IJESMR

International Journal of Engineering Sciences & Management Research

A HYBRID BLIND WATERMARKING SCHEME FOR SECURING E-GOVERNMENT DOCUMENT IMAGES

Samiksha Soni*[1], Manisha Sharma[2]
[*1,2]Department of Electronics and Telecommunication Engineering, Bhilai Institute of Technology, Durg, Chhattisgarh, INDIA
*Correspondence Author: samiksha.soni786@ gmail.com

Keywords: E-Government, Digital watermarking, DCT, SVD

ABSTRACT

With the advancement of information technology the ways of sharing information has become easier, cheaper and instant. This advancement has also changed the scenario of sharing information among government organization. E-governance is related to providing digital information of programmes and policies of the governments to its citizens in quick and transparent manner. This paper deals with the security issues in e- governance and a blind copyright protection scheme is developed for e-document images. In this paper a secure and robust watermarking scheme is developed by the integrated use of DCT and SVD. Robustness and transparency of proposed work is analyzed under various attack with varying payload. Experimental result shows that proposed work posses great robustness for random noise, salt and pepper noise, compression, cropping, row column blanking and row column copying attacks which is being evaluated from the values of NC, PSNR and BER.

I. INTRODUCTION

E-Government is among one of the major applications of information technology aims at providing information for the service of citizens, businesses and other areas of Government [1]. Main purpose of E-Government is to provide ease of access of government information and services to its citizens. This approach helps in providing better transparency among government and citizens that also leads to improvement in the quality of the services [2]. Thus we can say that e-government system provides overall efficient systems but as it is based on communication based technologies. So security is the key issue for an efficient e-government system. Some of the security issues in e-government are discussed below [3]:

- Confidentiality- Unintended users cannot access the information.
- Authenticity- When information is received; it should be verified by a person or a project claiming to be originator and vice versa.
- Integrity- At receiver end content of information must be exactly same as at that of sender's end
- Non- repudiation- After authorizing a message the sender should be unable at a letter time, denying having done so.

Thus e-Government system must be very secure enough to meet the above stated security aspects. Security, authenticity and verification should go with privacy laws and Government has to ensure the efficient protection of confidentiality and privacy of information. Digital watermarking is basically identified as a tool for copyright protection of digital data but due to its inherent characteristics it may improve the security feature of e-Government system.

II. DIGITAL WATERMARKING AS A SECURITY TOOL

Digital watermarking helps in protecting the digital data by inserting additional information in original digital data. Insertion of additional information is considered as noise thus care should be taken to obtain high peak signal to noise ratio. Watermark should be inserted in a way so that if illegitimate user have sense of digital data being watermarked it is hard to remove watermark from digital data. Watermark may contain security feature such as document serial number or other information related to data to originator such as date of birth. Watermarked document can give the information about modifications, counterfeits by comparing the watermarked data to original data. The watermark content depends upon the originator or needs to ensure the integrity of the information as well as authentication of the documents. Digital watermarking techniques can be categorized as private and public watermarks [4][8][9].

2.1. PRIVATE WATERMARKS

Private watermark is used to prove ownership in disputes. Secret key is required for retrieving the watermark information which is known only to intended sender. Private watermarks should ensure high robustness whereas got relaxation from heavy payload capacity

2.2. PUBLIC WATERMARKS

A public watermark is retrieved by the receiver of copyrighted material. It usually contains copyright or licensing information, such as the identifier of the copyright holder, the creator of the material, or a link (URL) through which to fetch more related information. A public watermark puts heavy demands on a watermarking algorithm regarding capacity.

III. PROPOSED WATERMARKING SCHEME

In the proposed work we integrated two major mathematical tools DCT and SVD [6][7] to develop a secure and robust watermarking scheme. First DCT operation is performed on original image to obtain its frequency components. Then reordering of DCT components is done in zigzag manner. After that block SVD operation is performed on scanned DCT coefficients then watermark is embedded inside the largest SV's of each block.

