

A Novel Application Framework for Image Manipulation and Protection for Internet Applications

Vijayalakshmi S
VIT University, Vellore,
Tamilnadu, India

vijayalakshmis@vit.ac.in

Prabu D
Wipro Technologies,
NJ, USA

prabud@ieee.org

Abstract

This paper proposes and evaluates a new framework for website image manipulation and its protection using ASP.NET framework in watermarking technique. The proposed framework shows how to protect the valuable website images from the unauthorized users and to preserve web server's bandwidth by preventing other unauthorized websites from directly linking to the images of the authorized web server. This framework effectively preserves the quality of the website image by embedding JPEG file metadata as EXIF tags in website images. This framework provides additional features to users, such as rotate, colors, and contrasts, and also reduces installation time required by supplementary software for image manipulation. The results show that ASP.NET framework in watermarking technique for Image manipulation and protection are encouraging.

Keywords: Watermarking, Authentication, Image manipulation, Meta data

Introduction

Piracy accounts for almost fifty percent of losses faced by all forms of the entertainment industry. From nationwide campaigns to strict anti piracy laws, nothing is left out. The cyber laws incorporated in any country state that piracy in any form will be liable to penal action and any person found guilty will be seriously dealt with. We do not believe in leaving anything to chance. So, through our work we have made an attempt to strike the problem at its root. A stitch in times saves nine. Keeping this adage in mind we have proposed anti-piracy techniques regarding the images. To manipulate images on the internet it's a troublesome task to install separating software for it by the user. Therefore, we have also done away with this by enabling the user to perform image manipulation and image generation. Our website can curb online piracy of images which has slowly begun to take its toll on the internet. This proposed work will be developed to increase the security, interoperability, robustness and extensibility of the work so that it

Material published as part of this publication, either on-line or in print, is copyrighted by the Informing Science Institute. Permission to make digital or paper copy of part or all of these works for personal or classroom use is granted without fee provided that the copies are not made or distributed for profit or commercial advantage AND that copies 1) bear this notice in full and 2) give the full citation on the first page. It is permissible to abstract these works so long as credit is given. To copy in all other cases or to republish or to post on a server or to redistribute to lists requires specific permission and payment of a fee. Contact Publisher@InformingScience.org to request redistribution permission.

can be further enhanced according to future requirements. The rest of the paper in sections addresses the following: description of the motivation behind the work, Proposed Framework (Algorithm) for the Image Manipulation and Protection for the Internet Application, Bit map Image Manipulation by using Microsoft .NET, an example of the proposed work: Image Manipulation

and Protection Results, Application of the proposed work and finally the conclusions of the proposed work and its future enhancements.

Related Work

The image watermarking and manipulation techniques are designed for decode or identify the original images. Nowadays several techniques have been adopted for ownership verification, authentication and piracy of images on the internet. All techniques we adopted for image authentication are classified into two types: fragile authentication and robust authentication. Labeling-based authentication scheme and watermarking based authentication scheme (Lin & Chang (2001) these schemes store the authentication data in a separate file. This kind of approach is suitable for the robust authentication.

However, separate authentication data may increase the demands for additional bandwidth and memory for transmission and storage, and the scheme makes it difficult to find out whether the modification is caused by allowable signal processing or by malicious manipulation (Chang, Hu, & Lu, 2006). A recent image authentication scheme was designed by Chang et al. There are many watermarking techniques were already adopted for image manipulations such as single watermark embedding; multiple watermark embedding and iterative watermark embedding. All the three adopted above mentioned watermarking techniques have their own merits and demerits. The above approaches, can only prevent the potential removal of a watermark in the recompression process of JPEG images and can give robustness, noise removal, etc. However, our proposed implementation procedure to reduce quality of JPEG files to conserve bandwidth and finally based on the experimental results of ASP.NET framework (Buczek, 2002; Parihar, 2002; Selly, Troelsen, & Barnaby, 2003) over watermarking technique for Image protection and manipulation (Bergman-Terrell, 2007) can give good image quality and are robust in varying degree to JPEG compression.

