Kurdistan Journal of Applied Research (KJAR)
Print-ISSN: 2411-7684 | Electronic-ISSN: 2411-7706
Volume 3 | Issue 1 | June 2018 | DOI: 10.24017/science.2018.1. 15

Received: June 1, 2018 | Accepted: June 25, 2018

Copyright Protection for Digital Certificate using Blind Watermarking Technique

Harith Raad Hasan
Computer Science Institute
Sulaimani Polytechnic University
Kurdistan Technical Institute
Sulaimani, Kurdistan, Iraq
Harith.hasan@spu.edu.iq | Harith.hasan@kti.edu.krd

Abstract - ***This paper proposes a copyright protection system for digital certificate image using blind watermarking technique by applying discrete wavelet transform algorithm (DWT). The proposed technique utilizes three interrelated watermarks namely, Red watermark (RW), Green-watermark (GW) and Blue-watermark (BW). Firstly, RGB cover and RGB watermark image are divided for three color space R,G,B. Then the R component is chosen for embedding (RW), the B component is selected for embedding the (BW) and the G component is selected for embedding the (GW), R,G and B of the cover image are converted into the transform domain using DWT, and is subsequently decomposed into three levels viz. LH1, LL2 and LL3 sub-bands. RW, GW and BW are then embedded onto LL3. Experimental results show that the performance of the proposed technique is very encouraging with average PSNR of 44 db, and NCC value of more than 0.99 for extracted watermarks after performing several types of attacks.***

Keywords: Digital Copyright Protection, Blind Watermarking Systems, Transform domain, Robustness, Discrete Wavelet transform (DWT).

1. INTRODUCTION

In recent years, The Internet and multimedia technologies due to the rapid growth, digital watermarking has become one of the important fields in image processing and multimedia research. This way can be driven to the need to protect multimedia digital contents from any person who want to make a manipulation in order to remove the ownership identity or to change the originality. In the past decades algorithms have been proposed like digital watermarking systems algorithms to solve the such issues. Digital watermarking methods can be classified into three main types which are Non-blind, Semi-blind and Blind techniques. In Non-blind watermarking schemes the information for original image and embedding information about watermarked image are known prior to watermark detection and extraction [1,2,3,4,5].

While, in Semi-blind approach a little information or a basic data is needed to extract watermark. In the blind watermarking system, extraction of the watermark image is performed which technically means no information is required [1,2,3,4]. Nevertheless generally, the blind approaches are more difficult than the non - blind and Semi- blind schemes in extraction stage especially after attacks. Moreover, in term of security and robustness stay the better [1,2,3]. For most application, security is considered as a vital aspect of digital watermarking techniques. Therefore, several studies suggest repeating the embedding for the same watermark, and this id known as a multiple watermarking [4,7].

2. LITERATURE REVIEW

Digital watermarking techniques can be categorized into two domains: the spatial domain and the transform domain [1,4,5,6]. The spatial domain watermarking enjoys the lower computational complexity [7,8,9], and is advantageous with respect to capacity and imperceptibility [10]. On the other hand, the transform domain is more superior in terms of robustness. The last but not the least the combination of the two domains is termed as the hybrid domain.

Transform based watermarking technique is well-known for its robustness against many types of attacks. In order to embed a watermark image, a transformation algorithm is applied to decompose the host image. Then, modifications are made to its coefficients. Possible transformation techniques include the Discrete Fourier Transform (DFT) [11], Discrete Cosine Transform (DCT), and Discrete Wavelet Transform (DWT) [1,5,12,13,14,15,16,19,20,21,22,]. On the other hand, spatial domain watermarking has been the fundamental scheme since the 90's. This domain makes use of selected bit-planes in a given host image for the watermark embedding process, consequently, some pixels of the host image are directly modified with respect to the image pixel values [3,17,18,23,24,25,26,27].

In 2009, Dejun et al [8] proposed a conversion of the cover image from the spatial to transform domain. The Low-Low (LL) sub-band of the image was used as the background for embedding the watermark. Then, the intermediate significant bit (ISB) (4^{th} bit-plane) of the cover image is used as a background for embedding the watermark in the spatial domain. The same watermark image was then formatted using the Arnold transform so that the spatial relationship of the visual recognizable part of the watermarked image can be distributed. Although their technique achieved good robustness and imperceptibility; however, its capacity is limited and computationally complex.

