A Spatial Domain Public Image Watermarking

B Surekha
Associate Professor,
Department of ECE,
TRR College of Engineering,
Patancheru, Hyderabad,
Andhra Pradesh, India - 502 319.
borra_surekha@yahoo.co.in

Dr GN Swamy
Professor & HOD,
Department of ECE,
Gudlavalleru Engineering College,
Gudlavalleru, Krishna District,
Andhra Pradesh, India - 521 356
gavini_s@yahoo.com

Abstract

In recent years, internet revolution resulted in an explosive growth in multimedia applications. Hence, concern about assurance of ownership rights has been mounting. In this paper, three public image watermarking techniques are proposed. The first one, called Single Watermark Embedding (SWE), uses the concept of Visual Cryptography (VC) to embed a watermark into a digital image. The second one, called Multiple Watermarks Embedding (MWE) extends SWE to embed multiple watermarks simultaneously in the same host image. Finally, Iterative Watermark Embedding (IWE) embeds the same binary watermark iteratively in different positions of the host image, to improve the robustness. Experimental results show that the proposed techniques satisfies all the properties of digital watermarking such as invisibility, security, capacity, low computational complexity and is robust to wide range of attacks.

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

1. Introduction

Today, many photo agencies expose their collection on the web with a view of selling access to the images. They typically create web pages of thumbnails, from which it is possible to purchase high resolution images. However, this kind of ultimate flexibility to avail digital images facilitates information piracy. Cryptographic techniques can solve the problem of unauthorized access to the information. But, it can't prevent an authorized user from illegally replicating the decrypted content.

Therefore robust methods are being developed to protect the proprietary rights of the data owners. Digital watermarking is a technology being developed, to provide protection from illegal copying [1]. In the embedding phase of digital image watermarking, a digital signature, called watermark is embedded into the host image. The resultant watermarked image is usually transmitted or stored. Detection or extraction of this watermark at a later time enables data owners to make an assertion about the authenticity and ownership of their object.

There are different ways to extract the watermark from the image. The techniques that require both the original host image and the secret key for watermark extraction are called Private watermarking schemes. Those, which require only the secret key, but not the original host image, are called Public watermarking schemes [2]. Semi-private watermarking schemes [3] require both the secret key and the original watermark for watermark extraction. In general, an effective watermarking technique should satisfy properties such as invisibility, robustness, security, capacity and low computational complexity [4].

Watermarks can be embedded in almost every domain (Spatial, DCT, Wavelet, Fourier etc.). The drawback of almost all the spatial domain techniques is that, they alter the host image during embedding phase. In addition, they have the lowest bit capacity and the lowest resistance to JPEG compression [5].

Recently, many researchers applied the concept of Visual Cryptography (VC) [6] for Copyright Protection of digital images. Visual Cryptography (VC) is basically a secret sharing scheme extended for images. It has the ability to restore a secret without the use of computations. References [7], [8] fully employ the visual decryption ability of VC. They first convert the original gray-level host image into a half-tone image. Two random shares of the watermark are then generated. One share is embedded into the half tone image. The other share is kept secret by the owner. Further, watermark can be extracted by simply superimposing the secret share over the half-tone-image. The drawback of this technique is that the host image is altered and that the size of the watermark is restricted. It can't support multiple watermarks and is not robust to many attacks.

Hwang [9] demonstrated a direct method of hiding binary watermarks into gray-level images without converting them into half-tone images. This technique overcomes the above drawbacks but, doesn't guarantee the security always. Hence it is unsuitable for digital image copyright protection. References [10], [11], [12] overcome the security drawbacks of Hwang's scheme, but are not robust to some attacks such as jitter, histogram equalization, cropping and rotations.

This paper proposes three simple spatial domain public watermarking techniques to overcome the above mentioned drawbacks. A Single Watermark Embedding (SWE) technique is proposed, to embed a binary watermark into a host image. It is based on the concept of (2, 2) Visual Cryptography (VC), and uses a secret key. Based on SWE, Multiple Watermarks Embedding (MWE) is developed to embed multiple watermarks simultaneously in the same host image. Here multiple secret keys are needed to embed multiple watermarks. Finally, in Iterative Watermark Embedding (IWE), a binary watermark image is embedded iteratively in different positions of the host image, to improve its robustness. Experimental results show that the proposed scheme is robust to wide range of attacks.

