ISSN 2278 - 3091
**International Journal of Advanced Trends in Computer Science and Engineering (IJATCSE), Vol. 4 No.1, Pages : 15 – 19 (2015)**
*Special Issue of ICACET 2015 - Held on February10, 2015, Malaysia*
***http://warse.org/pdfs/2015/icacet2015sp03.pdf***

# A Novel Three-Tier Protection for Digital Images Using Blind Watermarking Scheme


**K. Karthik[1] Dr M. A. Dorai Rangaswamy[2]**
[1]Research Scholar &Assistant Professor (Grade-II), Aarupadai Veedu Institute of Technology, India
karthik@avit.ac.in
[2] Senior Professor & HOD, Aarupadai Veedu Institue of Technology, India
drdorairs@yahoo.co.in

***Abstract:*** Digital watermark is an effectual way to protect the rightful ownership of multimedia data. In this paper, a three-tier Blind watermarking scheme is proposed, in which three independent binary watermarks are embedded in a grayscale digital image. In order to embed multi-watermarks simultaneously to improve the security of watermarked image and also robustness of extracted watermarks, the three 2-D watermarks were first recombined into a 3-D watermarking sequence. Then, the approximation sub-image of the original digital image was decomposed into non-overlapping blocks and the blocks with best abundant texture information were selected according to the size of binary watermark. Finally, the multi-watermark embedding was carried out by modifying the fractional part values of these selected block pixels based on the proposed discrete operation rule. A scheme was also developed correspondingly for multi-watermarking extraction from the distorted image. The experimental results show that one of multi-watermarks is secured enough against the common image processing such as noise addition, filtering, and JPEG compression, while the other two watermarks are immune to any image attacks.

**Keywords:** multi-watermark; security; Digital Image

## INTRODUCTION

Owing to the swift growth of the communication, computer and multimedia technology, the digital data like image, audio, and video are used and distributed through the Word Wide Web much simpler and faster than before. However, this convenience also causes substantial financial damage and becomes an important issue of copyright protection in the e-commerce era [1]. Recently, digital watermark has drawn much attention as an effective method to solve this pressing problem. Digital watermark is a technology to embed some copyright information such as company logo, signature, serial number, date or icon, called watermark, into the original media body by modifying the digital media data, and it can be detected or extracted later to assert the rightful ownership of the digital media if any conflict happens. In the last decade, plenty of digital watermarking schemes have been proposed [1-5].

According to the number of watermarks to be embedded, the digital watermarking can be classified into the single watermarking scheme [2,3] and the multi-watermarking scheme [4,5]. Compared to the former, the latter has much greater applications and can be used to solve the problems of multiple ownership or copyright. A multimedia work may have more than one author, each of them may expect to embed their watermarks in the multimedia works, and the agent company or collector may also need to embed their copyright logo in it. However, the multi-watermarking scheme is more complex than the single watermarking scheme. For example, the multiple watermarks require autonomy and uncorrelated in the multi-watermarking scheme, and the modification of one watermark should not impact other watermarks.

As well known, an effective watermarking scheme should have some better performance in terms of robustness [6], Security [7], and capacity [8]. Watermarking robustness refers to the capability of the embedded watermark to withstand intentional or unintentional media processing, called attacks, including filtering, compression, noising and so on. As used in the copyright protection, the embedded watermark should be detectable or extractable before the watermarked image is severely corrupted to a useless degree. Watermarking imperceptibility refers to whether the viewer can perceive the presence of an embedded watermark. Likewise, the perceptual difference between the original image and watermarked one should be invisible Watermarking capacity refers to the number of bits which can be embedded in the original media, that is, the size or number of the watermark. Of course, the embedded watermarking capacity is required as large as possible in general. However, these above requirements are conflict to each other. Hence, how to improve the robustness and security while keeping the bigger capacity for multi-watermarking scheme is still a difficult problem.

In this paper, a novel and robust digital image multi-blind watermarking scheme is proposed, in which three binary watermarks are embedded into a grayscale host image simultaneously. A series of experimental results reveal that the proposed multi-watermarking scheme has ideal performance.

