RESEARCH ARTICLE OPEN ACCESS

Data and Information Hiding on Color Images Using Digital Watermarking

Chetna[1], Krishan Kumar[2]
Student[1], Assistant Professor[2]
Department of Computer Science and Engineering
JCDM College of Engineering
Barnala Road, Sirsa
Haryana-India

ABSTRACT
Water marking is the art of hiding the fact that communication is taking place, by hiding information in other information. Many different carrier file formats can be used, but digital images are the most popular because of their frequency on the internet. For hiding secret information in images, there exist a large variety of invisible water marking techniques some are more complex than others and all of them have respective strong and weak points. Different applications may require absolute invisibility of the secret information, while others require a large secret message to be hidden. This project report intends to give an overview of image water marking, its uses and techniques. It also attempts to identify the requirements of a good invisible water marking algorithm and briefly reflects on which water marking techniques are more suitable for which applications.
Keywords:- Digital images, hidden, water marking.

I. INTRODUCTION

Digital watermarking is a technology for embedding various types of information in digital content. In general, information for protecting copyrights and proving the validity of data is embedded as a watermark. A digital watermark is a digital signal or pattern inserted into digital content. The digital content could be a still image, an audio clip, a video clip, a text document, or some form of digital data that the creator or owner would like to protect. The main purpose of the watermark is to identify who the owner of the digital data is, but it can also identify the intended recipient. Why do we need to embed such information in digital content using digital watermark technology? The Internet boom is one of the reasons. It has become easy to connect to the Internet from home computers and obtain or provide various information using the World Wide Web (WWW). All the information handled on the Internet is provided as digital content. Such digital content can be easily copied in a way that makes the new file indistinguishable from the original. Then the content can be reproduced in large quantities.

For example, if paper bank notes or stock certificates could be easily copied and used, trust in their authenticity would greatly be reduced, resulting in a big loss. To prevent this, currencies and stock certificates contain watermarks. These watermarks are one of the methods for preventing counterfeit and illegal use. Digital watermarks apply a similar method to digital content. Watermarked content can prove its origin, thereby protecting copyright. A watermark also discourages piracy by silently and psychologically deterring criminals from making illegal copies.

1.1 Principle of digital watermarks

A watermark on a bank note has a different transparency than the rest of the note when a light is shined on it. However, this method is useless in the digital world. Currently there are various techniques for embedding digital watermarks. Basically, they all digitally write desired information directly onto images or audio data in such a manner that the images or audio data are not damaged. Embedding a watermark should not result in a significant increase or reduction in the original data. Digital watermarks are added to images or audio data in such a way that they are invisible or inaudible Ñ unidentifiable by human eye or ear. Furthermore, they can be embedded in content with a variety of file formats. Digital watermarking is the content protection method for the multimedia era.

1.2 Materials suitable for watermarking

Digital watermarking is applicable to any type of digital content, including still images, animation, and audio data. It is easy to embed watermarks in material that has a comparatively high redundancy level ("wasted"), such as color still images, animation, and audio data; however, it is difficult to embed watermarks in material with a low redundancy level, such as black-and-white still images. To solve this problem, we developed a technique for embedding digital watermarks in black-and-white still images and a software application that can effectively embed and detect digital watermarks.

1.3 Structure of a digital watermark

The structure of a digital watermark is shown in the following figure

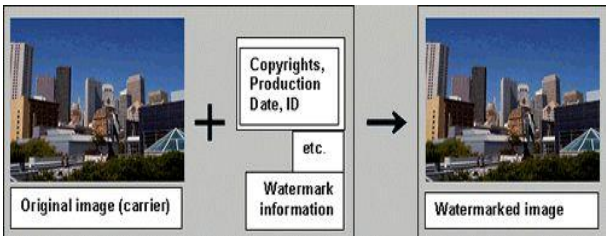

Fig 1: Original image with watermarked image

The material that contains a digital watermark is called a carrier. A digital watermark is not provided as a separate file or a link. It is information that is directly embedded in the carrier file. Therefore, simply viewing the carrier image containing it cannot identify the digital watermark. Special software is needed to embed and detect such digital watermarks. Kowa's Stegano Sign is one of these software packages.