The remaining part of the paper is organized as follows. Section2 briefly reviews basic (2, 2) Visual Cryptography. Section3 describes the proposed Single Watermark Embedding (SWE) technique. Section4 extends SWE for Multiple Watermark Embedding (MWE). The proposed Iterative Watermark Embedding (IWE) is introduced in Section5. Experimental results are illustrated in Section6 and Section7 concludes the paper.

2. A (2, 2) visual cryptography

Visual Cryptography (VC) was first introduced by Noar and Shamir at Eurocrypt'94[6]. To encode a secret using a (2, 2) Visual Cryptography, the original image is divided into two shares such that, each pixel in the original image is replaced with a non-overlapping block of two sub-pixels. Anyone who holds only one share will not be able to reveal any information about the secret. To decode the image, each of these shares is xeroxed onto a transparency. Stacking both these transparencies will permit visual recovery of the secret. Encoding of one pixel in a (2, 2) VC is illustrated in Table.1. A white pixel is shared into two identical blocks of sub-pixels. A black pixel is shared into two complementary blocks of sub-pixels. 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. If the given pixel *p* is black, then the encoder randomly chooses one of the last two columns of Table.1. Each block has half white and half black sub-pixels, independent of whether the corresponding pixel in the secret image is black or white. All the pixels in the original image are encrypted similarly using independent random selection of columns. Thus no information is gained by looking at any group of pixels on a share, either.

Table 1. A (2, 2) visual cryptography

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

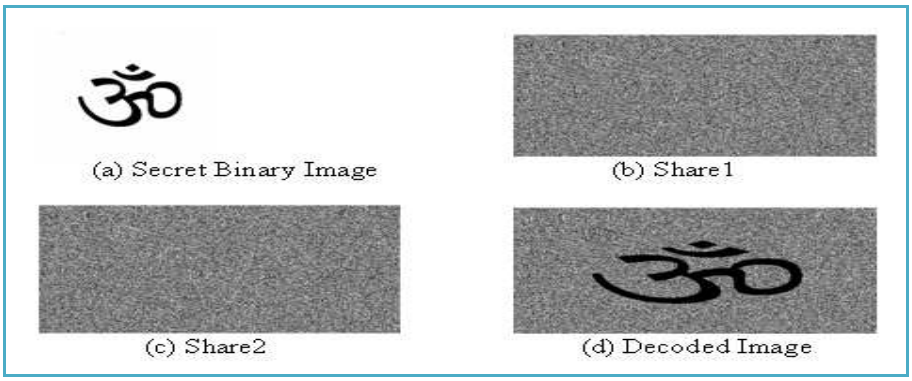
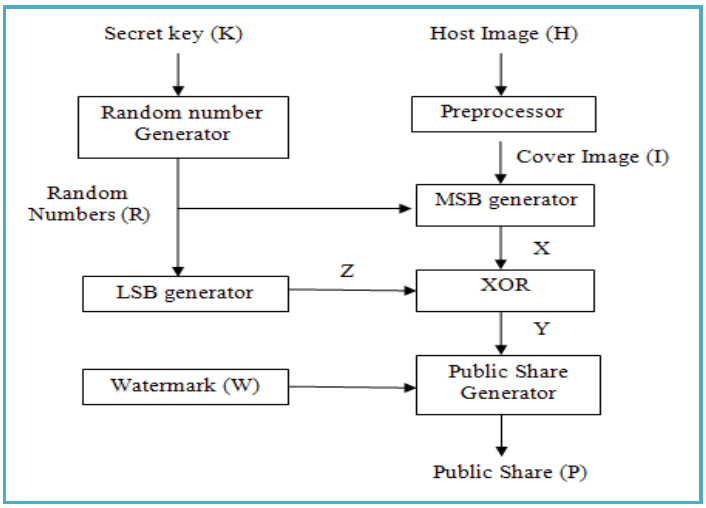