## RELATED THEOREIES

### Arnold Transform

In order to improve the watermarking safety and also visual presentation of the extracted watermarks, it is usually to employ scrambling operation to the original watermarks. Thus the error pixels will not be together if error occurs for one or some regions of watermarking image, but scatter throughout the whole image space when extracted. Considering the simplicity of Arnold transform [9], it is adopted in this paper. Arnold transform apping) is a clipping transform presented by V. J. Arnold when he did the research of the ergodic theory. Digital watermarking can be taken as

ISSN 2278 - 3091
**International Journal of Advanced Trends in Computer Science and Engineering (IJATCSE), Vol. 4 No.1, Pages : 15 – 19 (2015)**
*Special Issue of ICACET 2015 - Held on February10, 2015, Malaysia*
***http://warse.org/pdfs/2015/icacet2015sp03.pdf***

two dimensional matrixes. When applying Arnold transform to the watermarking image, the locations of pixels in the whole watermark was rearranged and after a few iterations, the watermark will become very chaotic as shown in Figure 1. The Arnold transform can be defined in the following form:.

$$\begin{bmatrix} i' \\ j' \end{bmatrix} = \begin{bmatrix} 1 & 1 \\ 1 & 2 \end{bmatrix} \times \begin{bmatrix} i \\ j \end{bmatrix} (\mathrm{mod}\ N)$$

where (i, j) and (i, j) represent the pixel coordinate of watermark before and after executing Arnold transform, and N is the order of digital watermarking image. The operator "mod" represents the modulus operation.

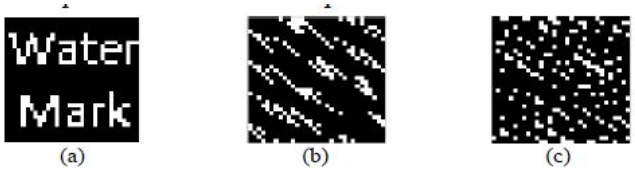



Fig.1. (a) The original digital watermark, and its Arnold transform after (b) 1-iteration, (c) 2-iterations

B. Discrete Wavelet Transform

As a powerful tool to provide both spatial and frequency multi-resolution decomposition, Discrete Wavelet Transform (DWT) has received considerable attention [10]. It exhibits a strong similarity to the way the Human Visual System (HVS) processes image. The dyadic frequency decomposition of the DWT resembles the signal processing of the HVS and thus allows adapting the distortion introduced by either quantization or watermark embedding to the masking properties of thehuman eye. In the first level decomposition of DWT, an original image is decomposed into four sub-images LL1, HL1, LH1, and HH1, where HL1, LH1, and HH1 represent the finest scale wavelet coefficients, that is, the detailed sub-images, while LL1 stands for the coarse level coefficients, that is, the approximation sub-image. To obtain the next coarse level of wavelet coefficients, the sub-image LL1 can be further decomposed into four sub-images LL2, HL2, LH2, and HH2 as shown in the Figure 2. This decomposition process continues until a certain final scale is reached. The low frequency approximation sub-image has better stability against the image processing attack of all sub-images obtained in the DWT.


Fig.2. (a) The original woman image, and (b) 2-level wavelet decomposition

## PROPOSED ALGORITHM

### Multi-watermarking Generation

In this paper, all the watermarks will be embedded synchronously in the DWT approximation sub-image due to its favorable stability. The synchronous embedding of multiple watermarks can avoid mutual interference with each other.

Each of the K watermarks $W_k=\{w_k(i,j)=0/1\}$, k=1, 2, …, K is a binary image with size of N×N. From these 2-D K watermarks, we can construct a 3-D watermarking sequence WT :

$$W_T = \{w_T(i,j,1:K) = [w_1(i,j), w_2(i,j), \cdots, w_K(i,j)]\}, \quad 1 \le i \le N, 1 \le j \le N \qquad (2)$$

where $w_T(i,j,z), 1 \le z \le K$ the 3-D watermarking pixel located at coordinate (i, j, z).

B. Multi-matermarking Embedding The original digital image is a grayscale image denoted as F fij =≤ ≤ {0 ( , ) 255} with size of M×M. Without loss of generality, the original image size M×M and watermarking size N×N satisfies M /N=r, r is an integer greater than one.