3.1. WATERMARK EMBEDDING PROCEDURE:

In first step convert the original color image in to gray scale. Then apply 2-D DCT to the gray scale image of scanned e-documents and perform the zigzag scanning operation on DCT coefficients shown in Eq. (1) and Eq. (2). Let the gray scale image be A

$$A_d = \mathrm{DCT2}(A) \qquad (1)$$
$$Z_d = \mathrm{Zigzag}(A_d) \qquad (2)$$

In next step two dimensional matrixes is formed from the zigzag scanned vector

$$M = \mathrm{Con2\_matrix}(Z_d) \qquad (3)$$

After that Matrix M is fractioned in to smaller blocks depending on the payload size $\left(m_{1,}m_{2,\dots\dots,}m_n\right) = \mathrm{divi}(M)$ where n is equal to watermark length, then using Eq. (4) SVD operation is performed on this blocks

$$[U_i S_i V_i] = \mathrm{svd}(m_i) \qquad (4)$$

Where i=1,2,3,4…….,n
After applying DCT SVD operation on original image the binary watermark is inserted by the following ways:

Modify the largest singular value of each block as

$$Y_i = S_i(1,1) \bmod Q$$

Where Q is predefined quantizing value, Q must be selected with the specification of an image both to obtain a maximum resistance towards attack and to obtain the minimum perceptibility.

When $W_i = 0$ it will be embedded as follows:

If $Y_i < 3Q/4$, then $S'_i(1,1) = S_i(1,1) + Q/4 - Y_i$ else $S'_i(1,1) = S_i(1,1) + 5Q/4 - Y_i$

When $W_i = 1$ it will be embedded as follows:

If $Y_i < Q/4$, then $S'_i(1,1) = S_i(1,1) - Q/4 - Y_i$ else $S'_i(1,1) = S_i(1,1) + 3Q/4 - Y_i$

Next check for negative $S'_i(1,1)$, if $S'_i(1,1)$ is negative modify $S'_i(1,1) = Q/2$

Next step is to perform inverse SVD operation on blocks to obtain modified DCT coefficients $m'_i = \mathrm{ISVD}(U_i S'_i V_i)$ and smaller blocks are recombined by$M' = \mathrm{merg}(m'_1, m'_2, \dots, m'_n)$, after that inverse zigzag operation is performed on M' to map DCT coefficients back to their position$A'_d = \mathrm{IZigzag}(M')$. Last step is to perform inverse DCT operation on A'_d using Eq. (5) to obtain watermarked imageA'
.

3.2. WATERMARK EXTRACTION PROCEDURE

The first step of the watermark-extraction process is to apply DCT to the watermarked image as shown in Eq. (5)

$$A'_{dr} = \mathrm{DCT2}(A') \qquad (5)$$

In Step two, using Eq. (6) scan the DCT coefficients in the zigzag manner

$$Z_{dr} = \mathrm{Zigzag}(A'_{dr}) \qquad (6)$$

After that two dimensional matrixes is formed from scanned vector using Eq. (7)

$$M_r = \mathrm{Con2\_matrix}(Z_{dr}) \qquad (7)$$

In step three matrix M_r is fractioned in to smaller blocks depending on the payload size $(m_{r1,} m_{r2,\dots\dots,} m_{rn}) = \mathrm{divi}(M_r)$ where n is equal to watermark length, then SVD operation is performed on this blocks as shown in Eq. (8)

$$[U_{ri} S_{ri} V_{ri}] = \mathrm{svd}(m_{ri}) \qquad (8)$$

Where i=1, 2, 3, 4……., n. In step four get the largest singular values from each block and extract the watermark

$Y_{ri} = S_{ri}(1,1) \mathrm{mod}\ Q$

If $Y_{ri} < Q/2$, then $W_{ri} = 0$, else $W_{ri} = 1$, these extracted bit values are used to construct the extracted watermark.

IV. RESULTS AND DISCUSSION

To verify the performance of the proposed watermarking algorithm, MATLAB platform is used and a number of experiments are performed on different e-document images of size 512×512 and binary logos of size 64×64, 128×128, 256×256.Here we provide the results for scanned image of Elsevier journal paper and SSC admit card with two different binary logos of size 128x128 shown in Figure 1 and Figure 2.