Figure 1. Example of (2, 2) visual cryptography scheme

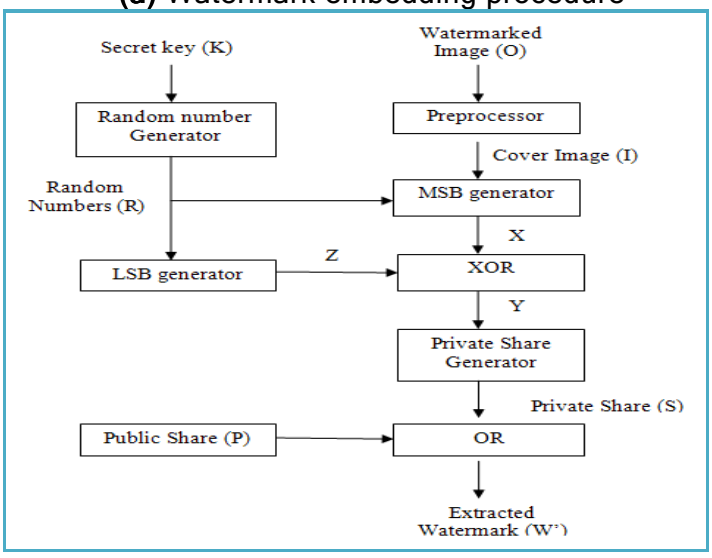
The results of basic (2, 2) VC Scheme are shown in Fig.1. When the two shares are stacked together, as in Fig.1.d, the black pixels in the original image remain black and the white pixels become gray. Although some contrast loss occurs, the decoded image can be clearly identified. Since each pixel in the original image is replaced by two sub-pixels in each share, the width of the decoded image is twice that of the original image.

3. Single watermark embedding (SWE)

The embedding and extraction phases of the proposed SWE method are shown in Fig.2. Unlike traditional watermarking schemes, the watermark is not embedded physically into the digital image. Instead, the proposed method constructs a Public Share and a Private Share to embed and extract a binary watermark from the host image.



(a) Watermark embedding procedure



(b) Watermark extraction procedure

Figure 2. Single watermarking embedding (SWE)

3.1. Embedding algorithm

The embedding algorithm embeds the watermark directly into the original host image *H* in case of a gray-scale, or into the intensity component, if it is a color image. Let the relevant component of the original host image is referred to as cover image *I*. Decomposition of the image to obtain the required component is done in the preprocessing stage of the algorithm.

After preprocessing, the real watermark embedding procedure follows as in Fig 2.a. A secret key *K* is used as a seed to generate *n* random numbers, where *n* is the size of the watermark. The random numbers must be any integer with in the size of the cover image. Let R_i be the i^{th} random number. A binary matrix *X* is generated such that, the entries in the array are the most significant bits of R_i^{th} pixel of the cover image *I*. A binary matrix *Z* is generated, such that the entries in the array are the least significant bits of the R_i^{th} random number. Now, bitwise XOR of *X* and *Z* matrices is done to create a binary matrix *Y*. A Public Share *P* is then generated by assigning a pair of bits for each element in the binary matrix *Y*. The encryption rules for generating a Public Share are given in Table2.

Table 2. Encryption rules to create public share

Color of i^{th} pixel in binary watermark (*W*)	i^{th} entry in binary matrix (*Y*)	Pair of bits to be assigned in Public Share (*P*)
Black	1	(0, 1)
Black	0	(1, 0)
White	1	(1, 0)
White	0	(0, 1)

Finally, the owner must register his watermark pattern and the corresponding Public Share at a neutral organization. While resolving the rightful ownership, the owner should provide the same secret key to the neutral organization, to retrieve a second share called Private Share. This share when combined with the Public Share, extracts the embedded watermark, which the owner has registered. As the watermark is not embedded physically into the digital image, the original image is not at all altered. Hence, at no point of time the watermark information is passed in the transmission channel, thereby providing maximum security.