Both images and audio data can carry watermarks. A digital watermark can be detected as shown in the following illustration.

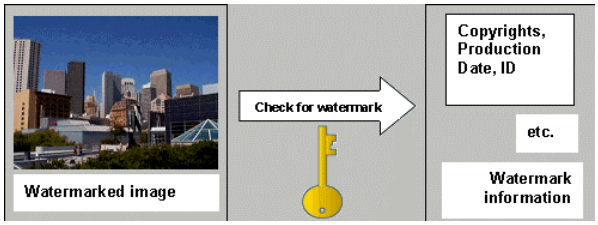

Fig 2: Unmarked watermarked image

1.4 Types of Watermarking:

Visible watermarks: A visible watermark is a visible translucent image which is overlaid on the primary image. Perhaps consisting of the logo or seal of the organization which holds the rights to the primary image, it allows the primary image to be viewed, but still marks it clearly as the property of the owning organization.

It is important to overlay the watermark in a way which makes it difficult to remove, if the goal of indicating property rights is to be achieved.

Invisible watermarks: An invisible watermark is an overlaid image which cannot be seen, but which can be detected algorithmically. Different applications of this technology call for two very different types of invisible watermarks:

A watermark which is destroyed when the image is manipulated digitally in any way may be useful in proving authenticity of an image. If the watermark is still intact, then the image has not been "doctored." If the watermark has been destroyed, then the image has been tampered with. Such a technology might be important, for example, in admitting digital images as evidence in court.

An invisible watermark which is very resistant to destruction under any image manipulation might be useful in verifying ownership of an image suspected of misappropriation. Digital detection of the watermark would indicate the source of the image.

II. LİTERATURE SURVEY

Radhika v. Totla, K.S.Bapat [2013] – have studied the Digital Watermarking has emerged as a new area of research in an attempt to prevent illegal copying and duplication. In this paper, I represent both methods i.e. DCT&DWT based algorithm for watermarking in digital images. In order to compare the imperceptibility & robustness of the both algorithms make use of simple attacks such as resizing, rotation & cropping [6]. **C.P.Sumathi, at al. [2013]** in this paper authors presents the information hiding as a security of information which has become a big concern in this internet era. As sharing of sensitive information via a common communication channel has become inevitable, Steganography – provides the art and science of hiding information has gained much attention. Steganography derives from the Greek word steganos, meaning covered or secret, and graphy (writing or drawing). In this paper different steganographic articles are studied and are categorized into different techniques. As many new application areas are identified like internet banking, mobile communication security, cloud security etc., the insight into the steganographic principles will definitely guide us to identify new areas and to improve its applications in the already existing application areas also [10]. **Mona M. Soliman, at al. [2012**], in this paper author present a secure patient medical images and authentication scheme which enhances the security, confidentiality and integrity of medical images transmitted through the Internet. This paper proposes a watermarking by invoking particle swarm optimization (PSO) technique in adaptive quantization index modulation and singular value decomposition in conjunction with discrete wavelet transform (DWT) and discrete cosine transform (DCT). The proposed approach promotes the robustness and watermarked image quality.

The experimental results show that the proposed algorithm yields a watermark which is invisible to human eyes, robust against a wide variety of common attacks and reliable enough for tracing colluders. This paper introduced a robust watermarking approach for protecting medical images using swarm intelligent technique. PSO approach is used to get basic quantization steps which are optimally varied to achieve the most suitable locations for various images with different frequency characteristics. The experimental results reveal that our method can improve the quality of the watermarked image and increase the robustness of the embedded watermark against various attacks[12]. **Sushila Kamble, at, al. [2012],** in this paper, a new robust

watermarking technique for copyright protection based on Discrete Wavelet Transform and Singular Value Decomposition is proposed. The high frequency subband of the wavelet decomposed cover image is modified by modifying its singular values. A secret key is generated from the original watermark with the help of visual cryptography to claim the ownership of the image. The ownership of the image can be claimed by superimposing this secret key on the extracted watermark from the watermarked image. The robustness of the technique is tested by applying different attacks and the visual quality of the extracted watermark after applying these attacks is good.