Fig:1. Simulation result with elsevier document scanned image

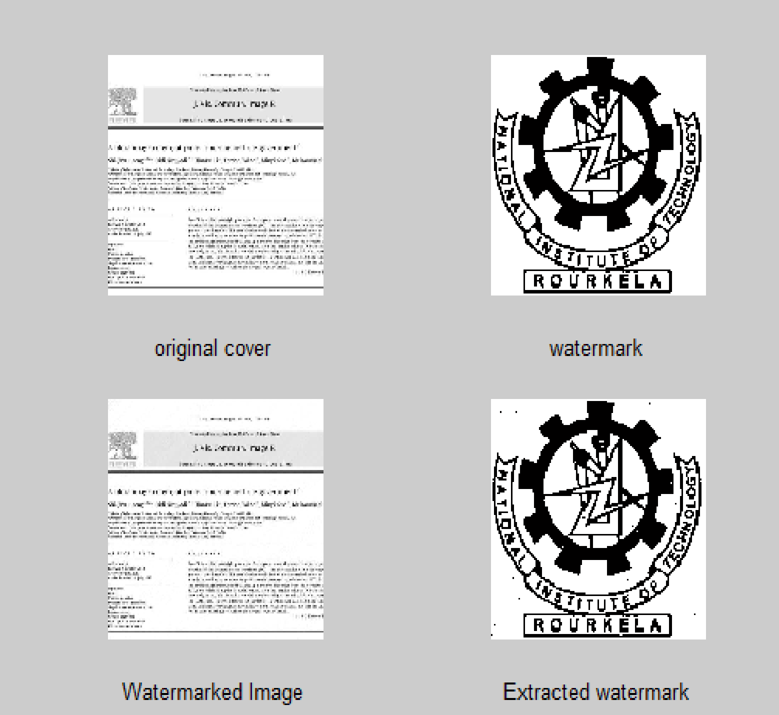
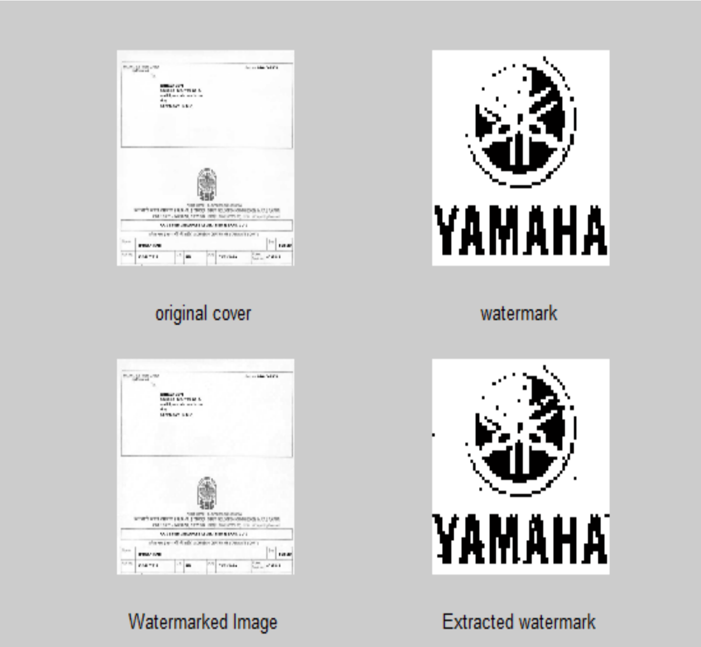


Fig:2. Simulation result with SSC admit card scanned image



The watermarked image quality is measured using PSNR (Peak Signal to Noise Ratio) given by Eq. (9).To verify the presence of watermark, two parametric measures are used to show the similarity between the original watermark and the extracted watermark. These two parameters are normalized correlation and bit error rate given by Eq. (9) and (10)

$$\mathrm{PSNR} = 10\mathrm{Log}_{10}\left[\frac{\sum_{i=1}^{N}\sum_{j=1}^{N}(A'(i,j))^2}{\sum_{i=1}^{N}\sum_{j=1}^{N}(A(i,j)-A'(i,j))^2}\right] \qquad (9)$$

$$\mathrm{NC} = \left[\frac{\sum_{i=1}^{N}\sum_{j=1}^{N}(w(i,j)-w_{mean})(w'(i,j)-w'_{mean})}{\sqrt{\sum_{i=1}^{N}\sum_{j=1}^{N}(w'(i,j)-w'_{mean})^2\sum_{i=1}^{N}\sum_{j=1}^{N}(w(i,j)-w_{mean})^2}}\right] \qquad (10)$$

$$\mathrm{BER} = \frac{\sum_{i=1}^{N}\sum_{j=1}^{N} w(i,j)\oplus w'(i,j)}{N\times N} \qquad (11)$$

Where w(i, j) be the original watermark image and the extracted watermark be w'(i, j) original watermark image and the extracted watermark be w'(i, j).