3.2. Extraction algorithm

The inputs to the extraction algorithm are the watermarked image *O*, the Public Share *P* and the secret key *K*. The output of the extraction algorithm is the extracted watermark W*'*.

The process of extracting the watermark from the watermarked image is shown in Fig.2.b. The procedure to create a binary matrix *Y* is same as in embedding algorithm.

A Private Share *S* is now generated in such a way that if the element in the binary matrix *Y* is '0' then assigns *S = (0, 1)* else assign *S = (1, 0)*. Finally, the watermark is extracted by performing bitwise logical OR operation on the Public Share and the Private Share.

The present version of the proposed scheme only deals with binary watermarks. It is also possible to extend the method to gray-level or color watermarks. They are first transformed into bi-level halftone images and then embedded into the host images using the same procedure.

3.3. Security analysis

The security in the proposed method is based on the generation of the binary matrix *Y*, which is used to create either Public Share or Private Share. This matrix is obtained by taking bitwise XOR of binary matrix *X* (most significant bits of the selected random pixels), and the binary matrix *Z* (least significant bits of the corresponding random numbers). The same large binary matrix *Y* resulted from the secret key, is to be used in the subsequent extraction process. Otherwise, there is no way an attacker can estimate the Private Share.

4. Multiple watermarks embedding (MWE)

MWE extends SWE to embed multiple watermarks in the same host image. Multiple watermarks are embedded in the cover image independently, as in SWE. Note that, the watermarks size need not be the same. Multiple secret keys are used with multiple watermarks to result multiple Public Shares. These Public Shares are then distributed to the corresponding owners. Since the watermark is not embedded directly into the digital image there is no restriction on the number of watermarks. When piracy happens, the detection of multiple watermarks is done independently as in SWE.

5. Iterative watermark embedding (IWE)

In practice, there is a very good chance for a watermarked image to be altered while being transmitted through the channel. These alterations may be a result of intentional attacks such as filtering, blurring, cropping etc. or unintentional distortions such as JPEG compression, channel noise addition etc. All the spatial domain techniques that are discussed in Section1 are not robust to cropping attacks. It is observed that an iterative approach ensures explicitly the existence of the watermark after cropping attacks. Thus, in IWE, the same watermark is embedded in four different positions as in Fig. 3, using the same secret key. The positions are chosen, to be robust against cropping attack from the bottom, the top, the left or from the right side of the watermarked image. For different positions, the embedding algorithm results in different Public Shares. During watermark extraction four different Private Shares are obtained from four positions of the host image. The corresponding Public Shares and Private Shares are stacked together to result in four different extracted watermarks of different qualities. The one with greatest match is chosen.

