International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 1 Issue 7, September - 2012

Novel Invisible And Blind Watermarking Scheme For Copy Right Protection Of Digital Images

B MANOJ KUMAR*,DR.T.V.S GIREENDRANATH =

**M.tech2ndyear., Department of Computer Science, Aditya Engg College, Surampalem, Kakinada.*

# Department of Computer Science &Engg, Aditya Engg College, Surampalem, Kakinada.

Abstract

The issue of protecting copyrights of digital contents has become very much critical owing to the swift growth of the Internet. Protecting the high-value digital assets and controlling the distribution and usage of those digital assets are the tasks of the Digital Rights Management (DRM) system. Watermarking technologies are being looked upon as promising means to safe guard the copyrights of digital images. Digital watermarking conceals the secret or personal information in digital images in order to guard their copyrights. In this paper, we present novel invisible and blind watermarking scheme for copyright protection against piracy of digital images. The proposed watermarking scheme embeds a binary watermark image invisibly into a host image for protecting its copyrights. For every 2x2 block of the host image, a watermark pixel is embedded using the proposed approach. As the proposed watermarking scheme is blind, the extraction of watermark requires only the watermarked image and it doesn't demand the original image or any of its characteristics. The experimental results have demonstrated the efficacy of the proposed watermarking scheme.

Key words:

Digital Rights Management (DRM), Digital images, Copyright Protection, Digital image watermarking, Blind Scheme, Invisible watermarking

