344	32.64	0.9136
Sharpening (3×3)	29.61	0.9792	28.29	0.9660	32.54	0.9782
Histogram Equalization	26.97	0.7240	27.57	0.7848	41.94	0.6062
Median Filter (3×3)	36.42	0.9872	31.69	0.9578	40.71	0.9856
Salt&Pepper noise(density=0.2)	34.05	0.8824	34.12	0.9412	34.20	0.8100
Scaling (1/2)	33.60	0.9818	30.99	0.9680	36.81	0.9700
Rotation (15^{o} left)	27.89	0.9364	27.63	0.9296	27.94	0.9172
Cropping (10%)	36.11	0.9632	36.11	0.9606	36.21	0.9588
Speckle noise (var=0.5)	27.52	0.8482	27.44	0.9084	27.89	0.8992