Also, the visual quality of the watermarked image is undistinguishable from the original image. In this paper a new robust watermarking technique for copyright protection has been proposed. We applied the singular value decomposition along with the Discrete Wavelet Transform. Since the technique utilizes the properties of both DWT and SVD the proposed technique is more robust against different attacks. The innovation of this paper is that the security of the algorithm is increased with the help of visual cryptography on the watermark image. If the second share of the watermark which acts as the key is not present then it is not possible to extract the exact watermark information. It is very difficult to change or remove the watermark without knowing the secret key share as the watermark is split into two shares with random patterns. The robustness of the technique is justified by giving analysis of the effect of attacks and still we are able to get good visual quality of the embedded watermark [14].

III. METHODOLOGY

Algorithm to apply the watermarking on image

Step 1: Start the program
Step 2: Read the original color image.
Step 3: Apply the DWT technique with Haar wavelet to divide the image for watermarking. When DWT is applied on the image then the image is divided into following four parts: h_LL, h_LH, h_HL, h_HH.
Step 4: Extract the RGB color from original image and apply SVD algorithm on red, green and blue color.
Step 5: Read the watermark image.
Step 6: Repeat the step 3 & 4 on watermark image.
Step 7: Apply watermarking with intensity and get output image with the help of IDWT.
Step 8: Save the watermarked image with the help of imwrite command.
Step 9: Calculate the parameters PSNR and MSE of watermarked image.

Algorithm to extract the watermarking on image

Step 1: Start the program
Step 2: Read the original color image.
Step 3: Apply the DWT technique with Haar wavelet to divide the image for watermarking. When DWT is applied on the image then the image is divided into following four parts: h_LL, h_LH, h_HL, h_HH.
Step 4: Extract the RGB color from original image and apply SVD algorithm on red , green and blue color .
Step 5: Read the watermark image.
Step 6: Repeat the step 3 & 4 on watermark image.
Step 7: Read the watermarked image.
Step 8: Repeat the step 3 & 4 on watermark image.
Step 9: Extract the watermarked image with the help of following commands:

```
S_ewatr=(S_imgr3-S_imgr1)/0.10;
S_ewatg=(S_imgg3-S_imgg1)/0.10;
S_ewatb=(S_imgb3-S_imgb1)/0.10;
ewatr = U_imgr2*S_ewatr*V_imgr2';
ewatg = U_imgg2*S_ewatg*V_imgg2';
ewatb = U_imgb2*S_ewatb*V_imgb2';
```

Step 10: Apply watermarking with intensity and get output image with the help of IDWT.
Step 11: Save the Extracted Watermark image with the help of imwrite command.
Step12: Calculate the parameters PSNR and MSE of watermarked image.

IV. RESULT & DISCUSSION

The work Data hiding using color palette in steganography shows different results that are shown below. The figure 3 shows the starting of the work, where we have to choose the operations and second figure 4, shows the window in which insert and extract button is provided for selecting options insert button to add watermarked in image or text and by button extract get out watermarked data. Figure 5 and 6, shows the adding information path of source image and for text hider box as image or text selection option with the same saving output file information, here number can also we selected for hiding information in a source image. Figure 7 and 8, shows the security key that we have entered by extracting window by selecting source for watermarked image and we can decode it and get the original text that we have hided.

Fig 3: Starting Window for watermarking with three different buttons

Above fig shown the window in which three different ways for hiding the image or text to be get out as a watermarked images.