In order to check the robustness of the proposed watermarking scheme the watermarked image is attacked by a variety of attacks namely Average and Median Filtering, Gaussian noise, Random noise, JPEG Compression, Cropping, Resize, Rotation, and Blur. After these attacks on the watermarked image, the extracted logo is compared with the original one.

- Addition of noise

Noise addition in watermarked image is another way of checking the robustness of the system. Noise addition leads to degradation and distortion of the image. Which affects the quality of extracted watermark? Here robustness is checked against salt and pepper noise and random noise as shown in figure 3 and figure 7.

- JPEG compression

Another most common manipulation in digital image is image compression. To check the robustness against Image Compression, the watermarked image is tested with JPEG100 and JPEG2000 compression attacks as shown in figure 4 and figure 8.

- Cropping

Cropping is the process of selecting and removing a portion of an image to create focus or strengthen its composition. Cropping an image is done by either hiding or deleting rows or columns. In the proposed work three variants of cropping is performed they are row column blanking, row column copying, cropping by deleting 70% area of top left corner as shown in figure 5, figure 6 and figure 9.

Fig:3. Simulation result under random noise attack

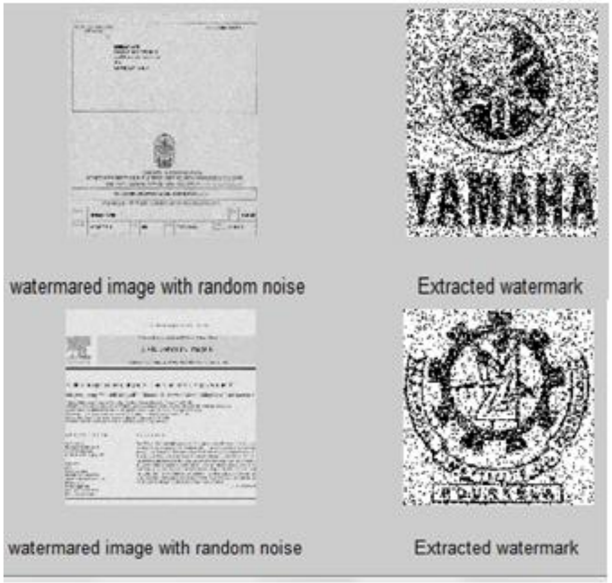

YAMAHA
watermared image with random noise
Extracted watermark
watermared image with random noise
Extracted watermark