Moreover, Perumal and Kumar [13] proposed a DWT-based watermarking technique using thresholds on

intermediate bit values. In their work, they utilized four stages in the embedding process, which are: 1) the computation of DWT, 2) determination of thresholds based on intermediate bit values, 3) execute watermark embedding in ISB and 4) computation of inverse DWT. The L-level DWT transform was performed on the host image to obtain discrete wavelet components. Subsequently, a triple or a quad of pixels was utilized instead of pair of pixel, and then, the bits of the digital watermark bit-stream were embedded within the ISB bit values. The transformed image was then converted to the watermarked image via L-level inverse DWT conversion. However, performance of the method is poor in terms of both computational cost and robustness.

This paper focuses on capitalizing on the advantages of using three watermark images to increase the security and the robustness to ensure the originality of the digital certificate. In subsequent subsection, a brief discussion on Discrete Wavelet Transform (DWT) is presented.

The discrete wavelet transform (DWT), which is used for embedding through filter bank iteration, is one of the most popular transforms, DWT is a transform algorithm which uses Haar wavelets and operates as a high-pass filter and low-pass filter simultaneously Decomposition of 2D Haar wavelet is processed using 1D Haar wavelet decompositions on 1D horizontal arrays (row) determined by the horizontal scanning raster followed by 1D Haar wavelet decompositions on 1D vertical arrays (column) determined by the vertical scanning raster on the resulting image.

3. METHODS AND MATERIALS

The proposed technique utilizes three interrelated watermarks namely, Red watermark (RW), Green-watermark (GW) and Blue-watermark (BW). Firstly, RGB cover and watermark images are divided for three color space R,G,B. Then the R component is chosen for embedding (RW), the B component is selected for embedding the (BW) and the G component is selected for embedding the (GW), R,G and B of the cover image are converted into the transform domain using DWT, and is subsequently decomposed into two levels viz. HL1 and LL2 sub-bands. RW,GW and BW are then embedded onto LL2. The advantage of using three components of watermark image is to ensure the integrity of the watermarked image beside the high robustness. Two block diagrams are given in Fig. 1 and Fig. 2 below that represent the flow of the abovementioned methodology.