Fig 4: Window for inserting and extracting watermarking button

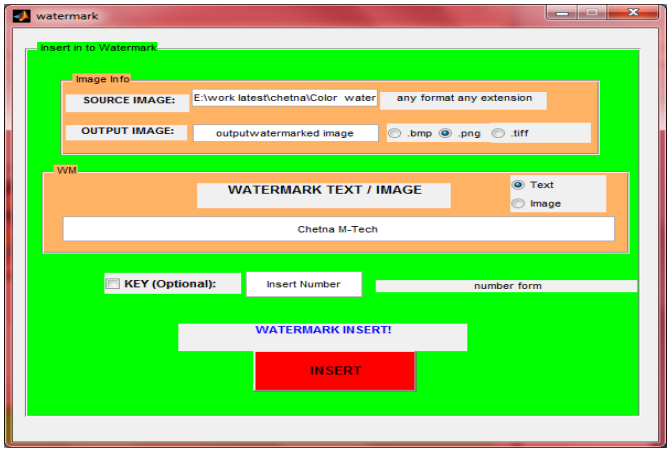

Fig 5: Window for inserting watermarking path for source file and text or image hiding

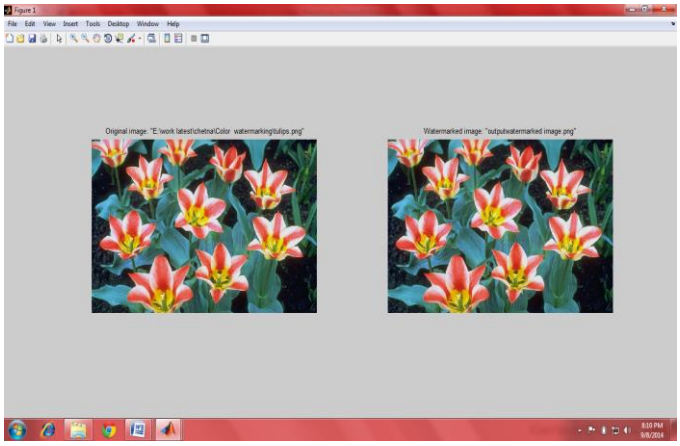

Fig 6: Window after inserting watermarking text with original and watermarked image

Fig 7: Window for Extracting watermarking path for source output file

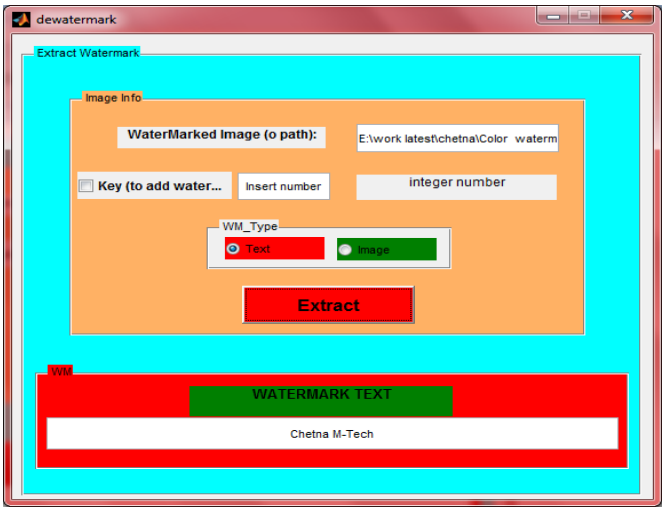

Fig 8: Window after Extracting hidden text from watermarked image

V. CONCLUSION & FUTURE

The proposed scheme used in this paper encrypts the secret information before embedding it in the image. Certainly the time complexity of the overall process increases but at the same time the security achieved at this cost is well worth it. In this invisible watermarking is used with Steganographic techniques. We have explained the basic mechanism of our proposed model and it is an alternative approach of Steganographic. It is not pure Steganographic technique but the effect is same with some additional advantage. First advantage is the data file and reference image is going through the open channel separately. The basic result is interception of any one cannot provide desired objective. Second advantage is that any amount of data can be transmitted using the method because it is not depending on the size of image. Final advantage, the said method is not affecting the image. There is no change of quality and color change of reference image. It is most vital achievement of method.