Fig:4. Simulation result under JPEG compression attack

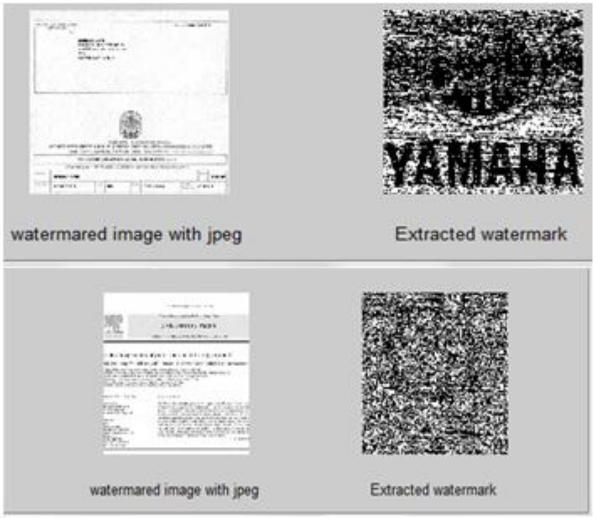


Fig:5. Simulation result under row column copying attack

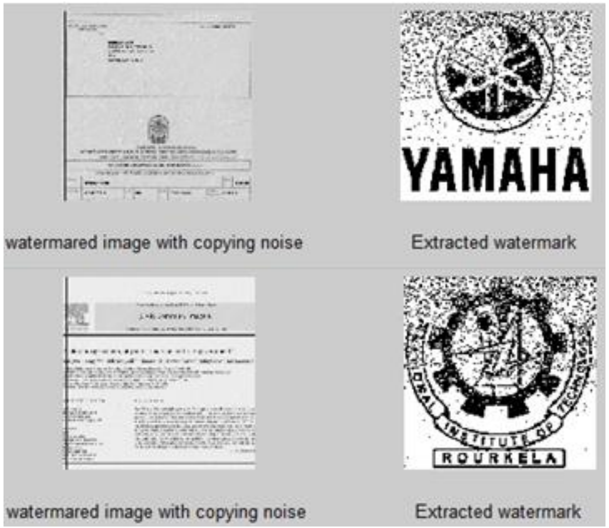

YAMAHA
watermared image with copying noise
Extracted watermark
NATIONAL INSTITUTE OF TECHNOLOGY
ROURKELA
watermared image with copying noise
Extracted watermark

Fig:6. Simulation result under row column blanking attack

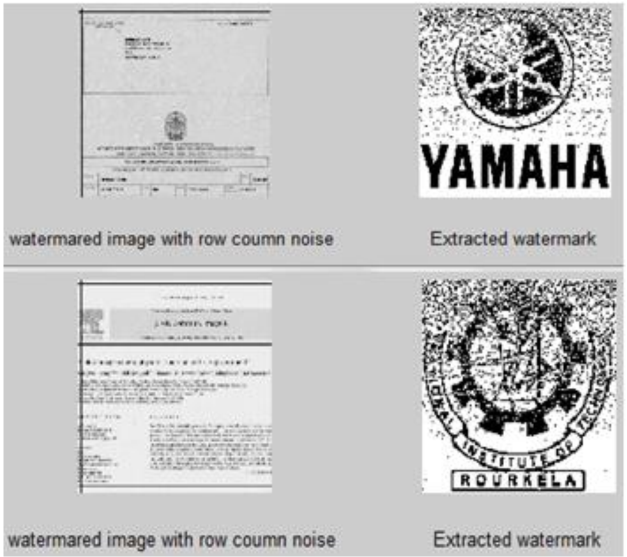

YAMAHA
watermared image with row coumn noise
Extracted watermark
INSTITUTE OF
ROURKELA
watermared image with row coumn noise
Extracted watermark

Fig:7. Simulation result under salt and pepper noise attack

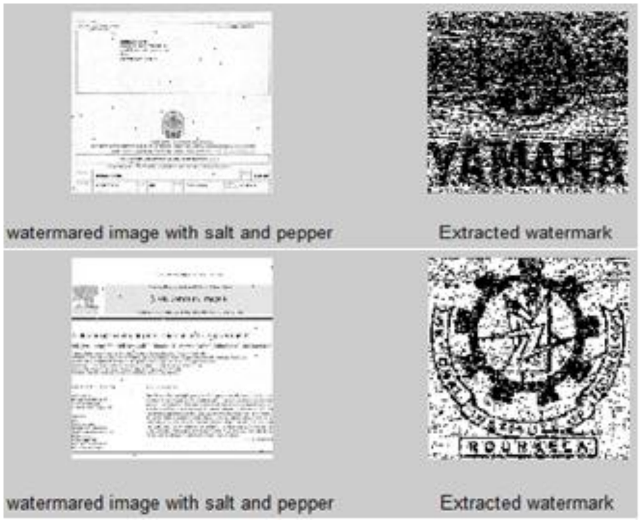

YAMAHA
watermared image with salt and pepper
Extracted watermark
ROURKELA
watermared image with salt and pepper
Extracted watermark