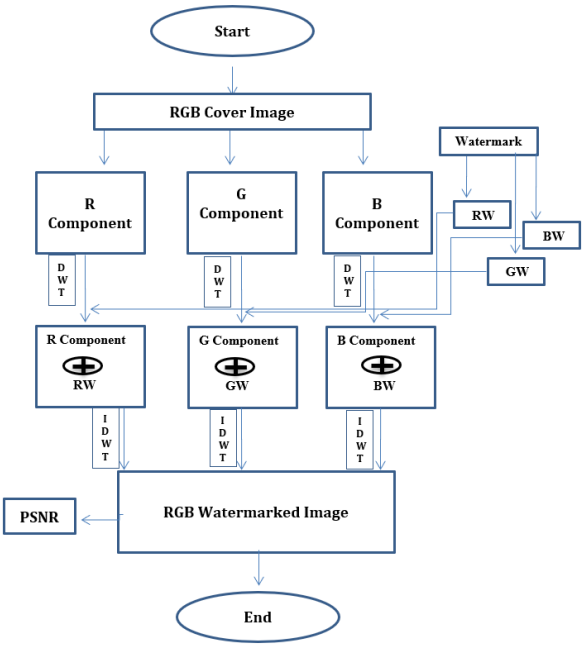

Fig. 1: Embedding stage of the watermarking technique

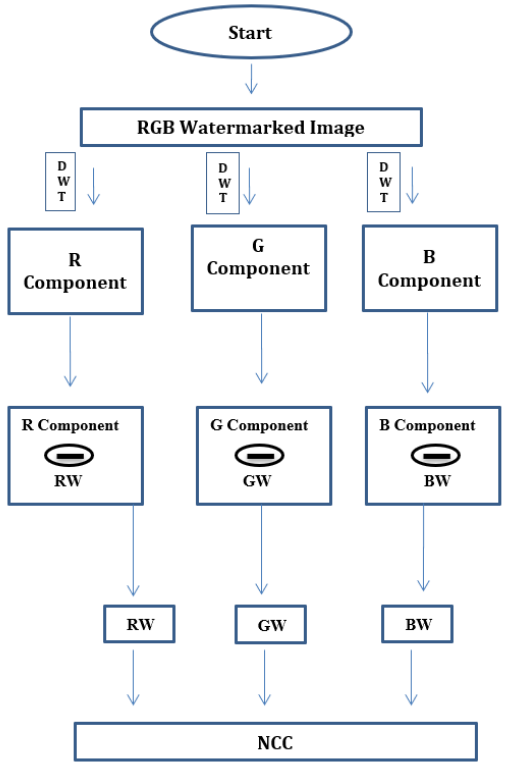

Fig. 2: Extraction stage of the watermarking technique

Pre-processing stage: At first, the RGB color image is divided to Red (R), Green (G) and Blue (B). Then R,G and B components are selected as the background for embedding the three watermark image Red Watermark image(RW),Green Watermark image (GW) and Blue Watermark image (BW). [5]

Embedding stage: It consists of three parts. For the first part, the embedding is performed on R component using DWT. The original size for the watermark image is a (64 X 64) pixels. Then, watermark image will divided to

create RW,GW and BW then RW is subsequently embedded onto the R. The embedding process will repeat in same procured on G and B components to embed the GW and BW. The embedding process is illustrated in Fig. 3.

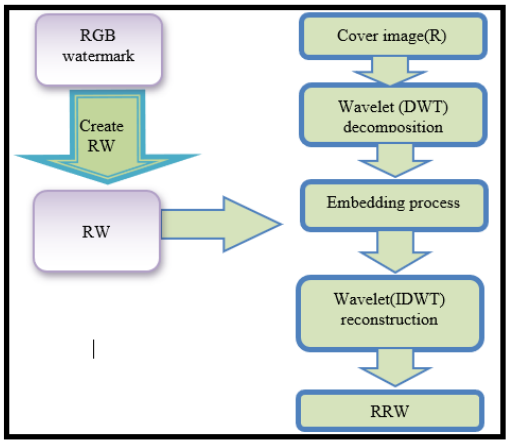

Fig.3: Embedding RW in transform domain

The DWT decomposes the R component from spatial domain to transform domain by changing its coefficient values and divide the R component two four sub-bands as Low-Low (LL), High-Low (HL), Low-High(LH) and High-High (HH). Then three levels of DWT are applied on the R. Level 1 is further divided into four frequency sub-bands, which are LL1, HL1, LH1, and HH1. The HL1 sub-band is then selected and level 2 is applied on it for further subdivision to four parts, which are LL2, HL2, LH2 and HH2. At this point the LL2 sub-band is then selected and level 3 is applied on it for further division to four more parts, which are LL3, HL3, LH3 and HH3. After all these divisions, the LL3 is finally selected for embedding the RW. The watermarked image is obtained by using the following equation:

$$\boldsymbol{LL3}\ (\boldsymbol{i},\boldsymbol{j})\ =\ \alpha\ x\ RW(i,j) \qquad \textbf{(1)}$$

Where α denotes a strength factor, (α between [0,1]), where α = 0.3 is chosen empirically;
RW (i,j) represents a R component of RGB watermark image.

Next, 3-level of IDWT is applied to create R-watermarked image (RRW). The embedding step is depicted in Fig. 4.

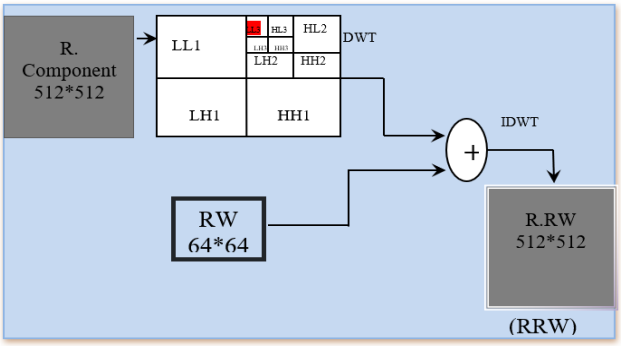

Fig. 4: Embedding process in transform domain

Upon the completion of the embedding phase, RRW, GGW and BBW components are merged, and then RGB color space to obtain a watermarked image is created.

Finally, an extraction process is performed to extract the watermarks RW,GW and BW. The same procedure as mentioned above is applied except it is done in reversal order.

4. RESULTS & DISCUSSION

The proposed technique is applied on the Kurdistan Technical Institute (KTI) Certificates after normalized the size to 512*512 pixels. Meanwhile, a RGB image of KTI logo sized 64*64 pixels is used as the main watermark image. A number of standard different attacks viz. Compression, Rotations, Resizing and some enhance filters are also applied to measure the robustness.

