Blind Watermarking Scheme for Digital Images

[1]K.Yogalakshmi and [2]R.Kanchana

[1] *Departmetn of Applied Electronics, Adhiparasakthi College of Engineering, Melmaruvattur.*
yogaeie@yahoo.com.
[2]*Assistant Professor, Adhiparasakthi College of Engineering, Melmaruvattur .*
Kanchanarajendran@yahoo.co.in.

***Abstract*— In modern times, the rapid growth of the Internet has made copyright protection of digital contents a critical issue. A Digital Rights Management (DRM) system is aimed at protecting the high-value digital assets and controlling the distribution and utilization of those digital assets. Watermarking technologies are being regarded as a vital mean to proffer copyright protection of digital images. Digital watermarking hides, in digital images, the information necessary for ownership identity to offer copyright protection. This paper proposes an innovative invisible and blind watermarking scheme for copyright protection of digital images with the purpose of defending against digital piracy. In the proposed watermarking scheme, a binary watermark image is invisibly embedded into the host image for achieving copyright protection. In watermark embedding, every pixel of the watermark image is embedded into the individual blocks of the host image sized 2x2. (ii) n-level RIVC scheme, the content of an image S is designated to multiple regions associated with n secret levels, and encoded to n+1 shares with the following features: (a) each share cannot obtain any of the secrets in S, (b) any t(2 ≤t≤n+1)shares can be used to reveal t-1 levels of secrets, (c) the number and locations of not-yet-revealed secrets are unknown to users, (d) all secrets in S can be disclosed when all of the n+1 shares are available, and (e) the secrets are recognized by visually inspecting correctly stacked shares without computation. The efficiency of the proposed watermarking scheme has been demonstrated via the experimental results**

Keywords: - Blind Scheme, Copyright Protection, Digital Rights Management (DRM), Digital image, Digital image watermarking; Image sharing, Image sharing invisible watermarking. secret sharing, visual cryptography, visual secret sharing.

1. INTRODUCTION

DRM is a method of entrusting copyright provisions established by the proprietors of the intellectual assets, such as license terms and usage agreements. DRM systems have been made use of for securing and limiting the distribution and utilization of valuable digital properties. The requirements of a DRM system are: offering a persistent content protection against unauthorized access to the digital content and also restricting access to authorized people. Moreover, the DRM system must be robust enough to govern access rights for various types of digital content (for instance: music files, video streams, digital books, images) across different platforms (for instance: PCs, laptops, PDAs, mobile phones) . DRM, in general, is composed of two components: 1) a collection of technologies like encryption, copy control, digital watermarking, fingerprinting, traitor tracing, authentication, integrity checking, access control, tamper-resistant hardware and software, key management, revocation and risk management architectures and 2) a set of technologies meant to convey copyright permissions in 'rights expression languages' and additional kinds of metadata that make a DRM policy machine-readable [3]. The watermark acts as a digital signature, offering a sense of ownership or authenticity to the image. One significant advantage of watermarking is the inseparability of the watermark from the content. Some of the vital characteristics of the watermark are: hard to perceive, resists ordinary distortions, endures malevolent attacks, carries numerous bits of information, capable of coexisting with other watermarks, and demands little computation to insert or identify [4]. Watermarks and watermarking techniques can be categorized into different types based on a number of ways.

Watermarking can be divided into Non-blind, Semi-Blind and Blind schemes [5], based on the requirements for watermark extraction or detection. Non-blind watermarking schemes necessitate the original image and secret keys for watermark detection. The Semi-Blind schemes require the secret key(s) and the watermark bit sequence for extraction, whereas, the blind schemes need only the secret key(s) for extraction. Another categorization of watermarks based on the embedded data (watermark) is: visible and invisible[6]. the pixel expansion, which refers to the number of pixels in a share used to encode a pixel of the secret image[7]. Proposed progressive VC schemes using more flexible decryption effects to produce higher quality images [8], There have also beensome VC schemes proposed [9]–[10] for sharing non-bilevel

secrets. Other VC schemes for generating shares with natural image appearances have been designed with the aim of further concealing the existence of the secret in the shares [11], [12].