Fig:8. Simulation result JPEG2000 attack

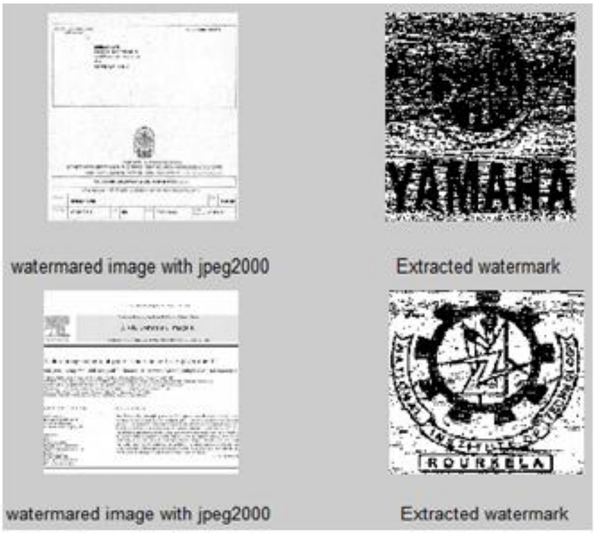
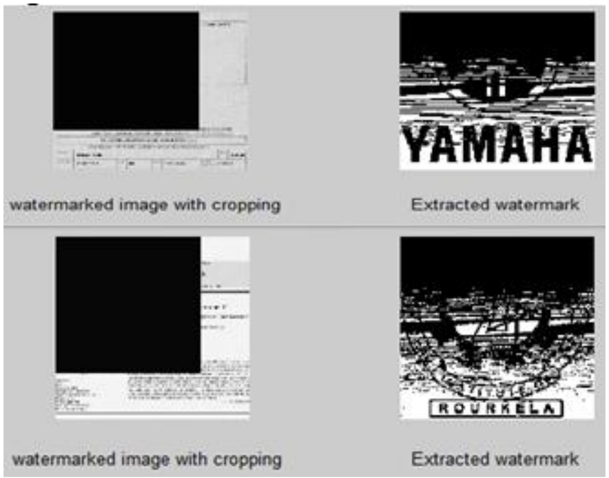

watermared image with jpeg2000
Extracted watermark
YAMAHA
watermared image with jpeg2000
Extracted watermark
ROURKELA

Fig:9. Simulation result under cropping attack


watermarked image with cropping
Extracted watermark
YAMAHA
watermarked image with cropping
Extracted watermark
ROURKELA

Types of attack	Image	NC	BER	PSNR
Without attack	SSC	0.9923	0.0030	42.0120
	Elsevier	0.9959	0.0003	40.2806
Random noise	SSC	0.4399	0.2093	33.1035
	Elsevier	0.5913	0.1793	33.1984
Crop	SSC	0.4812	0.3930	5.0500
	Elsevier	0.4647	0.4307	5.7196
JPEG 100	SSC	0.6448	0.2000	37.1100
	Elsevier	0.6891	0.3558	36.727
JPEG2000	SSC	0.8823	0.0060	41.2098
	Elsevier	0.4142	0.2415	30.0789
Salt & Pepper	SSC	0.7662	0.0996	31.0040
	Elsevier	0.4142	0.2415	30.0789
Row Column Blanking	SSC	0.8098	0.1000	28.3100
	Elsevier	0.7183	0.1505	26.6090
Row Column Copying	SSC	0.8816	0.0501	29.1211
	Elsevier	0.7682	0.1220	29.3956

Table 1. Parametric measures for evaluating robustness and perceptibility with payload of 128x128

Types of attack	Image	NC	BER	PSNR
Without attack	SSC	0.9897	0.0051	47.5611
	Elsevier	0.9859	0.0063	48.2806
Random noise	SSC	0.6620	0.1658	33.9148
	Elsevier	0.6590	0.1788	34.3213
Crop	SSC	0.4526	0.4216	5.7900
	Elsevier	0.4321	0.4678	5.9203
JPEG 100	SSC	0.9452	0.0278	42.9521

	Elsevier	0.9345	0.0510	43.2100
JPEG2000	SSC	0.9644	0.0178	46.9864
	Elsevier	0.9500	0.0218	48.1000
Salt & Pepper	SSC	0.8819	0.0583	30.2117
	Elsevier	0.8762	0.0657	32.0121
Row Column Blanking	SSC	0.6930	0.1624	26.6234
	Elsevier	0.6690	0.2300	28.9012
Row Column Copying	SSC	0.7842	0.1121	29.4226
	Elsevier	0.7700	0.2501	30.2359

Table 2. Parametric measures for evaluating robustness and perceptibility for payload of 64x64