4.1. Performance evaluation

Two measurements are used to evaluate the performances of the proposed method namely, the Peak Signal-to-Noise Ratio (PSNR) and Normalized Cross Correlation (NCC). The PSNR is used to measure the ratio of image quality between the original host image and watermarked image. PSNR value above 30 db is considered as the perceptual fidelity value [16]. The following formulae are used to calculate the PSNR value:

$$\boldsymbol{PSNR} = \mathbf{10}.\log_{10}\left(\frac{\boldsymbol{MAX_I^2}}{\boldsymbol{MSE}}\right) = \mathbf{20}.\log 10\left(\frac{\boldsymbol{MAX_I}}{\sqrt{\boldsymbol{MSE}}}\right) \qquad \textbf{(2)}$$

$$\boldsymbol{MSE} = \frac{1}{\boldsymbol{mn}}\sum_{\boldsymbol{i=0}}^{\boldsymbol{m-1}}\sum_{\boldsymbol{j=0}}^{\boldsymbol{n-1}}[\boldsymbol{I(i,j)} - \boldsymbol{K(i,j)}]^2 \qquad \textbf{(3)}$$

Where m and n denote the image size of watermarked and host images; I(i , j) represents pixel(i,j) value of host image; K(i , j) denotes pixel(i,j) value of the watermarked image; and MAX denotes the image maximum intensity, which is usually equal to 255.

The NCC, on the other hand, is used to determine the quality of the watermarked image after the extraction [22], and is defined as:

$$\boldsymbol{NCC} = \frac{\sum_x\sum_y(\boldsymbol{W_{x,y}}\ \boldsymbol{x}\ \boldsymbol{W'_{x,y}})}{\sum_x\sum_y(\boldsymbol{W_{x,y}})^2} \qquad \textbf{(4)}$$

Where Wx,y is the pixel value of the original watermark image at (x,y) coordinate, and W'x,y is the pixel value of the extracted watermark image in the same position as that of the original watermark image.

4.2. Before attack results.

Table 1 illustrate the experimental results before the attack is taken place. The results revealed that average PSNR value is between 43 - 44db was achieved, which is

considered very high with respect to high capacity of the embedding three watermark images are used. The results also showed that the NCC values prior to attack for the extracted watermarks RW, GW and BW almost equaled to 0.99, which indicates that the watermarks are not affected at all (i.e. Identical with their original copies).

Table 1: PSNR and NCC values before attacks

Host Image	Watermark Image	PSNR	NCC of RW	NCC of GW	NCC of BW
C1	KTI Logo	44.67	1	1	1
C2	KTI Logo	43.33	1	1	1
C3	KTI Logo	43.01	1	1	1

4.3. After attack results.

When the standard attacks are Gaussian noise, Salt & Peppers, Sharpening, Median filter, Rotation and JPEG compression, applied on the watermarked image when the cover image was C1 and the watermark image a KTI logo, the key measurements are as in Tables 2.

Table 2: NCC values after standard attacks

Types of Attacks	NCC of RW	NCC of GW	NCC of BW
Gaussian noise	0.9978	0.9999	0.9998
Salt & Peppers	0.9999	0.9997	0.9999
Sharpening	0.9987	0.9987	0.9987
Median filter	0.9877	0.9900	0.9900
Rotation	1	1	1
JPEG compression	0.9777	0.9777	0.9777

When tested using all dataset images and the C1 is selected to calculate and evaluate the performance of the proposed technique was found the NCC after applied JPEG Compression was found the worst possible case which equal to 0.9777, but in the rest of test almost high performance was achieved. This is means the proposed method has a strong robustness that can withstand all the prescribed attacks.

4.4. Comparison

In the proposed technique, a three watermark is embedded on to three components of cover image using discrete wavelet transform. The selected of LH1 area, then chosen of the low frequency areas give the proposed technique more robust than high and middle frequency areas. This technique optimally searches for the best quadrant for embedding on to the host image and chooses three channels to achieve a high level of security. To gain security and robustness, it embeds the three watermark images in the low frequency sub-band (LL3). This strategy helps the proposed technique have the advantage of capacity and robustness while, at the same time, making the embedding process simple and easy to implement. It is hoped that ongoing research which will implement the use of DWT for embedding and extracting RGB images, will result in improved efficiency of the proposed technique. The proposed technique is compared to the system suggested by R. Thanki et al. [3]. Comparison between the proposed technique to that proposed by R. Thanki et al. is displayed in Tables 3 when applied the on the same cover image which used in R. Thanki et al. [3].