Motivation of the Work

The main motivation for the proposed system is to protect and improve the quality of website images. There are many ways to protect our images from being downloaded or illegally lifted from a website. Image watermarking and authentication schemes are widely applied to ownership. Watermarking techniques provide ownership (Braudaway, 1997) and detect malicious image manipulation. Detecting the imparted image watermark after the image manipulation is a big task. In this work we are proposing a new method to protect images. To draw copyright notices on them, so the unauthorized users cannot download any images and misuse them on their website. To avoid such problems we proposed an efficient algorithm using ASP.NET 2.0. Our proposed algorithm consists of a pool of graphics built in DLL libraries to ease the scaling of images and reduce the quality of the JPEG to economize web server bandwidth.

Objective

The objective of the proposed work is mainly to protect images from image theft on the internet. Image theft is any unauthorized use of an image, photograph, drawing, or illustration. If the user wishes to protect his image, there are several image protection techniques that can be adopted. The most commonly used and known watermarking techniques placing a copyright symbol on the image or small symbol of our own in the corner or top of the image or ownership details like symbol, name of the copyright owner etc. Likewise we have various methods are there for to provide copyright. If we use small copyright symbol on our image it's easy to steal, if the size is larger then it's more visible. Other way of protecting image is using low resolution. A low resolution image can prevent theft because of the concern for quality - as quality can affect what the

image portrays. Preventing right clicks can prevent direct downloads but does not prevent 'screen dumps'. However, the combination of techniques can become powerful in discouraging unauthorized image usage." Every image protection technique will have its own pros and cons.

To overcome above mentioned difficulties the proposed framework uses ASP.NET framework in watermarking technique to provide website image authentication to the web user and prevents unauthorized web users from downloading and manipulating original images and linking with other websites.

Proposed Framework (Algorithm) for the Image Manipulation and Protection

The objective of the proposed work algorithm is to

- i) Prevent unauthorized users from downloading the unprotected original images from the website. The proposed work provides the tight security; all unauthorized users are authenticated before downloading any images from website.
- ii) Preserve protected web server bandwidth by protecting other websites from linking to it
- iii) Provide Image manipulation to authenticated web users such as cropping, scaling up and down then publish in website.
- iv) Provide the authentication to users in intranet or internet user in the same domain

To accomplish these above mentioned objectives we have designed the algorithm in the describing each step as follows:

- i) Take the sample image.
Watermark the sample image through the following algorithm. Draw copyright notices on the sample image (as a semitransparent watermark)
- ii) Add Exchangeable Image Format(EXIF) tags to the Meta data
- iii) Scale the sample images (displaying of each image in a variety of resolutions and quality levels) for to prevent the unauthorized user download the image.
- iv) Preserving web server bandwidth by using HTTP handlers. This HTTP handler prevents other websites from linking to our website.
- v) To give authentication to the images through intranet via internet

The website protected by this framework will defeat image piracy, maintain the integrity and contents of the images displayed, maintain the ownership and copyrights of the images displayed, save the server's bandwidth, and act as software where user can manipulate his images without installing any new software.

The first step towards protecting images is to draw copyrighting notices (as a semitransparent watermark) on them, so that no unauthorized users can download that image and put it up on their website claiming it to be theirs.

The second step is to add EXIF tags. The JPEG file format lets metadata be embedded as EXIF tags. For example Table 1 represents the EXIF specification includes defined tags such as Tag ID and Name.

Table 1: An EXIF Tags

Sl.No	TAG ID	FIELD NAME
S01	315	Creator (Person who created the image)
S02	3432	Copyright (Copyright holder)
S03	270	Image Description (Image title)

Authentication of Images: The third step is to display each image in a variety of resolution and quality levels so the users will have a variety of options to choose from, according to their requirements. The next step is to prevent unauthorized users from seeing the original images without the watermark. The main advantage of this application was that it was done in ASP .NET 2.0 where it is very easy to deal with images using bitmap and Graphics object. Also, on the fly image generation was possible.

BIT Map Image Manipulation by using Microsoft .NET and Image Authentication

Implementation of Proposed Algorithm

Following steps are involved in implementing the proposed algorithm

1. Add watermark method

Figure 2 shows the watermarking technique to prevent unauthorized users from downloading original images. It has been implemented through the following steps. In this framework initially the copyright notices are drawn on the images to be protected as a semitransparent watermark and semi-transparent text is drawn in the middle of bitmap. Include the Add Watermark () method which determines the size of bitmap image format that will contain the text and add specified metadata tag to the bitmap.