--- *** ---

1. INTRODUCTION

In recent years, digital content distribution is one of the rapidly up-and-coming fields owing to the latest progresses in digital technologies, in company with more and more interrelated high-speed networks and the reduction in costs of high-performance digital devices. There are immense prospects for business content suppliers owing to these developments in digital content distribution which however causes threats owing to the possibility of illegal copying and distribution of the digital data with great ease. Hence, in order to secure digital content from illegitimate utilization, business content suppliers necessitate technologies supported by the legislation [1]. Digital Rights Management (DRM) is one among the possible solutions for the abovementioned issue. The digital contents are protected with the aid of DRM, a collection of technologies that enforces the utilization of digital contents in accordance with the established privileges. DRM is a method of honoring copyright provisions ascertained by the proprietors of the intellectual assets, such as license terms and usage agreements [2]. Securing valuable digital properties and restricting their distribution and utilization can be achieved with the aid of DRM systems. A DRM system needs to provide a relentless content protection against unauthorized access to the digital content, restricting access to only the ones with the appropriate authorization. It needs to be robust enough to administer usage 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) [3]. DRM consists of two components. The first is a collection of technologies such as 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. Other technologies are employed to convey copyright permissions in 'rights expression languages' and additional kinds of metadata that make a DRM policy machine-readable [4]. In addition to all the above mentioned technologies, copyright protection plays a significant role in DRM. Copyright protection mechanisms is a solution that particularly focuses on avoiding disputes that arise out of ownership claims through buying and selling digital documents. The problem requires a fool-proof mechanism to authenticate the ownership of document prior to its sale and an identical structure to attest authentic buyers [5]. The emergence of image processing tools has brought about the vulnerability of illegitimate replication, alterations and distribution of digital images. The protection of digital images is a primary concern owing to the omnipresent internet. The concern for potential loss of revenue resulting from digital media piracy is on a rise among media content owners [6]. Whilst identifying the genuine need of the copyright owners, together with the content industry, to protect their copyrights despite technological progression, digital rights management systems will offend the copyright balance amid copyright owners and users. In order to avoid copying or to restrict utilization of a digital file, several techniques are included in DRM. There IJCSNS International Journal of Computer Science and Network 72 Security, VOL.9 No.4, April 2009 is a disagreement in such technology as the regular use of which is conventionally authorized is limited as well. Professed forensic techniques are not capable of preventing duplication, as an alternative, when unauthorized copies emerge, they facilitate the copyright holder to mark out the pirates and prosecute Owing to the fact that the forensic techniques are brought into action only when a crime is evident, and they are less controversial than DRM [7]. Even though there are numerous technological methods to encounter copyright piracy, there is abundant scope for innovative research as there is still no ideal or commonly established solution accessible. The attention paid towards digital watermarking, recommended as a method for copyrightprotection or ownership identification of digital images is rising. The digital images can be protected from illegal copying and manipulation through the digital watermarking technique. Watermarking is a process in which a data is embedded into a multimedia element like image, audio or video [8]. We can extract the embedded data in the future or perceive in, the multimedia element for various purposes which includes copyright protection, access control, and broadcast monitoring. On the basis of the application, the digital watermarking can be classified into image watermarking, video watermarking and audio watermarking. Image and video copyright protection is the prime objective of the existing digital watermarking methods [9]. It acts as a digital signature, offering the image with a sense of ownership or authenticity. The inseparability of the watermark from the content is the prime advantage of watermarking. A watermark consists of numerous vital characteristics. These encompasses that the watermark is hard to perceive, resists ordinary distortions, endures malevolent attacks, carries numerous bits of information, is capable of coexisting with other watermarks, and demands little computation to insert or identify [10]. Watermarks and watermarking techniques can be divided into various categories in a number of ways. On the basis of the necessities for watermark extraction or detection, the watermarking is categorized into Non-blind, Semi- Blind and Blind schemes [11], [12]. Non-blind watermarking schemes employ the original image and secret keys to detect the watermark. The secret key(s) and the watermark bit sequence are essential for Semi-Blind schemes. Nevertheless, only the secret key(s) are employed for extraction in the blind schemes. The embedded data (watermark) might either be visible or invisible. In case of visible watermarking of images a secondary image (the watermark) is embedded in a primary image in such a manner that it is deliberately perceptible to a human observer while in case of invisible watermarking the embedded data is not detectable, nevertheless it is possible to extract it by a computer program [13]. Commonly, robust watermarking is built to endure un-malicious or malicious attacks like scaling, cropping, lossy compression, and so forth. Robust watermarking is chiefly intended towards copyright protection. On the contrary fragile watermarking is built to identify any minute alternation to the original digital content [14]. A visible watermark is restricted in more than one way. It symbolizes the image fidelity and is vulnerable to attack through direct image processing. Numerous researches on copyright protection of digital images through watermarking schemes have been proposed [15 – 20]. This research work discusses a novel invisible and blind watermarking scheme for copyright protection against piracy of digital images. The proposed watermarking scheme is blind, since it doesn't require the original image or any of its characteristics for the extraction of watermark. This scheme makes use of a binary image as watermark data for protecting the copyrights of images. For every 2x2 non-overlapping block of the host image, a binary watermark image pixel is embedded with the aid of embedding strength and signum function using the approach discussed. The embedded binary watermark is extracted from the watermarked image using watermark image size and the embedding strength. The efficiency of the proposed scheme is demonstrated with the support of experimental results. The remaining sections of the paper are organized as follows. Section 2 presents a brief review of some of the recent works that employ digital watermarking for copyright protection of digital images. The proposed novel invisible and blind watermarking scheme is presented in Section 3. The experimental results are given in Section 4 and conclusions are summed up in Section 5.

2. RELATED WORK

The information of the watermark bit is distributed all over the large spatial regions. This feature enables the watermarking technique to resist the attacks in both frequency and time domains in a robust manner. Moreover, they demonstrated the robustness to time domain attacks such as pixel shifting and rotation. In addition to protection of copyrights, their proposed watermarking scheme backs data hiding or image authentication. The enhancement of the watermark space concept of their preceding symmetric watermarking method in their method made their asymmetric design a robust one. It is improbable to eradicate the watermark without visibly deforming the watermarked image owing to the significant dependence of their watermark on the original image. They employed SDM fulfill the requirements of robustness and nambiguousness, since many common attacks found it hard to alter the parameters of the statistics of an image.They demonstrated that their proposed scheme can defend against numerous familiar attacks, in particular, the lightening and darkening attacks through the results. Moreover, the host image is not modified by their scheme which does not need the original image to recognize the proprietorship. Consequently, the security of the digital images that cannot be modified, for instance medical images find their scheme to be appropriate. watermarking scheme which extracts both the grayscale watermark and the binary one from the protected images their scheme employed the pixel values of the original image to construct a grayscale watermark image. Then, their scheme intends to retrieve a binary watermark image by employing the just-procured-permuted grayscale watermark from the first phase. The outcome of their scheme is the lossless embedding i.e. the protected images and the original ones are identical when viewed. The authentication process in general does not necessitate the original image. Only the possessors of original grayscale watermark and the corresponding secret keys can extract the grayscale and binary watermarks in sequence. Thus, the system is enhanced in terms of security and robustness. Their proposed system fulfills the common necessities of image watermarking and is superior in comparison with the existing system in terms of transparency and robustness, which is demonstrated by the acquired results. Essentially, their watermarking scheme cannot resolve rightful ownership as the embedded watermark is detected without using the original image. Instead of protecting the ownership of digital images, the watermarking scheme in their algorithm protects the embedded watermark.