Table 3: Comparative with R. Thanki et al. [3].

Types of Attacks	Proposed Technique			R. Thanki et al. [3]		
	NCC 1	NCC 2	NCC 3	NCC 1	NCC 2	NCC 3
Gaussian noise	0.9999	0.9998	0.9999	0.9435	0.9946	0.9742
Salt & Peppers	0.9999	0.9999	0.9999	0.9436	0.9985	0.9725
Sharpening	0.9999	0.9999	0.9999	0.9534	1.0000	0.9755
Median filter	0.9977	0.99870	0.9980	0.9460	1.0000	0.9731
Rotation	1	1	1	0.9864	0.9891	0.9929
JPEG compression	0.9878	0.9988	0.9977	0.9474	0.9919	0.9753

5. CONCLUSION

In this paper, a new system which improves Copyright Protection for Digital Certificate Image using Blind Watermarking Technique is proposed. The new technique fulfills the two requirements which are important to identify the original certificate, namely: Security and robustness. Current research work is focused on embedding a multiple watermark image in different component of RGB image to see if it is advantageous with it. Finding the best ratio between the high frequency and low frequency parts of the watermark image and sorting out which part is suitable for embedding on to the cover image for both high and low frequency bands, is a challenge. The proposed technique takes into account Security and robustness beside to capacity and very good imperceptibility, which are a vital aspect of effective watermarking. Finally, the purpose of this proposed technique is to keep the digital certificate in secure mode and all the time the second party who will receive the digital certificate will be sure that the certificate is an original certificate after verifying the extracted watermark.

6. Future work

This section highlights some interesting future research directions laid down by this work. which requires further work will be how to connect this method with one of the optimization algorithms such as: Genetic algorithm (GA), Particle Swarm Optimization (PSO), and etc. to determine the optimal location of embedding for cover image based on the values of PSNR and NCC.

REFERENCE

[1] Y.Chang “A Blind Watermarking Algorithm” International Research Journal Of Engineering And Technology (IRJET), Volume: 04 Issue: 01 | Jan -2017.

[2] M. CEDILLO-HERNANDEZ, A. CEDILLO-HERNANDEZ, F. GARCIA-UGALDE” Digital Color Images Ownership Authentication Via Efficient And Robust Watermarking In A Hybrid Domain” RADIOENGINEERING, VOL. 26, NO. 2, JUNE 2017.

[3] R. Thanki And Vedvyas Dwivedi “A Watermarking Algorithm For Multiple Watermarks Protection Using RDWT-SVD And Compressive Sensing” Informatica 41 (2017) 479–493 479.