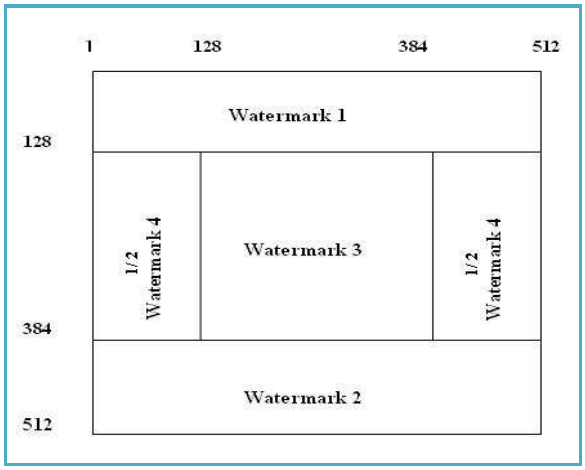


Figure 3. Watermarking embedding positions in IWE

6. Experimental results

To verify the effectiveness of the proposed method, a series of experiments were conducted in Matlab 7.0. Fig.4. shows the results of Single Watermark Embedding (SWE). Fig.4.a. shows the Original Lena image into which the watermark is embedded. Fig.4.b. shows the binary watermark of size 100×100. Fig.4.c shows the watermarked image. Since the host image is not altered during the embedding phase the watermarked image is same as the original host image. Fig.4.d. shows the Public Share generated during watermark embedding process. Fig.4.e. shows the Private Share generated during watermark extraction.Fig.4.f. shows the extracted watermark resulted from stacking the Public Share and the Private Share. Although some contrast loss occurs, the extracted watermark can be clearly identified. However, a threshold technique [13] is used to resize the extracted watermark to its original size and contrast. The threshold technique evaluates every set of two sub pixels in the stacked result, against the threshold. Here, the threshold is chosen as one. The pixel in the resized watermark is black, if the number of black sub pixels is two and white, if one. Fig.4.g. shows the resized watermark.

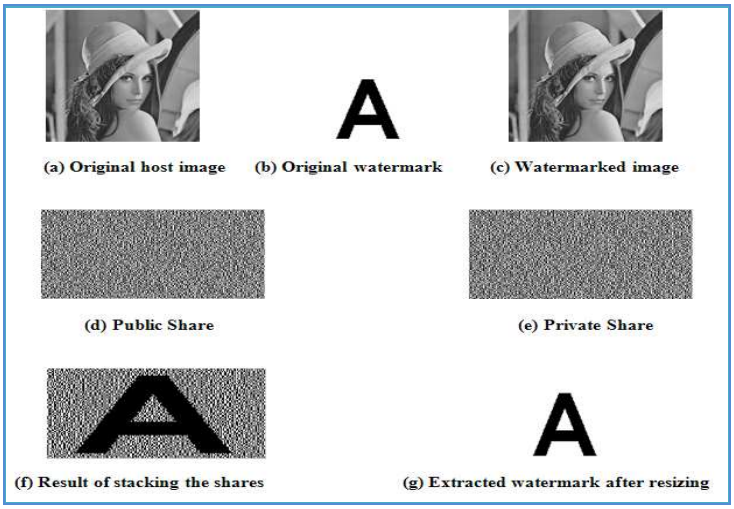


Figure 4. Results of single watermark embedding (SWE)

Fig.5. shows the results of Multiple Watermark Embedding (MWE) in the same Lena image. Fig.5.a. shows four different sized binary watermark images, used in the experiments. Fig.5.b. shows the results of stacking the corresponding Public Shares and Private Shares.

(a) Multiple watermarks used in the experiments

(b) Results of stacking the corresponding shares

Figure 5. Results of multiple watermarks embedding (MWE)

The robustness of the proposed algorithm is tested, by subjecting the watermarked images to various image manipulating operations and compression attacks. All attacks are implemented using the MATLAB Image Processing Tool box. Peak Signal to Noise Ratio *(PNSR)* and Normalized Correlation *(NC)* are used to evaluate perceptual distortion of this watermarking scheme. *PSNR* is used to evaluate the similarity of original and attacked grey-level images. It is defined in terms of Mean Square Error *(MSE)* as follows:

$$PSNR = 10 \times \log \frac{255^2}{MSE} \quad \textbf{(1)}$$

$$MSE = \frac{1}{r \times c} \sum_{i=1}^{r} \sum_{j=1}^{c} (h_{i,j} - h'_{i,j})^2 \quad \textbf{(2)}$$

Where $h_{i,j}$ denotes pixel color of original host image and $h'_{i,j}$ denotes a pixel color of attacked watermarked image, and $r \times c$ denotes the image size.

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

$$NC = \frac{\sum_{i=1}^{w}\sum_{j=1}^{h}(\overline{s_{i,j} \oplus s'_{i,j}})}{w \times h} \times 100\% \quad \textbf{(3)}$$

Where $s_{i,j}$ denotes pixel color of original watermark image and $s'_{i,j}$ denotes a pixel color of extracted watermark image, and $w \times h$ is the watermark size.

Fig.6. portrays the result of cropping the watermarked image by 10% at top right corner, with *PSNR= 36.2dB,* along with its extracted watermark *(NC=100%)*.