3.WATERMARK EMBEDDING

The embedding process of the binary watermark image into the host image is presented in this sub-section. The host image's size should be dyadic (2nx2n) and a binary image is used as watermark. Initially, the non-overlapping blocks of size 2x2 are extracted from the host image. A pixel of binary watermark image is embedded into a single block. The mean calculation, embedding strength (γ) and signum function are employed in the process of embedding the watermark. Originally, each onoverlapping block is converted into a vector, and the mean value of the vector is computed. Afterwards, the mean value is divided by the embedding strength (γ) and used in the embedding. As the watermark is a binary image, the bedding of watermark involves two cases: embedding pixel value '1' and embedding pixel value '0'. Two distinct mathematical operations are performed for mbedding pixel value '0' and '1'. Fig: 1 shows the block diagram of the watermark embedding process.

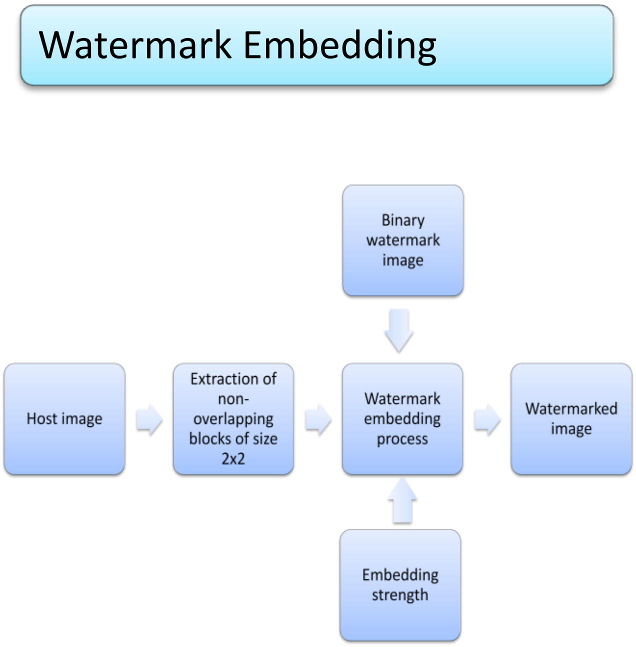

Fig. 1 Watermark Embedding Process

1. Host Image (I), Binary Watermark Image (W),
2. Embedding strength (γ)
3. Watermarked Image (WI)

4 WATERMARK EXTRACTION

The extraction of binary watermark image from the watermarked image is explained in this sub-section. As the Proposed sheme is blind, the extraction requires:watermarked image, size of watermark image, embedding strength and it doesn't require the original image or any of its characteristics. To begin with, 2x2 non overlapping blocks are extracted from the watermarked image and the number of blocks extracted depends on the size of the watermark image. The blocks thus extracted are stored in a vector. Afterwards all the extracted blocks are converted into a vector and the mean value of the vector is calculated. Subsequently the mean values of all the blocks are divided by the embedding strength. The resultant value is utilized in the extraction of watermark. Finally, a matrix with size of watermark image is initialized and the extracted pixel values are placed in it in order to obtain the watermark image. Fig. 2 portrays the block diagram of the watermark extraction process.