Draw copyright notices on the pictures (as a semitransparent watermark)

To scale the images in ASP.NET the website uses a DLL named “Graphics DLL”, draw copyright notices, add metadata to JPEG images, and reduce the quality of JPEG files to conserve bandwidth. ASP.NET using pool of Graphics DLL operates on bitmap objects, because they are easy to manipulate and serve up in ASP.NET in wider range of applications.

The instructions below, Figure 4 draw a copyright notice in the middle of the image as a semi-transparent “watermark” by using the Add watermark method. Watermarking opacity of the image can be calculated from the percentage of opacity parameter. The Opacity values has been taken as any value between 0 for completely transparent image, 255 for completely opaque. The opacity of the watermark is calculated from the OpacityPercent parameter. Graphics, Font, and Brush objects are instantiated. After opacity is calculated, then DrawString is called to draw the text.

2. Add EXIF Tags

The JPEG file format lets metadata be embedded as EXIF tags. EXIF tags are represented as PropertyItem objects. To add the EXIF tags, create the property items and change the necessary values like ID, type, length and value. Return an encoder of specified Multipurpose Internet Mail Extensions (MIME) type and save the bitmap to the stream. If it is in JPEG format, save with

the specified quality level. Adjust the quality of JPEG images if necessary. There are a hundred ways to superimpose a watermark on an image, but this requires a process of doing that to each of the images before placing them on a website. Finally save the image using the JPEG encoder with the specified quality level. The implemented code takes the first PropertyItem object in the JPEG, changes it to the specified EXIF tag and inserts it into the Bitmap by calling Bitmap.SetPropertyItem. The encoder of specified MIME type is returned using GetEncoderInfo (String MIME Type) method.

3. Image authentication

After adding the EXIF tags, embed the original image with watermarking. If the unauthorized user while trying to download or trying to hack the original image, it will ask the authentication. So that our valuable image on the internet can be only used by the authorized users. The authorized users only can do image manipulation and download the image. Other users only can see the watermarked image. The user is validated through their intranet ID and password via internet.

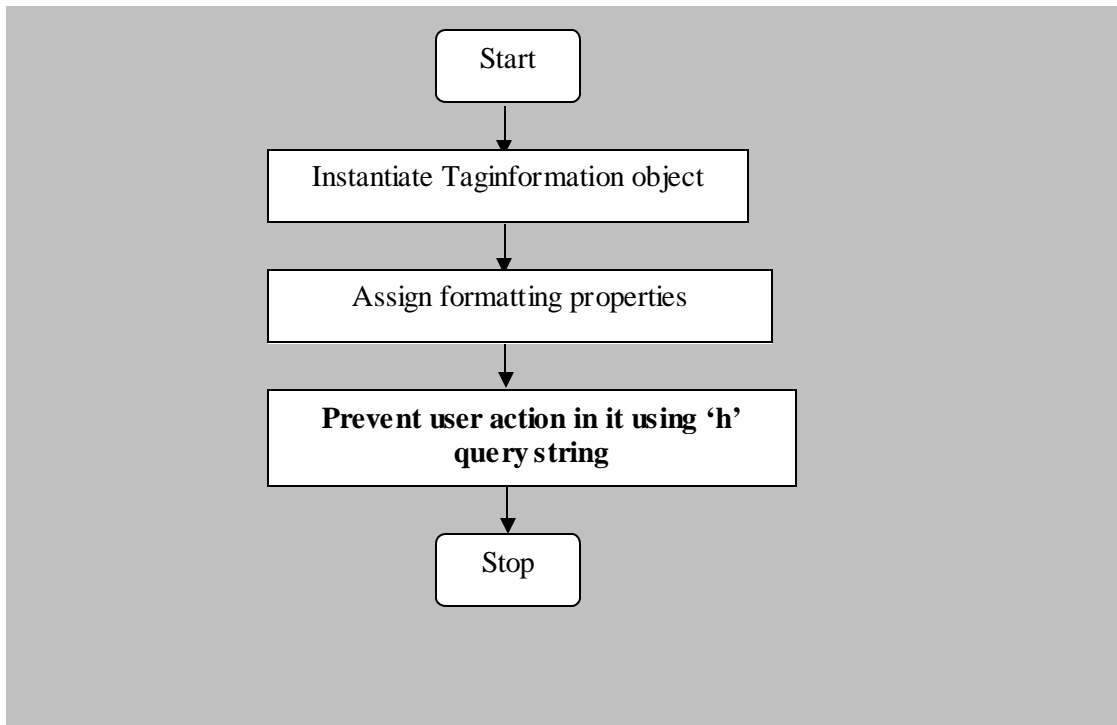


Figure: 1 Copyright.aspx

For example, see the copyright page's code-behind (Copyright.aspx.cs):