II. BLIND WATERMARKING SCHEME

This section presents the proposed innovative invisible and blind watermarking scheme for copyright protection of digital images. As the proposed digital watermarking scheme doesn't require the original image or any of its characteristics for extraction, the proposed watermarking scheme is blind. The watermark data utilized is a binary image and its pixels are invisibly embedded into the host image for copyright protection. The following subsections describe the steps involved in the watermark embedding and extraction processes.

ii (a)WATERMARK EMBEDDING

This sub-section presents the process of binary watermark image embedment into the host image. The size of the host image chosen is dyadic (2nx2n) and the watermark used is a binary image. Firstly, non-overlapping blocks sized 2x2 are extracted from the host image and every pixel of the binary watermark image is embedded into a single block of the host image. The watermark embedding process involves: mean calculation, embedding strength (γ)and signum function. Each non-overlapping block is converted into a vector, and the mean value of the vector is computed and divided with the embedding strength (□). Since, the watermark is a binary image; the process of watermark embedding involves two cases: embedding pixel value '1' and embedding pixel value '0'. Two different mathematical operations are carried out for embedding pixel value '0' and '1'. Figure 1 shows the block diagram of the watermark embedding process.

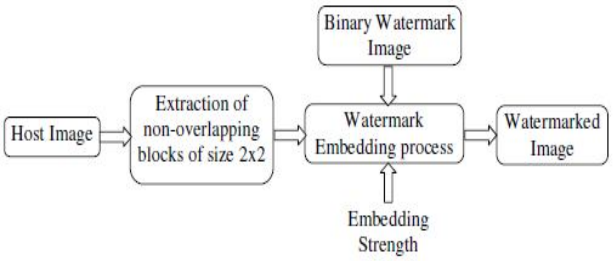


Figure 1. Watermark Embedding Process

Watermark Embedding Steps:

Input: Host Image (*I*), Binary Watermark Image (*W*), Embedding strength ($\tilde{\gamma}$

Output : Watermarked Image (*Iw*)

1. The binary watermark image (*W*) sized n x n is composed of *n*2 number of pixels. *n*2 number of 2x2 non-overlapping blocks are extracted from the host image and stored in a vector *B* .

$$B = [b_1, b_2, b_3, ..., b_N]; \ where\ 0 < N \le n^2 \qquad (1)$$

2. Every matrix in the vector *B* is converted into a vector V_B.

$$V_B = [x_1, x_2, x_3, x_4] \qquad (2)$$

3. The mean value of all the converted vectors *VB* is calculated.

$$\overline{V_B} = \frac{\sum_{i=1}^{k} V_{B_k}}{k}; \ where\ 0 < k \le 4 \qquad (3)$$

4. A value*Q* is computed by dividing the mean value $\overline{VB}$ of every vector by embedding strength ($\tilde{\gamma}$.

$$Q = \frac{\overline{V_B}}{\gamma}; \ where\ \gamma = 2 \qquad (4)$$

5. Making use of a predetermined *Q* value and embedding strength(γ, the binary watermark image pixels are embedded into the blocks in vector *B* : (i) The signum function of each block in vector *B* is calculated and stored in another vector *X* The signum function is the real valued function defined for real *x* as follows .

$$\operatorname{sgn}(x) = \begin{cases} +1, & if\ x > 0, \\ 0, & if\ x = 0, \\ -1, & if\ x < 0. \end{cases} \qquad (5)$$

For all real x we have $\operatorname{sgn}(-x) = -\operatorname{sgn}(x)$. Similarly, $|x| = \operatorname{sgn}(x)x$ .If $x \neq 0$ then also $\frac{d}{dx}|x| = \operatorname{sgn}(x)$. The second property implies that for real non-zero x we have $\operatorname{sgn}(x) = x/|x|$

(ii) For pixel value '0' perform the following mathematical operation,

$$t = ((round\,(Q * 0.5) * 2) * \gamma) \qquad (6)$$

(iii) For pixel value '1' the following mathematical operation is carried out.

$$Q_t = (Q-1)$$
$$t = ((round(Q_t * 0.5) * 3) * \gamma)) \quad (7)$$

(iv) Each block in vector X is multiplied by the calculated value t with respect to watermark pixel and placed in a vector B .

$$B << (X_{(i)} .* t) \;\; ; \; where \; 0 < i \leq k \quad (8)$$

6. The modified blocks in the vector B are mapped back to its original position in host image I to attain the watermarked image IW.

ii(b)WATERMARK EXTRACTION

This sub-section detail the steps involved in the extraction of the binary watermark image from the watermarked image. As the proposed scheme is blind, watermark extraction necessitates the watermarked image, size of watermark image and the embedding strength, whereas doesn't require the original image or any of its characteristics. Initially, non overlapping blocks sized 2x2 are extracted from the watermarked image and the number of blocks extracted varies based on the size of the watermark image. The blocks that are extracted are stored in a vector. Subsequently, all the extracted blocks are converted into a vector and the mean value of the vector is computed. Afterwards, the mean values of all the blocks are divided by the embedding strength. The resultant value is made use of in the extraction of watermark. Finally, a matrix of the size of the watermark image is created and the extracted pixel values are placed in it so as to obtain the watermark image. Figure 2 portrays the block diagram of the watermark extraction process.