Types of attack	Image	NC	BER	PSNR
Without attack	SSC	0.9999	0.0004	33.0320
	Elsevier	0.9899	0.0006	35.1412
Random noise	SSC	0.5514	0.2355	30.3307
	Elsevier	0.5325	0.3319	32.3501
Crop	SSC	0.5225	0.4483	5.7890
	Elsevier	0.5100	0.4891	5.9010
JPEG 100	SSC	0.4886	0.4813	34.3801
	Elsevier	0.4671	0.4910	35.6714
JPEG2000	SSC	0.4822	0.4621	34.8921
	Elsevier	0.4717	0.4847	35.923
Salt & Pepper	SSC	0.3822	0.4641	29.2650
	Elsevier	0.3610	0.4891	30.5671
Row Column Blanking	SSC	0.8049	0.1072	26.5313
	Elsevier	0.7810	0.2110	28.1121

Row Column Copying	SSC	0.8271	0.0970	29.2410
	Elsevier	0.8101	0.1001	31.0910

Table 3. Parametric measures for evaluating robustness and perceptibility for payload of 256x256

Type of attack	Proposed work	Horng et al.
Optimization/ Iteration	No	yes
	PSNR	PSNR
Cropping 60%	09.92	06.30
JPEG Compression(50)	36.27	34.27
Salt & Pepper Noise(0.02)	25.14	22.61

Table 4. Comparison between proposed method and Horng et al. method

V. CONCLUSION

In this paper applicability of information technology in government organization and various security issues is discussed in detail. To resolve one of the security issues of e-government system a blind watermarking system for copyright protection for e-document image is proposed. Experimental results shows that watermark can be successfully extracted from uncropped portion of image, great robustness towards row column blanking and row column copying attack. However the resistivity towards rest of attacks is dependent on type of document and logo used for watermarking.

VI. REFERENCES

[1] E-government in India: Opportunities and challenges, JOAAG, Vol.3

[2] Didi Rosiyadi, Shi-Jinn Horng, Pingzhi Fan, Xian Wang, Muhammad Khurram Khan, Pan Yi, An efficient copyright protection scheme for e-government document images, IEEE Multimedia 19 (3) (2012) 62–73.

[3] Sengupta, A., Mazumdar, C. and Barik, M.programmes., "e-Commerce security – A life cycle approach", in Sadhana, Journal of the Indian Academy of Sciences, Bangalore, India, Vol. 30, Part 2 & 3, April/June 2005, Pages 119-140.

[4] Fernando P. Gonzalez and Juan R. Hernbdez, " A TUTORIAL ON DIGITAL WATERMARKING, " IEEE Trans. on Information Forensics Security, 1999

[5] NIST (National Institute of Standards & Technology), Thornton, J. (2004). E-Authentication Guidance. available at http://csrc.nist.gov/kba/Presentations. Accessed Sept. 2007.

[6] *Sun, R., Sun, H., Yao, T., "A SVD and quantization based semi-fragile watermarking technique for image authentication", Proc. IEEE International Conf. Signal Process, 2002., pp. 1592-95.*

[7] *A. Sverdlov, S. Dexter, and A.M. Eskicioglu, ''Robust DCT-SVD Domain Image Watermarking for Copyright Protection: Embedding Data in all Frequencies'', Proceedings of 13th European Signal Processing Conference (Eusipco), 2005; http://www.theparticle. com/documents/EUSIPCO_2005-WM.pdf. , pp.1099–1105.*

[8] *Engineering Principles for IT Security –NIST document*

[9] *Clarkke, R. A hidden challenge to the regulation of data surveillance, Journal of Law and Information Science 4(2), 1993. No. 2, 2008.Accessed from www.epaper.techbarrack.com on 2012-04-08*

VII. AUTHOR BIBLOGRAPHY

	Samiksha Soni was born in Chhattisgarh, India in 1988.She received the B.E. degree from CSVTU, Pursuing M.Tech. degree at the CSVTU, Bhilai , India. Her research interests include Image Processing, Watermarking, Cryptography, Steganography.
	Dr. Manisha Sharma was born in 1970. She received the B.E. from Barkhattullah University, Bhopal in 1992 , M.E. from Government Engineering College, Jabalpur Rani Durgavati University, Jabalpur in 1995 and Ph.D. from C.S.V.T.U., Bhilai, India in 2010. Presently she is working as a professor & Head of the department at, Bhilai Institute of Technology, Durg, CHHATTISGARH, India. Her research Interest includes Image Processing , Image Segmentation , Video Processing , watermarking and Authentication