Step 1: Decompose the original image F by applying Llevel DWT, and obtain a L-level approximation sub-image FL with size of $M/2^L \times M/2^L$

Step 2: Split the approximation sub-image FL into multiple non-overlapping blocks with size of n×n, and calculate its uniformity d of each block based on the following equation [11]:

ISSN 2278 - 3091
**International Journal of Advanced Trends in Computer Science and Engineering (IJATCSE), Vol. 4 No.1, Pages : 15 – 19 (2015)**
*Special Issue of ICACET 2015 - Held on February10, 2015, Malaysia*
***http://warse.org/pdfs/2015/icacet2015sp03.pdf***

$$d(B_k)=\frac{1}{n^2}\bullet\sum_{(i,j)\in B_k}\frac{|f(i,j)-m_k|}{m_k^{1+\alpha}}$$

where $B_k$ ($1\le k\le(M/2^L n)^2$ n×n size block, $m_k$ is the average value of block $B_k$ , α is the weight correction factor (0.6～0.7). The larger the block uniformity value, the more abundant the texture information, and the larger the visual capacity.

Step 3: Select the blocks with the largest block uniformity and denoted as $BF_L^s$ (s=1, 2, …, S). The selected block number S meets the requirement that the pixel number sum of selected blocks just equals to the pixel number of binary watermark to be embedded.

Step 4: Extract the fractional part of each pixel value from the selected blocks

Step 5: Embed the multi-watermarks simultaneously by modifying the value of $DBF_L^s(i, j)$ based on the following discrete algorithm, meanwhile returning a logical table Lg:

```
If 0≤DBF_L^s(i,j)<0.5,
    DBF_L^s(i,j)=0.25, Lg(i,j)=Dec(w_T(i,j,1:K));
else
    DBF_L^s(i,j)=0.75;
    If mod(Dec(w_T(i,j,1:K)),2)=0
        Lg(i,j)=Dec(w_T(i,j,1:K))+1;
    else
        Lg(i,j)=Dec(w_T(i,j,1:K))-1;
    end
end
```

where function Dec(x) denotes to convert a binary vector x to the decimal integer

Step 6: Recombine the modified fractional part DBFLs (i, j) with its original integer part and form the new S blocks

Finally, the watermarked image is created from the new approximation sub-image $F'_L$ and the original detail sub-images by executing *L*-level inverse wavelet transform.

**Multi-matermarking Extraction**

Step 1: Decompose the tested image *T_F* with size of *M*×*M* by applying the *L*-level DWT, and obtain an approximation sub-image $T\_F_L$.

Step 2: Split the approximation sub-image $T\_F_L$ into multiple non-overlapping blocks with size of *n*×*n* in the same way as it was done before, and select the corresponding blocks $T\_BF_L^s(s=1, 2, \ldots, S)$ according to the position information recorded in the watermarking embedding process.

Step 3: Extract the fractional part of each pixel for blocks $T\_BF_L^s$: $T\_DBF_L^s(i, j)=T\_BF_L^s(i, j)-\text{floor}(T\_BF_L^s(i, j))(s=1, 2, \ldots, S)$.

Step 4: Recover the multi-watermarks $w_k^*$ ( $k=1, 2, , K$ )

based on the following discrete operation according to the fractional part value $T\_DBF_L^s(i, j)$ of the selected blocks and the logical table *Lg*.

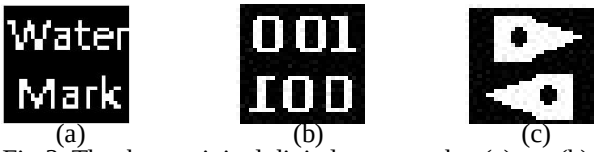
```
If 0≤T_DBF_L^s(i,j)<0.5,
    w_T(i,j,1:K)=Bin(Lg(i,j));
else
    if mod(Dec(Lg(i,j)),2)=0
        w_T(i,j,1:K)=Bin(Lg(i,j)+1);
    else
        w_T(i,j,1:K)=Bin(Lg(i,j)-1);
    end
end
```

$$w_1^*(i,j)=w_T(i,j,1),\ w_2^*(i,j)=w_T(i,j,2),\ \ldots\ldots,\ w_K^*(i,j)=w_T(i,j,K) \quad (5)$$

where function Bin(*x*) denotes to convert the decimal integer *x* to a binary vector.

## EXPERIMENTAL RESULTS

In the experimental simulation, three binary images with size of 32×32 are selected as digital watermarks to be embedded. They are named as $w_1$, $w_2$ and $w_3$, respectively, and are shown in Figure 3. The original image, shown in Figure 2(a), is a grayscale 8-bit woman image of size 512×512 and is normalized first before embedding watermark. Considering the size of original image and actual watermark, a 3-level wavelet decomposition and reconstruction was applied to the image. The quality of watermarked image is evaluated by peak signal to noise ratio (*PSNR*), and the objective evaluation of extracted watermarking results uses the error rate ( $\rho_b$ ) defined as below, respectively.