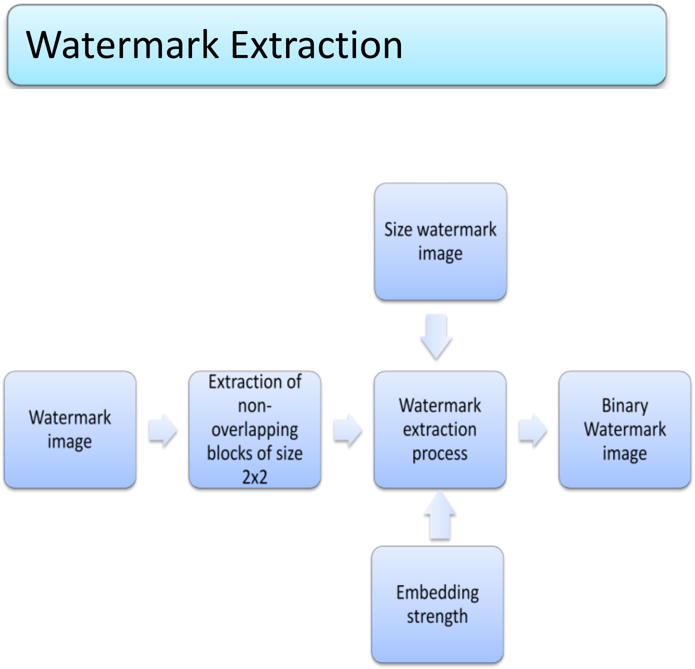

Fig.2 Watermark Extraction Process

1. Watermarked Image (WI), Size of watermark image W)
2. Embedding strength (γ)
3. Watermark Image (W)

5 SYSTEM OVERVIEW

5.1 Embedding:

For embedding a watermark into host image, first we need to select the secret image and host image. Then we have to specify the location and filenames for both watermarked image and key file.

Original image Secret image

Fig:5.1 Embedding

5.2 Extraction

For extracting the secret image from the watermarked image, first we need to select a watermarked image and key (text) file (size of watermark), which are saved while embedding. We need to provide the location and file name to save the retrieved image. We can view the images by choosing show screen window.

Watermarked image Secret image

Fig :5.2 Extraction

Watermarked image with PSNR value: **5.3706** He PSNR is defined as (Peak Signal-To-Noise Ratio)

$$PSNR = 10 \cdot \log_{10}\left(\frac{MAX_I^2}{MSE}\right)$$
$$= 20 \cdot \log_{10}\left(\frac{MAX_I}{\sqrt{MSE}}\right)$$

- Here, MAX_I is the maximum possible pixel value of the ima

- mean squared error (**MSE**) measures the average of the sqa of the errors. which for two $m\times n$ monochrome images I and where one of the images is considered a noisy approximatio of the other is defined as:

$$MSE = \frac{1}{mn}\sum_{i=0}^{m-1}\sum_{j=0}^{n-1}[I(i,j) - K(i,j)]^{\,2}$$

6 HISTOGRAM ANALSIS

Image Histogram was shown the number of pixels per gray level. In general more uniformed Histogram resulted less statistical attacks.

