Watermark Captioning for Images in E-Governance

Jobin Abraham[#], Varghese Paul[*]

[#]*BPC College, Piravom, Kerala, India*
**CUSAT, Kochi, Kerala, India*

[#]jnabpc@gmail.com
[*]vp.itcusat@gmail.com

***Abstract*— Watermarking is well known as a tool for copyright protection of documents. Digital watermarking is also useful for content authentication and tamper detection. Watermarking could be migrated to e-governance for enhancing security of various e-governance applications. Successful e-governance implementation requires all digital documents issued by the government is protected from illegal attacks attempting to modify the original contents. This paper proposes a method for uniquely watermarking images, including photographs and biometric images collected from the public by various government agencies. Method also proposes any digital certificates or documents issued by the government can be watermarked. The integrity and authenticity of these documents can thus be ascertained.**

***Keywords*— Image Watermarking, DCT, e-governance, security, psnr**

I. INTRODUCTION

Over the years Internet has emerged as the biggest network and now, is the main framework for information transfer and communication. Along with internet, usage of digital data formats gained popularity mainly due to its easiness in storage, editing, availability of data recovery and error correction techniques. Though digital data formats are very convenient, most of its advantages are offset by the fact that digital data lend very easily to illegal attacks as copying and misuses after modifying the original contents. As a result, the intellectual copyright protection and authentication has become a prime concern while using the Internet for communication and business applications. Digital watermarking is used to address these issues and resolve them to a great extent.

Digital watermarking is the process of embedding an identification signal known as watermark imperceptibly and securely within a host media [1, 2]. These hidden Watermarks can authenticate the originality of the contents [3]. Watermarking techniques can be broadly grouped into two as spatial domain methods and transform domain methods. Spatial domain based techniques use LSB substitution method or histogram modification for integrating watermark bits inside the host media. Transform domain techniques uses DCT, DFT or DWT transforms for selecting the regions in the image for hiding the watermark signal.

This paper proposes a DCT based image watermarking scheme. DCT segments the image into three regions as high frequency, medium frequency and low frequency regions. Low frequency regions represent most of the visual characteristics of the image. Modifications in medium frequency regions do not degrade the visual features of the image much. Hence medium frequency regions are used to embed the watermark. Also medium frequencies are less exposed to noise attacks compared to high frequency components [4, 5].

The paper is organized as follows. Section II briefly discuss the security issues in e-governance and also proposes few applications for watermarking in e-governance. Section III introduces the watermarking algorithm. Section IV is experimental analysis and results from the study and finally, the conclusion is in Section V.

II. WATERMARKING IN E-GOVERNANCE

A. Security issues in E-Governance

Though the governments spend a lot over e-governance and infrastructure development, the public seldom accepts these initiatives instantly. Fear of lack in security and other similar concerns prevent public from accepting and using most of e-Governance or e-Commerce applications. The security of citizen's data and other related confidential government documents is a key issue for the government while adopting e-Governance [6].

The biggest security challenges faced are authentication, integrity verification and protection of the digital multimedia contents [7]. Conventional access control and other firewall mechanism effectively protect the resources residing in the data bases. However, any pitfalls in such protections mechanism can lead to data leakages in the form of unauthorized downloads and illegal tampering. Several other data protection mechanism as cryptography, steganography,

watermarking, digital rights management (DRM) etc are available and can be applied in many ways for enhancing the security of the system. Hence, e-security now is not just firewalls and anti-viruses for intruder prevention and protecting digital contents.

B. Proposed Uses for Digital Watermarking

As a part of E-Governance implementation large amount of documentation works are underway. Documents as government employee details, police records, land records etc are digitalized. These documents can be more securely safeguarded using watermarking along with other conventional data security mechanisms [8]. Watermarked documents can be easily traced to their source using their hidden watermarks. Many instances of content tampering and unauthorized redistributions of the documents can be discouraged.

A method for watermarking photographs or an image, in general, is described in the following sections. As a part of the AADHAAR project, the government of India is issuing UID (Unique Identification Number) for all 1.2 billon citizens. Several data's including the photograph and fingerprints is to be collected [9, 10]. The proposed method explains how the various images collected from an individual can be watermarked using the UID itself. When watermarked using a specific UID, the watermark forms a basic link between all the resources collected from a single individual. This common chord also reduces the chances of data linking error between varied resources pertaining to a person.

In short, watermarking can be adopted for the following in e-governance:

- Captioning the images and other multimedia documents uniquely to address its owner
- Linking various related documents and images of an individual.
- Forgery detection when images or a photograph of an individual is replaced with another image.

III. IMAGE WATERMARKING ALGORITHM

The watermarking process comprises two stages: Watermark Embedding and Watermark Extraction. The core of any watermark embedding process is an algorithm which securely hides a watermark signal into the host media. Robustness of watermarked images to signal processing attacks depends greatly on the strength and non-decode ability of the algorithm employed.