These codes will instantiate an ImageTagInfo object and it assigns values to its properties to specify various image-formatting options (Figure 1). For example, the ScaleX property, which corresponds to size of the image, specifies that the image width is 50 percent of its original value. The Copyright.aspx page contains a single image tag. The source attribute value is filled in by the ImageTagInfo object's Source Attribute Value property (Figure 2). When the HTML page is rendered the image tag looks according to the properties set in Figure 1.

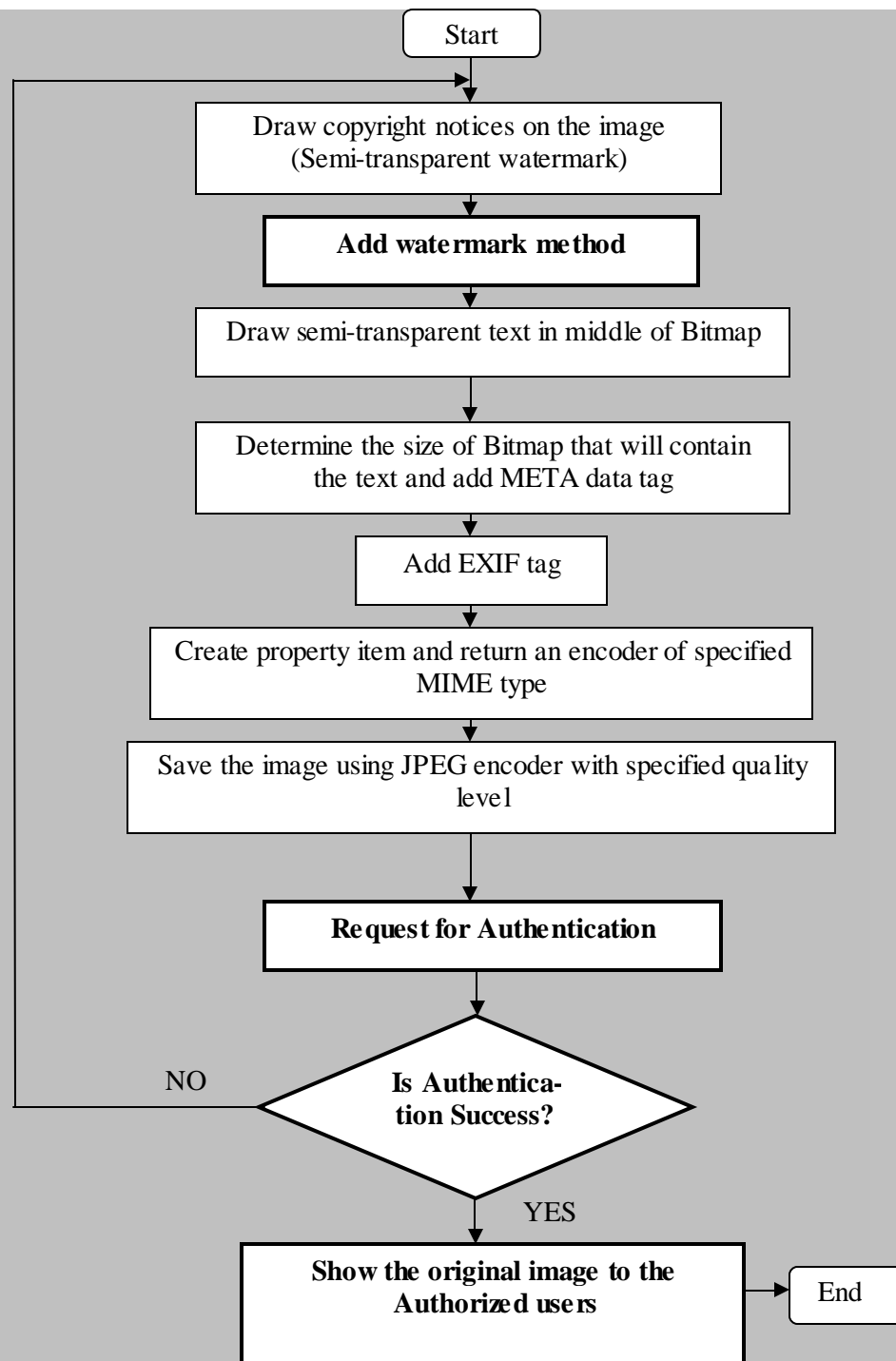


Figure: 2 Watermarking and Image Authentication

In order to prevent the users from changing image URLs to remove copyright notices, the 'h' query string parameter is used and it is also used for increase the image resolution, and so on. For example, if your website displays thumbnail images for free and charges users for full-resolution images, you don't want users to be able to gain access to full-resolution images by changing the query string parameters to 1. The 'h' parameter is an SHA-1 hash of the query string