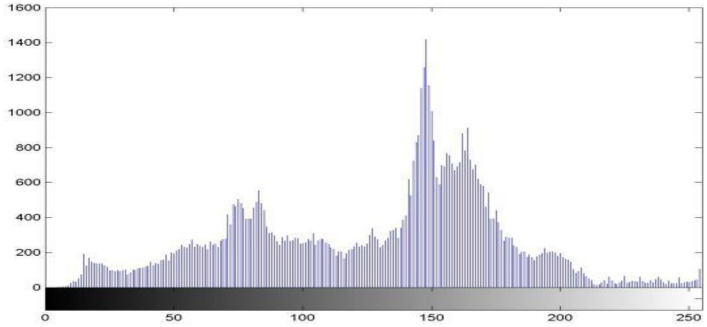

Fig: 6.1 Original image histogram

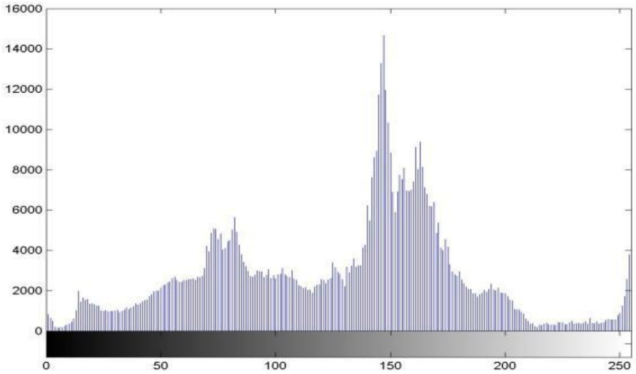

Fig 6.2 Watermarked histogram

Algorithm : Embedding

1: The water marking image(W) of size(r *c) consists of r*c number of pixels

2: Calculate the mean value for every 2*2 block B of the host image and store them in a vector V(B)

3: Divide the mean value 'V' of the vector by embedding strength

Q=V(B) / γ Where γ=2

4:The water marking bits are embedded into the block in vector B.using the perdetermind Q and embedding strength γ as follows

5: Calulate the **Signum** function of the each block in vector B and store it in another vector X

Sgn(X) +1, if x>0
0, if x=0
-1,if x<0
$\forall \in \text{sgn}(-x) = -\text{sgn}(x)$.

Similarly $/\,x\,/ = \text{sgn}(x)x$. if $x \neq 0$ then

also d/dx $/x/= \text{sgn}(x)$

6: The second property implies that for real non-zero x we

have $\text{sgn}(x) = x\,/\,/x/$

i) For pixel value '0' Follows

$$t = (\,(\,round\,(Q{*}0.5) * 2) *\gamma\,)$$

ii) For pixel value '1' Follows

$$Q\ t = (Q - 1)$$
$$t = (\,(\,round\,(Q{*}0.5) * 3) *\gamma\,)$$

```
        iii)  Multiply each block in vector $X$ by the alculated
    value $t$ with respect to watermark pixel and place it in vector
              .B= (X(i)*t);  Where $0 < i \le k$
7: Map the modified blocks in the vector $B$ back to its original
     position in host image $I$ to obtain the watermarked image
              ($W I$) .
```

Algorithm : Extraction

```
1: Extract 2x2 non-overlapping blocks from the watermarked
     image ( $W I$ )
2:  The number of extracted block B should be equiva lent to
     8 times the size of the water marking image store the in a
     vector(V)
3: Calculate the mean value of all the converted vectors $B V$ .
4: .Divide the calculated mean value $B V$ of all the vectors by
     the embedding strength $\gamma$.The value thus resulting is
     denoted as $Y$
          $Y=V(B) / \gamma$        Where $\gamma=2$
5: Perform the following mathematical operation and store the
     result in a vector $W$(p)
          W(p)=(Y[i]mod 2) ;     Where $0 < i \le$/w/

6: Initialize a matrix with size of watermark image and place
the   extracted pixel values ( $p W$ ) in it to obtain the
watermark     image ($W$) .
```

7 CONCLUSIONS

The development of electronic computer commerce applications and online services has been incredible in the recent times. However, the apprehension of unrestricted duplication and distribution of copyrighted material has crept in to the minds of service providers. As a digital watermark, a gray image is used. The gray image bits are embedded into 2*2 non-overlapping blocks of the host image. Subsequently, the watermark image is extracted from the watermarked image using the approach discussed. The watermarked images are in good visual quality and have good PSNR values entropy and histogram analysis. When entropy is considered for both cover image and secret image are identical with a deviation of 0.001% entropy which is supported by the histogram obtained. The effectiveness of the proposed scheme has been demonstrated the required degree of security with the aid of experimental results.

ACKNOWLEDGMENTS

I am thankful to my guide, Mr.Dr.T.V.S.Gireendranath who co-operated me through discussions and references.