The proposed method uses discrete cosine transform (DCT) for watermarking. As the watermark signal, we use the unique twelve digits UID assigned to each citizen by the government [11]. The UID may be embedded into all documents and images collected from an individual and whenever required, the integrated watermark can be extracted for authentication.

A. Watermark Embedding Algorithm

Consider a photograph image, I and let the watermark, w, be his twelve digits UID. The original image is decomposed into four sub-images, I_1, I_2, I_3 and I_4, prior to applying the embedding algorithm. Image I is segmented into sub-images as:

$I_1(p, q) = I(i, j)$,
$I_2(p, q) = I(i, j+1)$,
$I_3(p, q) = I(i+1, j)$ and
$I_4(p, q) = I(i+1, j+1)$ for i =1, 3, 5,7 ….N-1 and p, q = 1,2,3…N/2.

The sub-images will be visually alike as they share the neighbouring pixels. These sub-images are compared block-wise to select suitable positions for hiding the watermark bit. Detailed steps for watermark insertion are outlined below.

1. Input the host image I, of size M x M.
2. Pre-process the watermark to binary one dimensional array, W_k, k = 1 to m, where m is number of bits.
3. Decompose the image into four sub-images, I_1, I_2, I_3 and I_4, each of size M/2 x M/2.
4. Consider first set of four 8x8 blocks $f1_i$, $f2_i$, $f3_i$ and $f4_i$ from each of the four sub-images. Here, i = 1 to M/16, the number of blocks and f1 is a representative 8X8 block from first sub-image I_1, f2 from second sub-image I_2 and so on.
5. Find DCT, for the sub-blocks taken from f1, f2, f3 and f4.
6. Compare coefficients at some specific position (i, j) in pairs as: f1 with f2 and f3 with f4.
7. Apply the embedding criteria. If (f1 > f2) and (f3>f4) assume bit 1 is embedded. And, if (f1 < f2) and (f3 < f4) assume bit 0 is embedded. Whenever any coefficient is found not satisfying this order, swap them accordingly to satisfy the criteria.
8. Increment W_k, for accessing the next watermark bit. If k>m, reset to k=1and start from W_1 onwards for watermarking the remaining blocks.
9. Apply inverse DCT on sub-blocks.
10. Increment i for accessing next set of blocks and repeat from step4, till all 8x8 blocks are watermarked.
11. Recombine the four sub-images.
12. Output the watermarked image I_w.

B. Watermark Extraction Algorithm

The extraction algorithm retrieves the watermark signal from watermarked image I_w. The proposed method is a blind watermarking scheme, which does not require the original image for comparison with the watermarked image for extracting the watermark. The extraction algorithm accepts the watermarked image as input and decodes the embedded UID. Steps for watermark extraction are:

1. Input the watermarked image, I_w.
2. Split the image I_w into four sub-images, I_{w1}, I_{w2}, I_{w3} and I_{w4}, as done by the embedding algorithm.
3. Construct first four 8x8 blocks, $f1_t$, $f2_t$, $f3_t$ and $f4_t$, from each sub-images Iw_1, Iw_2, Iw_3 and Iw_4, for t=1 to M/16.
4. Apply DCT on blocks selected.
5. Compare the values at (i, j) in blocks, $f1_t$ with $f2_t$ and $f3_t$ with $f4_t$. If ($f1_t$>$f2_t$) and ($f3_t$>$f4_t$) extract bit 1. And, if ($f1_t$<$f2_t$) and ($f3_t$<$f4_t$) extract bit 0.
6. Increment t and repeat from step 3, till all 8X8 blocks in the image is examined.
7. Reconstruct the digits from the binary array and display the watermark extracted.

Channel noises and even unintentional attacks many times alter the image pixels values by slightly modifying them. However, the availability of redundant watermark information at different locations in the image increases the probability for retrieval of accurate watermark. During extraction the process skips the blocks pairs, ($f1_t$, $f2_t$) and ($f3_t$, $f4_t$), if their ordering is not alike and negate the relation stated in embedding criteria. In the proposed method, accurate bits could be extracted form other block pairs taken from less affected portions in the image.