The algorithm time complexity is simple and always proportional to O(n). The performance of hiding algorithm is totally depending on the length of text to hide and size of image. Similarly Unhidden algorithm is reverse process of previous one and complexity character is same. At end, this can be said that the aforesaid method may be improved, instead of text small image may be hiding, invisible watermarking may be used or much improvement in this field may be incorporated in future. Lastly it is expected by the authors that any kind of future endeavors in this field will definitely route it a path to design a secure system using the proposed algorithm for both Internet and Mobile Communication Technology

REFERENCES

[1] Zhen-Ming Lu, Dian-Guo Sheng Xu,and -He Sun, "Multipurpose Image WatermarkingAlgorithm Based on Multistage Vector Quantization," IEEE Transactions on ImageProcessing, vol. 14, no. 6, June 2005

[2] J. J. K. O'Ruanaidh, W. J. Dowling, and F. M. Boland, "Watermarking digital images for copyright protection,"

[3] Feng-Hsing Wang, Lakhmi C. Jain, Jeng-Shyang Pan,"IEEE Hiding Watermark in Watermark", IEEE, (2005),4-8.

[4] Jian Ren, TongTong Li, Mehrdad Nadooshan, "A Cryptographic Watermark Embedding Technique", IEEE,(2004), 382-386.

[5] Ping Wah Wong "Secret and Public Key Image Watermarking Schemes for Image Authentication and Ownership Verification" IEEE TRANSACTIONS ON IMAGE PROCESSING, VOL. 10, NO. 10, OCTOBER 2001.

[6] Mauro Barni "Improved Wavelet-Based Watermarking Through Pixel-Wise Masking "IEEE transactions on image processing, vol. 10, no. 5, may 2001 .

[7] Farid Ahmed, Ira S. Moskowitz"Correlation-based watermarking method for image authentication applications"Opt. Eng. 43(8) 1833–1838 (August 2004) 0091-3286/2004.

[8] Santa Agrestea, Guido Andalorob, Daniela Prestipinob, Luigia Puccio "An image adaptive, wavelet-based watermarking of digital images " science direct Journal of Computational and Applied Mathematics 210 (2007) 13 – 21.

[9] Ahmad A. Mohammad_, Ali Alhaj, Sameer Shaltaf "An improved SVD-based watermarking scheme for protecting rightful ownership "science direct Journal of Computational and Applied Mathematics Signal Processing 88 (2008) 2158–2180 .

[10] Manjit Thapa, Sandeep Kumar Sood" On Secure Digital Image Watermarking Techniques "Journal of Information Security, 2011, 2, 169-184 doi:10.4236/jis.2011.24017 Published Online October 2011.

[11] Cun Shang and Peng Yang" Research of Colorde Image Digital Watermark" Advances in CSIE, Vol. 2, AISC 169, pp. 559–563.

[12] Sushila Kamble, Vikas Maheshkar , Suneeta Agarwal , Vinay K "dwt-svd based secured image watermarking for copyright protection using visual cryptography "Natarajan Meghanathan, et al. (Eds): ITCS, SIP, JSE-2012, CS & IT 04, pp. 143–150, 2012.

[13] Preeti Gupta" Cryptography based digital image watermarking algorithm to increase security of watermark data" International Journal of Scientific & Engineering Research, Volume 3, Issue 9, September 2012 1 ISSN 2229-5518.

[14] Radhika v. Totla, K.S.Bapat " comparative study of watermarking in digital image using DCT&DWT" International Journal of Scientific and Research Publications, Volume 3, Issue 2, February 2013 1 ISSN 2250-3153.

[15] R. Chandramouli. Data hiding capacity in the presence of an imperfectly known channel. Proc.SPIE Security and Watermarking of Multimedia Contents III,2001.

[16] R. Chandramouli. Watermarking capacity in thepresence of multiple watermarks and partially knownchannel. Proc. of SPIE Multimedia Systems andApplications IV, 4518, Aug. 2001.