parameters and values, plus a private key. The hash is recomputed from the query string values when the image is requested from the web server. If it matches the original hash, the image is returned (because it's clear that the query string parameters weren't changed). If you click on the website's Incorrect Hash link, you'll see what happens when the hash has been manipulated; no image is displayed. If this hashing scheme didn't exist, the website would be vulnerable to Denial-of-Service (DoS) attacks. Flooding the web server with requests for images scaled to ludicrously large sizes would swamp the web server and drastically reduce the site's responsiveness.

Image Manipulation and Protection Results of the Proposed Framework

All the following figures (Figure 3 to Figure 9) are self explanatory .Let us take a sample jpeg image

“sample.jpeg”



Figure 3: Sample.jpeg

Lets us take our watermark image called “abc.jpeg”. Let our copyright string be “Copyright @ 2008 – VIT Photos/ Soumo Tim”.

The original image with watermark is:

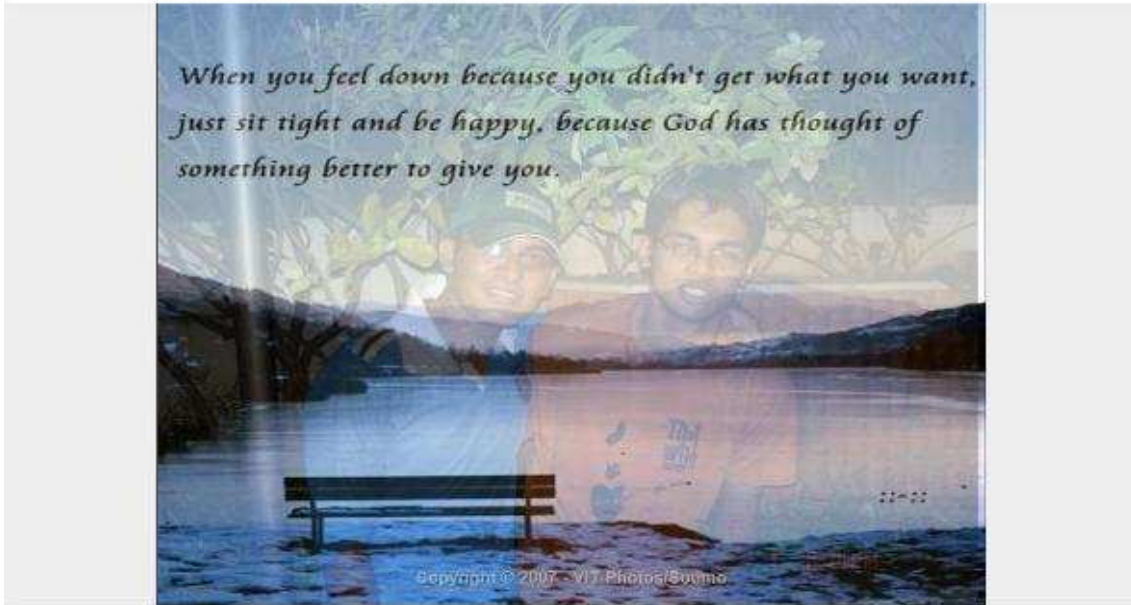


Figure 4: Watermark Image.