(a) Watermarked image **(b)** Extracted watermark

Figure 6 (a) Results of cropping attack

In the same way, various attacks have been performed on some test images to further evaluate the robustness of the proposed algorithm. All the test images are of size 512×512 and are shown in Fig.7. The watermarking survived all.

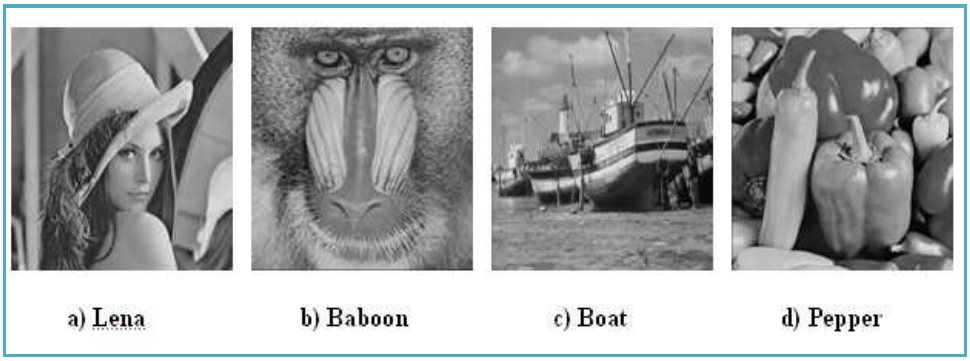


Figure.7. Test images used in the experiments

The performance of the algorithm with respect to attack resilience has been established by the results shown in Table.3. Experimental results illustrates that the proposed algorithm is resistant to several attacks such as cropping, JPEG compression, blurring, sharpening, median filtering, wiener filtering, noise adding, intensity adjustments, jitter, blanking rows and columns, rotations and scaling with NC values almost approaching 100%.

Table 3. Test results for robustness against several attacks

Attacks	Lena PSNR (dB)	Lena NC (%)	Baboon PSNR (dB)	Baboon NC (%)	Boat PSNR (dB)	Boat NC (%)	Pepper PSNR (dB)	Pepper NC (%)
10% Cropping	36.20	100	36.10	100	36.10	100	36.21	100
25% Cropping	30.24	100	30.19	100	30.18	100	30.25	100
50% Cropping	27.19	100	27.13	100	27.12	100	27.21	100
75% Cropping	25.37	100	25.31	100	25.34	100	25.37	100
Remove_columns_32	36.18	96.79	36.11	95.13	36.12	95.58	36.19	95.93
Remove_rows_32	36.17	96.38	36.10	94.87	36.12	95.36	36.18	95.36
Jitter	41.39	98.34	41.25	99.97	41.73	100	41.40	99.75
Blurring	32.64	95.38	29.11	98.00	30.51	98.90	31.08	97.17
Sharpening	32.54	94.11	28.29	95.20	29.60	98.38	30.27	96.71
Histogram Equalization	41.93	94.08	27.56	93.89	26.96	98.13	29.84	9600
Median Filter 3*3	40.71	98.47	31.68	99.39	36.42	99.90	38.99	99.75
Wiener Filter 5*5	39.94	98.09	30.76	99.33	34.84	99.77	37.95	99.71
Salt & Pepper Noise	38.04	96.29	44.10	99.17	44.07	99.23	44.26	99.26
Rotation_35	24.84	56.40	24.64	92.98	24.92	68.33	24.72	79.14
Scale_0.5	36.80	97.44	30.99	98.45	33.59	99.68	35.34	99.02
JPEG_80	42.81	99.68	35.77	99.66	39.44	99.83	39.82	99.60
JPEG_50	40.21	98.27	32.68	98.49	36.77	99.92	37.97	99.60
JPEG_10	35.35	96.96	30.42	99.12	32.92	99.85	34.28	99.35
JPEG_1	30.81	91.30	29.33	98.60	30.08	98.34	30.76	98.21

7. Conclusions

In this paper three invisible public watermarking techniques are proposed, to embed binary watermarks into digital images. Unlike traditional watermarking techniques, the watermark is not embedded physically into the digital image and the original image is not altered at all. Hence, at no point of time the watermark information is passed in the transmission channel, thereby providing maximum security. In addition, the size of the watermarks is not restricted to being smaller than that of the host image. Experimental results show that the proposed scheme is robust and secure, against a wide range of intentional and unintentional attacks, with *NC* values almost approaching 100%. The proposed algorithm can resist to rotations to some extent.