IV. Experimental Results

The figure.1.a shows one of the base images I used for testing the proposed algorithm. The watermark w embedded in the image I, is twelve digits UID, say, 123456789123. The resultant watermarked image I_w is shown in fig.1. b.

a) Host Image b) Watermarked Image

Fig.1. Watermarking Process

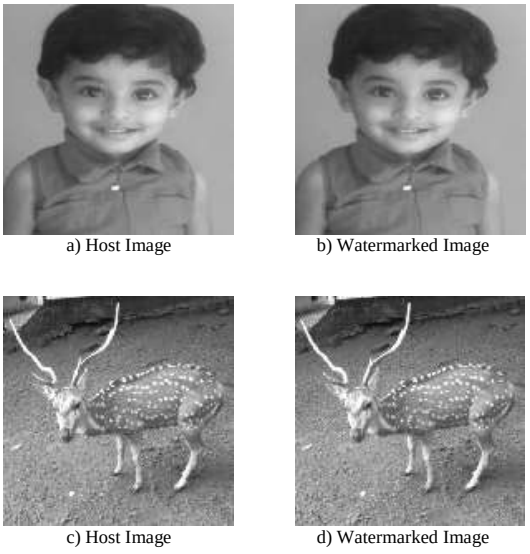
The quality of watermarked image is compared with that of the original image using PSNR (Peak Signal to Noise Ratio) measurement. To calculate PSNR, mean squared error (MSE) of the watermarked image is computed using the equation.1. The summation is over all i, j = 1 to N.

$$MSE = \Sigma \left(\frac{I(i,j) - Iw(i,j)}{N^2} \right)^2 \quad (1)$$

The root mean squared error (RMSE) is the square root of MSE. PSNR in decibels (dB) is then estimated using the equation.2

$$PSNR = 20\log_{10}\left(\frac{255}{RMSE} \right) \quad (2)$$

Fig. 2 shows more examples of image watermarking using the proposed algorithm. During the watermark extraction stage, the embedded UID is successfully regenerated from the watermarked image I_w.



a) Host Image b) Watermarked Image

c) Host Image d) Watermarked Image

Fig.2. Watermarking Various Images

Table.1 contains the experimental results for PSNR measurement after watermark insertion in various test images.

TABLE I
EXPERIMENTAL RESULTS

PSNR Measurement	**Image**		
	Lena	Deer	Child
PSNR (dB)	41.24	41.74	49.86

A higher PSNR indicates the watermarked image is not significantly distorted. A lower value for MSE means lesser error during the embedding process. And as seen from equation.2 there is an inverse relation between MSE and PSNR. Logically it means that the ratio of Signal to Noise is higher.

V. Conclusion

Watermarking could be used effectively in E-governance for marking any multimedia digital

documents. Digital watermarking can immensely contribute in enhancing the system reliability. All digitalized details, including biometric images and other documents collected from individuals as a part of e-governance implementation could be tagged before storing in databases. This minimizes chances for misallocation and misalignment of various documents pertaining to single individual. The robustness of watermark is enhanced here by redundant watermark insertion at multiple regions in the image. Hence, the non detection of watermark bits from one pair of blocks will not affect much as there will be more blocks in the watermarked image that represent the same watermark bit. As a result the probability for retrieving the correct bits during watermark extraction stage is higher.

REFERENCES

[1] I.J Cox, Matt L Miller, Jeffrey A Bloom, "Watermarking Applications and their Properties", International Conference on Information Technology: Coding and Computing, 2000.

[2] Vidyasagar M Potdar, Song Han, Elizabeth Chang," A Survey of Digital Image Watermarking Techniques ", IEEE International Conference on Industrial Informatics, 2005

[3] S.S Sherakar, V.M Thakare, Sanjeev Jain, "Role of Watermarking in E-Governance and e-Commerce", International Journal of Computer Science and Network Security, Vol.8, 2008, pp257-261.

[4] Tribhuvan Kumari, Vikas Saxena, "An Improved Robust DCT based Digital Image Watermarking Scheme", International Journal of Computer Applications, (3) 2010, pp28-31.

[5] Ali Al Haj, "Combined DWT-DCT Digital Image Watermarking", Journal of Computer Science, 3(9) 2007 pp740-746.

[6] Min Shiang Hwang, Chun Ta Li, Jau Ji Shan, Yen-Ping Chu, "Challenges in e-Governance and security of Information", Information and Security International Journal, Vol.15 2004.

[7] Maria Wimmer, Bianca Von Bredow, "A Holistic Approach for Providing Security Solutions in e-Government", Proceedings of 35th Hawaii International Conference on System Science, 2002.

[8] Dilip Kumar Sharma, Vinay Kumar pathak, G.P Sharma, "Digital Watermarking for Secure e-Governance", Towards next generation e-Government**,**Computer Society of Iindia, 2007

[9] Subhash Chander, Ashwani Kush, "Unique Identification Number and e-Governance Security", International Journal of Computing and Business Research, 2010.

[10] Alankrit Patnaik, Deepak Gupta, "Unique Identification Number ", International Journal of Computer Application, 2010.

[11] Hemant Kanakia, Srikanth Nadhamuni, S Sarma, "A UID Numbering Scheme", Available: http://uidai.gov.in, May 2010.