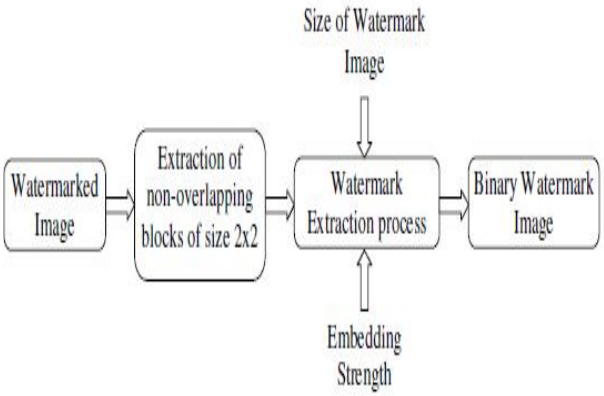


Figure 2. Watermark Extraction Process

Watermark Extraction Steps:

Input: Watermarked Image ($W I$), Size of watermark image (W) , Embedding strength (γ

Output: Watermark Image (W)

extracted blocks will be identical to the size of watermark image. The extracted blocks are stored in a vector BV.

$$BV = [b_1, b_2, b_3, ..., b_N]; \; where \; 0 < N \leq n^2 \quad (9)$$

2. Each block in the vector BV is converted into a vector VB .

$$V_B = [x_1, x_2, x_3, x_4] \quad (10)$$

3. The mean value is calculated for all the converted Vectors VB.

$$\overline{V_B} = \frac{\sum_{i=1}^{k} V_{B_k}}{k}; \; where \; 0 < k \leq 4 \quad (11)$$

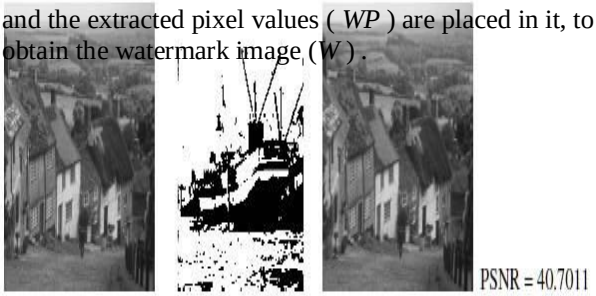
4. The calculated mean value $\overline{VB}$of every vector is divided by the embedding strength(γ). The value thus obtained is represented as$Y$.

$$Y = (\overline{V_B} / \gamma); \; where \; \gamma = 2 \quad (12)$$

5. The following mathematical operation is performed and the result is stored in a vector WP .

$$W_p << (Y[i] \bmod 2) \;\; ; \;\; 0 \leq i \leq |W| \quad (13)$$

6. A matrix of the size of the watermark image is created
and the extracted pixel values (WP) are placed in it, to obtain the watermark image (W) .



(a) (b) (c)

Attack	Cropping (Left Upper 100x100)	Cropping (Middle 100x100)	Cropping (Right Upper 100x112)
Attacked Images			
Extracted Watermark			
Correlation Coefficient	0.8123	1	0.7609

Attack	Sharpening (α = 0.2)	Sharpening (α = 0.6)	Sharpening (α = 0.9)
Attacked Images			
Extracted Watermark			
Correlation Coefficient	0.9058	0.7488	0.6622

(a)Watermark image,(b)host image,(c)watermarked image .

III. CONSTRUCTION OF AN N-LEVEL RIVC WITH SMALL N

The concept of our -level RIVC scheme involves applying n level kernels to encode the secret image. In additional to the basic requirements of the ,(t,n+1), t=2,3,……(n+1) VC scheme for these level kernels, the n level kernels used to generate our -level RIVC should also meet the following two constraints: 1) the level kernels must have the same degree of pixel expansion in order to arrange the encoded subpixels of all regions within a share and 2) the areas where no secret is revealed in the stacked image should appear visually uniform so as not to reveal the number and regions of not-yet-revealed secrets.