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] Qiong Liu, Reihaneh Safavi-Naini and Nicholas Paul Sheppard, "Digital Rights Management for Content Distribution", Proceedings of the Australasian information security workshop conference on ACSW frontiers, Adelaide, Australia, Vol. 21, pp. 49 - 58, 2003 [4] Ian Kerr, "Hacking@privacy: Why We Need Protection from the Technologies That Protect Copyright", In proc. Of Conference on privacy and identity, 2007. [5] A. Piva, F. Bartolini, and M. Barni, “Managing copyright in open networks,” IEEE Trans. Internet Computing, vol. 6, no. 3, pp. 18–26, May–Jun. 2002.[6] 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. [7] Hans Georg Schaathun, "On watermarking/fingerprinting for copyright protection", First International Conference on Innovative Computing, Information and Control, ICICIC '06, Beijing, Vol. 3, pp. 50-53, Aug. 30 2006-Sept. 1 2006. [8] Authors Emir Ganic, Ahmet M. Eskicioglu, "Robust DWTSVD domain image watermarking: embedding data in all frequencies", International Multimedia Conference, Magdeburg, Germany, pp. 166 - 174, 2004. [9] Xiang-Yang Wang and Hong Zhao, "A Novel Synchronization Invariant Audio Watermarking Scheme Based on DWT and DCT", IEEE Transactions On Signal Processing, Vol. 54, No. 12, December 2006. [10] Miller, M.; Cox, I.J.; Linnartz, J.P.M.G.; Kalker, T., “A review of watermarking principles and practices,” In Digital Signal Processing in Multimedia Systems, Edit. K. K. Parhi and T. Nishitani, Marcell Dekker Inc., pp. 461-485, 1999. [11] 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. [12] 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. [13] Yeung, M. & Minzter, F., “An Invisible Watermarking technique for image verification,” Proceeding on the IEEE International Conference on Image Processing, pp: 680-683, 1997. [14] Shaowei Weng, Yao Zhao and Jeng-Shyang Pan, “A Novel Reversible Data Hiding Scheme,” International Journal of Innovative Computing, Information and Control, Vol. 4, No. 2, pp. 351-358, 2008. [15] Shih-Hao Wang and Yuan-Pei Lin,

"Wavelet Tree Quantization for Copyright Protection Watermarking", IEEE Transactions On Image Processing, Vol. 13, No. 2, February 2004. [16] Jengnan Tzeng, Wen-Liang Hwang, and I-Liang Chern, "An Asymmetric Subspace Watermarking Method for Copyright Protection", IEEE Transactions on Signal Processing, Vol. 53, No. 2, February 2005 [17] Ching-Sheng Hsu, Young-Chang Hou, "Copyright protection scheme for digital images using visual cryptography and sampling methods", Optical Engineering,Vol. 44, No. 7, July 2005. [18] Xu Zhou, Yu Ren, and Xuezeng Pan, "Watermark Embedded in Polygonal Line for Copyright Protection of Contour Map", IJCSNS International Journal of Computer Science and Network Security, Vol.6 No.7B, pp. 202-205, July 2006. [19] Ming-Chiang Hu, Der-Chyuan Lou and Ming-Chang Chang, "Dual-wrapped digital watermarking scheme for image copyright protection," Computers & Security, Vol. 26, No. 4, pp. 319-330,2007. [20] 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, October 2008. [21] W. Zeng and B. Liu, "A statistical watermark detection technique without using original images for resolving rightful ownerships of digital images", IEEE Transactions on Image Processing, Vol. 8, No. 11, pp. 1534-1548, 1999. [22] Zhe-Ming Lu, Wei-Min Zheng, Jeng-Shyang Pan and Zhen Sun, "Multipurpose Image Watermarking ethod Based on Mean-removed Vector Quantization", Journal of Information Assurance and Security, Vol. 1, pp. 33-42, 2006.
[23] Ming-Shi Wang and Wei-Che Chen, "Digital image copyright protection scheme based on visual cryptography and singular value decomposition", Optical Engineering, Vol. 46, No. 6, 2007. [24] Stefean Porubsky, "Signum Function", Retrieved 2009/4/30 from Interactive Information Portal for Algorithmic