[4] C. Cox And M. Miller,(1997), A Review Of Watermarking And The Importance Of Perceptual Modeling, Proceedings Of Proc. SPIE, Vol. 3016, Pp. 92.
[5] M.S. Emami, Ghazali Bin Sulong, Jasni Mohamad Zain, 2011.“ A New Performance Trade-Off Measurement Technique For Evaluating Image Watermarking Schemes”, Communications In Computer And Information Science, Springer.
[6] R. G. V. Schyndel, A. Z. Tirke And C.F. Osborne, 1994.“A Digital Watermark”,Proc, Proceeding Of The 1st IEEE Image Processing Conference, Nov. 15-17, RMIT, Houston TX., Pp: 86-90.
[7] P. Taoa And A. M. Eskicioglub, 2004 “A Robust Multiple Watermarking Scheme In The Discrete Wavelet Transform Domain”, SPIE, Internet Multimedia Management Systems V, Vol. 5601, 133, Philadelphia, PA, USA.
[8] G. Bin Sulong, Harith Hasan**,** Ali Selamat**,** Mohammed Ibrahim And Saparudin, 2012. “A New Color Image Watermarking Technique Using Hybrid Domain”, IJCSI International Journal Of Computer Science Issues, Vol. 9, Issue 6, No 1.
[9] M. H. Al-Otum And N. A. Samara, 2010.“A Robust Blind Color Image Watermarking Based On Wavelet-Tree Bit Host Difference Selection.Pdf”, Signal Processing, Elsevier, Vol :90, PP 2498-2512.
[10] I. N. Wu, And M. Hwang, 2007. “Data Hiding: Current Status And Key Issues”, Ternational Journal Of Network Security, Vol.4, No.1, PP.1–9.
[11] Y. Dejun, Y. Rijing, Y. Yuhai And X. Huijie, 2009. “Blind Digital Image Watermarking Technique Based On Intermediate Significant Bit And Discrete Wavelet Transform”, *Proc*, International Conference On Computational Intelligence And Software Engineering, IEEE Computer Society.
[12] D. Zhang, J. Xu, H. Li And H. Li, 2009. “A Novel Image Watermarking Algorithm With Fast Processing Speed”, International Conference On Information Engineering And Computer Science, IEEE Computer Society.
[13] M. Ozturk, A. Akan And Y. Cekic, 2010. “A Robust Image Processing In The Joint Time-Frequency Domain”, EURASIP Journal On Advances In Signal Processing, Hindawi Publishing Corporation.
[14] S.Voloshynovskiy, F. Deguillaume, S. Pereira, And T. Pun, 2001. “Optimal Adaptive Diversity Watermarking With Channe State Estimation”, Proc, SPIE: Security And Watermarking Of Multimedia Contents.
[15] L. Li, B. Guo And J. Pan, 2008. ” Robust Image Watermarking Using Feature Based Local Invariant Regions”, International Journal Of Innovative Computing, Information And Control, Vol. 4, No. 8, PP. 1977-1986.
[16] M. S. Perumal And V.Vijayakumar, 2011. “A Wavelet Based Digital Watermarking Method Using Thresholds On Intermediate Bit Values” International Journal Of Computer Applications,Vol. 15, No.3.
[17] C. Chang, C. Lin And Y. Hu, 2007. “An SVD Oriented Watermark Embedding Scheme With High Qualities For The Restored Images”, International Journal Of Innovative Computing, Information And Control, Vol. 3, No. 3, PP. 609-620.
[18] M. Barni, F. Bartoloni, V. Cappellini, And A. Piva, 1998. “A DCT-Domain System For Robust Image Image Watermarking”, Signal Processing, Elsevier, Vol:66(3), PP 357-372.
[19] J. Bennour, Dugelay, J, And Matta, F, 2007. “Watermarking Attack (BOWS Contest”, Security, Steganography, And Watermarking Of Multimedia Contents, Proceedings Of SPIE-IS&T Electronic Imaging, Vol. 6505, Pp. 650518-1 - 650518-6, SPIE-IS&T.
[20] J. O’Ruanaidh, And T. Pun, 1997. “Rotation Scale And Translation Invariant Digital Watermarking”, Proc, IEEE Int’ Conf. On Image Processing, IEEE Computer Society, PP 536-538.
[21] G. Depovere, T. Kalker, And J. Linnartz, 1998. “Improved Watermark Detection Using Filtering Before Correlation”, International Conference On Image Processing, Vol. 1, Pp. 430,
[22] A. A. Mohammed, & Haval Sidqi, 2011.” Robust Image Watermarking Scheme Based On Wavelet Technique”. International Journal Of Computer Science And Security (IJCSS), 5.
[23] M. S. Emami, Ghazali And Salbiah 2012. A Novel Multiple Semi-Blind Enhanced ISB Watermarking Algorithm Using Watermark Bit-Pattern Histogram For Copyright Protection. International Journal Of Innovative Computing, Information And Control. 8(3.), 1665-1687.
[24] M.Khalili 2003. “A Comparison Between Digital Images Watermarking in Tow Different Color Spaces Using DWT ”. National Academy of Science of Armenia Yerevan, Armenia.
[25] C. Kung, S. Chao, Y. Tu, Y. Yan and C. Kung, 2009. “A Robust Watermarking and Image Authentication Scheme used for Digital Content Application”, Journal of Multimedia, Vol. 4, No. 3.
[26] K. Deb, S. Agrawal, A. Pratab, T. Meyarivan, “A Fast Elitist Non-dominated Sorting Genetic Algorithms for Multiobjective Optimization: NSGA II,” KanGAL report 200001, Indian Institute of Technology, Kanpur, India, 2000. (technical report style)
[27] J. Geralds, "Sega Ends Production of Dreamcast," vnunet.com, para. 2, Jan. 31, 2001. [Online]. Available: http://nl1.vnunet.com/news/1116995. [Accessed: Sept. 12, 2004]. (General Internet site).