Based on the above requirements, below we provide the basis matrices for the construction of -level RIVC schemes with n=2, 3, 4. The two level kernels for our two-level RIVC with fourfold pixel expansion are

$$LK_1^0 = LK_2^0 = \begin{bmatrix} 0011 \\ 0101 \\ 0110 \end{bmatrix}, \quad LK_1^1 = \begin{bmatrix} 0011 \\ 0011 \\ 0011 \end{bmatrix},$$
$$LK_2^1 = \begin{bmatrix} 0011 \\ 0101 \\ 1001 \end{bmatrix}. \qquad (1)$$

The same basis matrices are used to encode a white pixel in the two level kernels, which guarantees that the number and locations of not-yet-revealed secrets remain invisible. Any single row inLMm, m=0,1 n=1,2 contains two black and two white pixels, which makes a single share appear with a uniform contrast so as not to

stacking all three shares reveals the secrets at levels 1 and 2 with contrasts of 1/2 and 1/4, respectively.

The level kernels for constructing the three-level RIVC with ten-fold pixel expansion are

$$LK_1^0 = LK_2^0 = LK_3^0 = \begin{bmatrix} 0000111111 \\ 0011001111 \\ 0101010111 \\ 0110100111 \end{bmatrix}, \qquad (2)$$
$$LK_1^1 = \begin{bmatrix} 0000111111 \\ 0000111111 \\ 0000111111 \\ 0000111111 \end{bmatrix},$$
$$LK_2^1 = \begin{bmatrix} 0111011100 \\ 1011101100 \\ 1101110100 \\ 1110111000 \end{bmatrix},$$
$$LK_3^1 = \begin{bmatrix} 0000111111 \\ 0011001111 \\ 0101010111 \\ 1001011011 \end{bmatrix}. \qquad (3)$$

Stacking any two of the four shares reveals the first level secret with a contrast of 1/5; stacking any three shares reveals the secrets at levels 1 and 2 with contrasts of 3/10 and 1/10, respectively; and stacking all four shares reveals all the secrets at levels 1, 2, and 3 with contrasts of 3/10, 1/10, and 1/10, respectively. The basis matrices for constructing the four-level RIVC with 23-fold pixel expansion are

$$LK_1^0 = LK_2^0 = LK_3^0$$

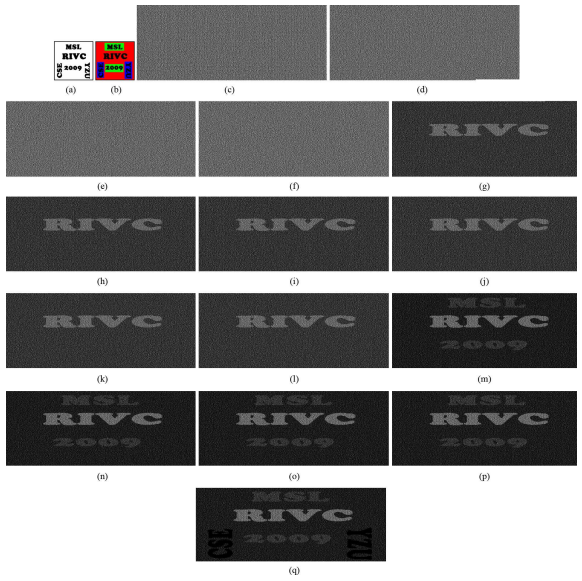
$$= LK_4^0 = \begin{bmatrix} 0000000011 & 1111111100 & 000 \\ 0000111100 & 0011111100 & 000 \\ 0011001100 & 1100111100 & 000 \\ 0101010101 & 0101011100 & 000 \\ 0110100110 & 0101101100 & 000 \end{bmatrix}. \quad (4)$$

$$LK_1^1 = \begin{bmatrix} 0000000000 & 0001111111 & 111 \\ 0000000000 & 0001111111 & 111 \\ 0000000000 & 0001111111 & 111 \\ 0000000000 & 0001111111 & 111 \\ 0000000000 & 0001111111 & 111 \end{bmatrix},$$

$$LK_2^1 = \begin{bmatrix} 0111110000 & 1000010000 & 111 \\ 1011101000 & 0100001000 & 111 \\ 1101100100 & 0010000100 & 111 \\ 1110100010 & 0001000010 & 111 \\ 1111000001 & 0000100001 & 111 \end{bmatrix}, \quad (5)$$

$$LK_3^1 = \begin{bmatrix} 0111101111 & 1000010000 & 000 \\ 1011110111 & 0100001000 & 000 \\ 1101111011 & 0010000100 & 000 \\ 1110111101 & 0001000010 & 000 \\ 1111011110 & 0000100001 & 000 \end{bmatrix},$$

$$LK_4^1 = \begin{bmatrix} 0000000011 & 1111111100 & 000 \\ 0000111100 & 0011111100 & 000 \\ 0011001100 & 1100111100 & 000 \\ 0101010101 & 0101011100 & 000 \\ 1001011001 & 1010011100 & 000 \end{bmatrix}. \quad (6)$$



Results of an experiment with the proposed three-level RIVC scheme: (a) Secret image, (b) secrecy-level decomposition, (c)–(f) four encoded shares,(g)–(l) superimposing any two of the four shares, (m)–(p) superimposing any three of the four shares, and (q) superimposing all four shares.