Image Authentication



Figure 5: Embed Image with watermarking

Various Image Manipulations

1. Image Scaling (down)

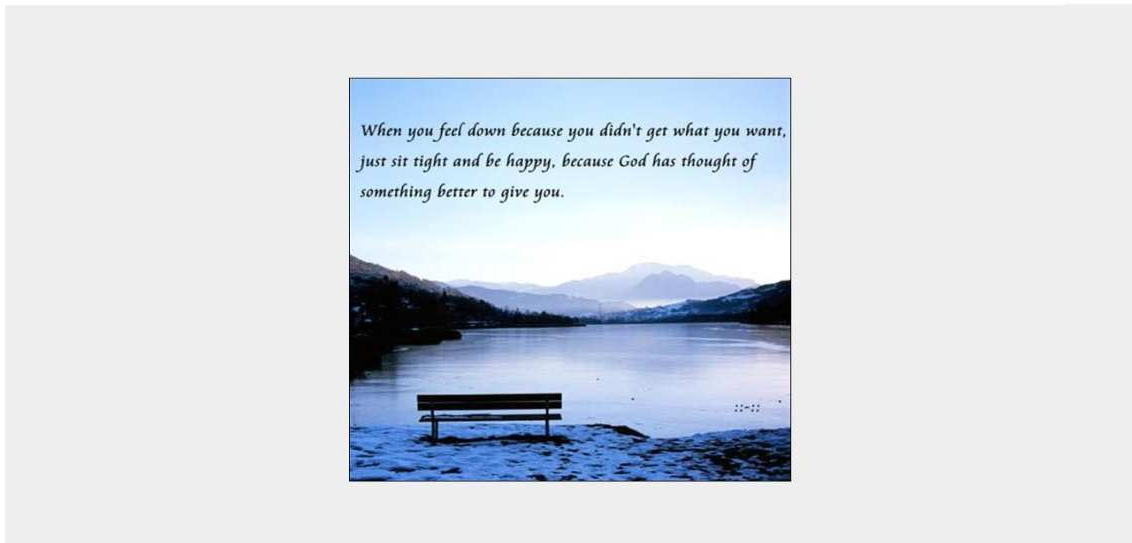


Figure 6: Scaling Down Image

2. Image Cropping



Figure 7: Before Cropping the Image



Figure 8: After Scaling the Cropped Image

3. Image Rotation



Figure 9: Image Rotation

Applicability of the Proposed Work in the Possible Areas

This proposed work can be used to prevent the access to “fraud websites” which save immense bandwidth by not enabling communication to link directly to inner pages of healthy websites. Thus, the load factor of the website is hugely decreased. In addition this proposed work can be further used to develop an image analyzer where an image can be analyzed, functions like cropping, rotation, and many more can be applied to further study the image thoroughly. This proposed work can be used in forensic field to study with more depth the images available and derive a conclusion based on it. Beside it can be used together with a pattern recognition system

and a fingerprint analyzer to aid in solving a crime cases effectively. As we all know “A picture is worth a thousand words”. This application can also be used in the image and film industry to prevent piracy by providing the possibility to embed a watermark on videos or still images. This can lead to large economic savings in the entertainment industry where loss due to piracy is prevalent. The animation industry is one that shows much promise internationally. We can enhance this application to use it in doing various types of animation and in the making of 3-D images and provide various types of manipulations options on it.

Conclusions and Future Work

We have presented a unified novel framework for websites image manipulations and image protection through watermarking technique. With this framework we have identified following significant advantages as follows (i) the website image owner will be able to prevent website images from being used for illegitimate purposes by displaying a watermark of user choice in it. (ii) We can save the server’s bandwidth by preventing other websites from directly linking to our images in the inner pages of our website. (iii) This framework has been designed using ASP .NET along with C#. It is very simple to do various types of operations on the image such as rotating around an axis, cropping the important part of the picture, scaling up or down converting to bright, highly contrasting, black and white images as well as invert different colors in the image. (iv) This framework prevents the infringement on the part of invalid web user: We used the Bitmap and Graphics class of the application very frequently for image manipulation. (v) ASP.NET 2.0 platform over watermarking provides various functionalities which serves our purpose for image manipulation and protection.