(a) (b) (c)

Fig.3. The three original digital watermarks: (a) $w_1$, (b) $w_2$ and (c) $w_3$

$$PSNR=10\cdot\log_{10}(1^2\ MSE)\ (\text{dB}) \quad (6)$$

$$MSE=\frac{\sum_{i=1}^{N}\sum_{j=1}^{N}(f(i,j)-f^*(i,j))^2}{N^2} \quad (7)$$

$$\rho_b=T_{error}/T_b \quad (8)$$

where $f(i, j)$ and $f^*(i, j)$ represent the pixel values of the original and watermarked image, respectively. $T_b$ represents the total pixel number of the embedded digital watermark,

ISSN 2278 - 3091
**International Journal of Advanced Trends in Computer Science and Engineering (IJATCSE), Vol. 4 No.1, Pages : 15 – 19 (2015)**
*Special Issue of ICACET 2015 - Held on February10, 2015, Malaysia*
***http://warse.org/pdfs/2015/icacet2015sp03.pdf***

$T_{error}$ represents the total error pixel number occurred in the extracted watermark.

The robustness of the proposed multi-watermarking scheme is evaluated below by performing several typical image processing attacks.

**Noise Addition**

Fig.4 (a) is the watermarked woman image added by Gaussian noise with mean of 0 and variance of 0.01. It is shown clearly that the watermarked woman image is very noisy and the perceptual quality degrades obviously. The *PSNR* reduces from 40.76dB of the original watermarked image to 20.12dB now. However, the extracted watermark $w_1$ shown in Fig.4 (b) can be well identified and its error rate $\rho_b$ is only about 1.27%, while the other two extracted watermarks $w_2$ and $w_3$ without any affected. The detailed simulation results under different intensity noise addition are presented in Table 1, indicating the watermarking robustness against noise attack.

(a) (b)

Fig.4. (a) The noised watermarked image and (b) the extracted results

| Gauss noise (mean, variance) | *PSNR* of the watermarked image/dB | $\rho_b$ of the extracted $w_1$ /% | $\rho_b$ of the extracted $w_2$ /% | $\rho_b$ of the extracted $w_3$ /% |
|---|---|---|---|---|
| 0, 0.005 | 23.02 | 0 | 0 | 0 |
| 0, 0.01 | 20.12 | 1.27 | 0 | 0 |
| 0, 0.02 | 17.32 | 7.03 | 0 | 0 |
| 0, 0.03 | 15.76 | 17.18 | 0 | 0 |
| 0, 0.04 | 14.65 | 23.92 | 0 | 0 |
| | | | | |

Table 1 The detected results after Gaussian noise addition

**Median Filtering**

Fig.5 (a) is the watermarked woman image filtered by median filter with window size of [7×7]. After low-pass filtering, lot of detail information is lost and the *PSNR* of the watermarked image reduces to 31.19dB. Fig.5 (b) is the corresponding extracted watermarks. It is shown that the watermark $w_1$ can be well recognized ($\rho_b$=3.12%) and the watermarks $w_2$ and $w_3$ are completely recovered. The detailed simulation results under median filtering with different window size are listed in Table 2.

(a) (b)

Fig.5. (a) The filtered watermarked image and (b) the extracted results

Table 2 The detected results after median *filtering*

| The window size of median filter | *PSNR* of the watermarked image/dB | $\rho_b$ of the extracted $w_1$ /% | $\rho_b$ of the extracted $w_2$ /% | $\rho_b$ of the extracted $w_3$ /% |
|---|---|---|---|---|
| 5×5 | 35.20 | 0 | 0 | 0 |
| 7×7 | 31.19 | 3.12 | 0 | 0 |
| 9×9 | 28.09 | 9.66 | 0 | 0 |
| 11×11 | 26.59 | 16.69 | 0 | 0 |
| 13×13 | 25.77 | 24.02 | 0 | 0 |

**JPEG Compression**

Fig.6 (a) is the JPEG compressed version of the watermarked woman image with compression quality factor of 7% and the extracted watermarks are shown in Fig.6 (b). The detailed simulation results under different quality factor are presented in Table 3. It is shown that the embedded three watermarks will be not affected by JPEG compression during the range of quality factor from 100 to 7%. When the quality factor is lower than 10%, the box compression effect of watermarked image is clearly seen. However, the extracted results are very satisfactory, indicating the proposed multi-watermarking scheme has better robustness against the image compression.