IV. EXPERIMENTAL RESULTS

The results obtained from experimentation of the proposed watermarking scheme are presented in this section. The proposed watermarking scheme is programmed in Matlab.

V. CONCLUSION

In modern times, the incredible development of electronic commerce applications and online services has created anxiety of unrestricted duplication and distribution of copyrighted material, in the minds of the service providers. There has been an increasing need to secure digital images because of the ubiquitous existence of the internet. In this paper, we have presented an innovative blind and invisible digital watermarking scheme for protecting the copyrights of images.

The proposed scheme makes use of a binary image as the digital watermark. The host image is initially divided into nonoverlapping blocks of size 2x2, and for every non-overlapping block; an individual pixel of the binary watermark image is embedded. Afterwards, using the approach discussed, the watermark image is extracted from the watermarked image. The watermarked images are in good visual quality and exhibit good PSNR values. The experimental results have portrayed the efficacy of the proposed digital watermarking scheme. VC can be applied to protect image-based secret information with the advantage that the decoding process can be performed by the unaided eye without computation. This letter has described the -level RIVC scheme that enables the dealer to specify the content of a secret image to multiple regions,where each region has its own secrecy property. Like traditionalVC schemes, each generated share has a noise-like appearanceand cannot obtain any secret in the secret image.

REFERENCES

[1] Claudine Conrado, Milan Petkovic, Michiel van der Veen and Wytse van der Velde "Controlled Sharing of Personal Content Using Digital Rights Management", Journal of Research and Practice in Information Technology, Vol. 38, No. 1, February 2006.

[2] L. C. Anderson, J. B. Lotspiech, “Rights Management and Security in the Electronic Library,” Bulletin of the American Society for Information Science, Vol. 22, No.1, pp.21-3, October-November 1995

[3] Ian Kerr, "Hacking@privacy: Why We Need Protection from the Technologies That Protect Copyright", In proc. of Conference on privacy and identity, 2007.

[4] Shang-Lin Hsieh, Lung-Yao Hsu, and I-Ju Tsai, “A Copyright Protection Scheme for Color Images using

Secret Sharing and Wavelet Transform", proceedings of World Academy of Science, Engineering and Technology, Vol. 10, December 2005.

[5] P. Tao and A. M. Eskicioglu, "A Robust Multiple Watermarking Scheme in the DWT Domain," Optics East 2004 Symposium, Internet Multimedia Management Systems V Conference, Philadelphia, PA, pp. 133-144, October 25-28, 2004.

[6] Ersin Elbasi and Ahmet M. Eskicioglu, "A Semi-Blind Watermarking Scheme for Color Images Using a Tree Structure," in proc. of IEEE Sarnoff Symposium, March, 2006.

[7] Yeung, M. & Minzter, F., "An Invisible Watermarking technique for image verification," Proceeding on the IEEE International Conference on Image Processing, pp:

Advances in Cryptography:Eurocrypt'94. Berlin, Germany: Springer, 1995, pp. 1–12.

[9] D. Jin, W. Q. Yan, and M. S. Kankanhalli, "Progressive color visual cryptography," *J. Electron. Imag.*, vol. 14, no. 3, p. 033019, 2005.

[10] H. C. Wu and C. C. Chang, "Sharing visual multi-secrets using circle shares," *Comput. Stand. Interfaces.*, vol. 134, no. 28, pp. 123–135, 2005.

[11] J. B. Feng, H. C. Wu, C. S. Tsai, Y. F. Chang, and Y. P. Chu, "Visual secret sharing for multiple secrets," *Pattern Recognit.*, vol. 41, no. 12, pp. 3572–3581, 2008.

[12] M.A.Dorairangaswamy, "A Robust Blind Image Watermarking Scheme in Spatial Domain for Copyright Protection," International Journal of Engineering and Technology (IJET), Vol. 1, No.3, pp. 249 - 255, August 2009.