The transparent and opaque watermark was stamped on all the images to mark our ownership and authority on those images by this way images can be protected. Though we use secured algorithm for watermarking the image, the hackers on the internet may easily be access the image in various ways like, the unauthorized user can take a picture from high resolution camera, even though we put copyright symbol on our own image there is also a chance of misusing the valuable image. Our proposed research work shows how the valuable image on the internet can be protected through embed the watermarked image, give authentication through intranet users via internet; which helps authorized users only to see or do the manipulation of the original image other unauthorized users can only view the watermarked image. It provides the tight security of the valuable image. This proposed work may further be enhanced through improving the watermarking capabilities and provide the symmetric key to the authorized users which would avoid the unauthorized person to download our valuable image on the internet and claim theirs.

References

- Berg man-Terrell, E. (2007). Image manipulation with ASP.NET 2.0. *Dr.Dobb’s Journal, March*, 34-39.
- Braudaway, G. W. (1997). Protecting publicly -available images with an invisible image watermark. *Proceedings of the 1997 International Conference on Image Processing (ICIP '97) - Volume 1*, pp.524.
- Buczek, G. (2002). *ASP.NET tips & techniques*. USA : Tata McGraw Hill Education.
- Chang, C-C., Hu, Y-S., & Lu, T-C., (2006), A watermarking-based image ownership and tampering authentication scheme, *Pattern Recognition Lett*, 27(5), 439-446.
- Chang, E-C., Kankanhalli, M. S., Guan, X., Huang, Z., & Wu, Y. (2003). Robust image authentication using content based compression, *Multimedia Systems*, 9, 121–130.
- Lin, C-Y., & Chang, S-F. (2001). Robust image authentication method distinguishing JPEG compression from malicious manipulation. *IEEE Transactions on Circuits and Systems of Video Technology*, 11(2), 153.

Parihar, M. (2002). *ASP.NET bible*. USA : Wiley Dreamtech India.

Selly, D., Troelsen, A., & Barnaby, T. (2003). *Expert ASP.NET 2.0 advanced application design*. Apress Edition.

Biographies



Vijayalakshmi S is the Assistant Professor (Senior) in Architecture and Embedded Systems Divisions, School of Computing Sciences at Vellore Institute of Technology (VIT University), Vellore, India. Her current research interests are Image Processing and Computer architecture, Internet Security. She is currently serving as a technical reviewer and program committee member for international conferences. She holds a Bachelor of Engineering (B.E.) in Electrical and Electronics Engineering from Bharathiar University (now Anna University, Chennai), India and M.S. in Information Technology from Manonmaniam Sundaranar University, India. She has written a book titled 'Operating System' to be published by Duvvuri publishers, Andhra Pradesh, India which will be available in stores by August 2009. She is serving as a Technical Evangelist for Asia Open Source Software Community, CICC, Japan and all over Asian Countries. She is a Member of IEEE, ACM, CSI and a member of N2WOMEN (Networking Networking Women) IEEE/ACM Women in Engineer. She can be reached at viji@ieee.org.



Prabu D is the Technical Leader at the Wipro Technologies, USA. His current research interests are Data Storage technologies, High Performance Computing, Robotics and Artificial Intelligence. He is currently serving as Editorial Board member for International Journals and International Program Committee member for several IEEE Conferences around the globe. He holds a Bachelor of Engineering (B.E.) in Electrical and Electronics Engineering from University of Madras (now Anna University Chennai), India and a Masters degree in Technology (M.Tech.) in Electrical Engineering (system engineering) from the Indian Institute of Technology (IIT) at Roorkee, India. His M. Tech research thesis carried out at IIT, Roorkee has also been referred as a chapter in a book entitled "Advances in Robot Manipulators", ISBN 978-953-7619 to be published by IN-TECH publishers, Vienna, Austria which will be available by November 2009. He is the Colorado Chapter Representative for IIT Roorkee Heritage Fund in USA. His profile is listed in the "2000 Outstanding Scientists 2008-09" awarded by International Biographical Centre (IBC), Cambridge, U.K. He has been chosen for inclusion in the 26th Edition (2008 to 2009) of Marquis "Who's Who in the World", USA. He is a member of IEEE, ACM and CMG. <http://prabud.iitr.googlepages.com>. He can be reached at prabud@ieee.org.