(a) (b)

Fig.6. (a) The compressed watermarked image and (b) the extracted results

ISSN 2278 - 3091
**International Journal of Advanced Trends in Computer Science and Engineering (IJATCSE), Vol. 4 No.1, Pages : 15 – 19 (2015)**
*Special Issue of ICACET 2015 - Held on February10, 2015, Malaysia*
***http://warse.org/pdfs/2015/icacet2015sp03.pdf***

Table 3 The detected results after JPEG compression

| The quality factor (%) | *PSNR* of the watermarked image/dB | $\rho_b$ of the extracted $w_1$ /% | $\rho_b$ of the extracted $w_2$ /% | $\rho_b$ of the extracted $w_3$ /% |
|---|---|---|---|---|
| 10 | 31.81 | 0 | 0 | 0 |
| 8 | 30.66 | 0 | 0 | 0 |
| 7 | 30.00 | 0 | 0 | 0 |
| 6 | 28.98 | 12.20 | 0 | 0 |
| 5 | 28.07 | 23.92 | 0 | 0 |

**Geometric Rotation**

Fig.7 is the watermarked woman image (*PSNR*=12.07dB) after rotated clockwise by 10 degree and the extracted results. It is shown again that the proposed algorithm has better robustness against the geometric distortion, and the error rate of extracted watermark $w_1$ is only about 3.12% while the other two watermarks $w_2$ and $w_3$ are completely recovered without any error.

(a) (b)

Fig.7. (a) The rotated watermarked woman image and (b) the extracted results

## CONCLUSION

In this paper, multiple binary watermarks are embedded in a grayscale digital image simultaneously based on the novel discrete operation. replication results indicate that the proposed scheme has ideal imperceptibility and capacity which are independent of the embedded watermarking number, especially the scheme can guarantee the embedded multi-watermarks in addition to one be immune to any attacks. Even so, this watermark is also robust enough against the common image processing attacks.

## REFERENCES

[1] L. H. Tian, N. N. Zheng, J. R. Xue, C. Li and X. F. Wang, “An integrated visual saliency-based watermarking approach for synchronous image authentication and copyright protection,” Signal Processing: Image Communication, vol. 26, pp. 427-437, 2011

[2] Dr m.a .Dorai Rangaswamy”A Roboust Blind Image water marking Scheme in Spatial Domain in Copy Right Protection” International Journal on Engineering and Technology(IJET),Vol 1No 3,pp 245-249,2009

[3] K.Yogalakshmi ,R. Kanchana “ Blind Water marking for Color Images”

[4] R. S. Run, S. J. Horng, J. L. Lai, T. W. Kao and R. J. Chen, “An improved SVD-based watermarking technique for copyright protection,” Expert Systems with Applications, vol. 39, pp. 673-689, 2012

[5] X. Feng, H. Zhang, H. C. Wu and Y. Wu, “A new approach for optimal multiple watermarks jnjection,” IEEE Signal Processing Letters, vol. 18, pp. 575-578, 2011

[6] S. Kiani and M. E. Moghaddam, “A multi-purpose digital image watermarking using fractal block coding,” The Journal of Systems and Software, vol. 84, pp. 1550-1562, 2011

[7] N. Nikolaidis and I. Pitas, “Robust image watermarking in the spatial domain,” Signal Processing, vol. 66, pp. 385-403, 1998

[8] K. C. Liu, “Wavelet-based watermarking for color images through visual masking,” AEU-International Journal of Electronics and Communications, vol. 64, pp.112-114, 2010

[9] A. Cheddad, J. Condell, K. Curran and P. Mc Kevitt, “Digital image steganography: Survey and analysis of current methods,” Signal Processing, vol. 90, pp.727-752, 2010

[10] W. Sun, “The periodicity of Arnold transformation,” Journal of North China University of Technology, vol. 11, pp. 29-32, 1999 (in Chinese)

[11] C. H. Hsia, J. M. Guo and J. S. Chiang, “A fast discrete wavelet transform algorithm for visual processing applications,” Signal Processing, vol. 92, pp. 89-106, 2012