8. References

[1] Anderson, R. J, Ed., "Information Hiding", First International Workshop, Lecture Notes in Computer Science, Springer-Verlag, vol. 1174, 1996, pp. 1-7.

[2] Cox, I. J., Miller, M. L., and Bloom, J. A., "Digital Watermarking", New York: Morgan Kaufmann Publishers Inc., San Fransisco, CA, 2002.

[3]Kutter, M., and Petitcolas, F. A. P., "A fair benchmark for image watermarking systems", Proc. of Security and Watermarking of Multimedia Contents, Jan 1999, pp. 226–239.

[4] Cox, I. J., Kilian, J., Leighton, T., and Shamoon, T., "Secure Spread Spectrum Watermarking for Multimedia", proc. of IEEE Transactions on Image Processing, vol. 6, no. 12, Dec 1997, pp. 1673−1687.

[5]Langelaar, G.C., van der Lubbe, J., and Biemond, J., "Copy protection for multimedia data based on labelling techniques'`, 17th Symposium on Information Theory, May 1996.

[6] Noar, M., and Shamir, A., "Visual Cryptography", Advances in Cryptography Eurocrypt'94, Lecture Notes in Computer Science, Springer-Verlag, vol. 950, 1995, pp. 1-12.

[7] Fu, M. S., Au, 0. C., "Joint Visual Cryptography and Watermarking", Proc. of IEEE International Conference on Multimedia and Expo, June 2004, pp. 975-978.

[8] Hou, Y-C., Chen, P-M., "An Asymmetric Watermarking Scheme based on Visual Cryptography", proc. of Fifth IEEE International Conference on Signal Processing, vol. 2, Aug 2002, pp.992 -995.

[9]Hwang, R., "A Digital Image Copyright Protection Scheme based on Visual Cryptography", Tamkang Journal of science and Engineering, vol.3, no.2, 2002, pp. 97 - 106.

[10]Mahmoud Hassan, A., and Mohammed Khalili, A., "Self Watermarking based on Visual Cryptography", proc. of World Academy of Science, Engineering and Technology, vol. 8, Oct 2005,pp. 159-162.

[11]Azzam SLEIT, Adel ABUSITTA, "A Visual Cryptography Based Watermark Technology for Individual and Group Images", Journal of Systemics, Cybernetics and Informatics, vol. 5, no. 2, 2008, pp. 24-32.

[12]Surekha B, Swamy GN, Srinivasa Rao K, Ravi Kumar A, "A Watermarking Technique based on Visual Cryptography", International Journal of Information Assurance and Security, vol. 4, no.6,2009, pp. 470-473.

[13]Hawkes, W., Yasinsac, A., Cline, C., "An Application of Visual Cryptography to Financial Documents", Technical report TR001001, Florida State University, 2000

Authors

Ms B Surekha is currently working as an Associate Professor in the Dept of ECE, TRR College of Engineering, Hyderabad, AP, India. She has received the B. Tech degree from the Nagarjuna University, India and the M.Tech degree from the JNT University, India, both in Electronics and Communication Engineering. She is currently pursuing PhD degree at JNT University, India. She has several publications in various conferences and journals at international repute. Her research interests include Cryptography and Copyright Protection

Dr GN Swamy is currently working as a Professor and Head of the Department, Dept of ECE, Gudlavalleru Engineering College, Gudlavalleru, India. He has received his Ph D degree in Signal Processing from the Andhra University, India. He has 16 years of teaching experience and is actively associated with national professional bodies like IETE and ISTE, India. He has several publications to his credit at national and international level. His research interests include Electronic Devices, Microwaves, Signal Processing and Cryptography.