ISSN:0975-9646

Digital Watermarking for Secure Online Transmission

Anubhav Bewerwal [#1], Kailash Patidar [*2]

[#] *Research Scholar, Rajiv Gandhi Proudyogiki Vishwavidyalaya*
Bhopal, India
[*] *Rajiv Gandhi Proudyogiki Vishwavidyalaya*
Bhopal, India

***Abstract*— Due to the emergence of the online applications user data along the network is not very secure. Also in surveillance applications data security is essential. In this paper, a two folded security is considered, where first using Least Significant Bits (LSB) stenography data decryption key is send in advance to the receiver. Later actual information is send using digital watermarking as an encrypted image. This twofold security makes the information more secure. In the watermarked technique Discrete Cosine Transform (DCT) is considered. The performance measure is done in terms of Peak Signal to Noise Ratio (PSNR) and Structural Similarity (SSIM).**

***Keywords*— LSB, PSNR, watermarking, SSIM**

I. INTRODUCTION

The concept of digital watermark is all that much like a conventional watermark basically found on the paper. The addition of traditional watermarks is done to offer proof of authenticity. Correspondingly, digital watermarks are added to still images in a manner that can be distinguished by a PC, however is undetectable to the human eye. A digital watermark conveys a message containing information about the inventor or distributor of the image, or even about the image itself.

The copyright information of an image is communicated by using a watermark with a specific end goal to reduce copyright infringement. An individual opening a watermarked image in a Digimarc-supported image-altering application gets intimation through a copyright image ((c)) that the image contains copyright and possessed information. A link is provided by the watermark to complete contact details for the copyright holder or image distributor, making it simple for the viewer to license the image, license another one like it, or commission new work. Although, the Digimarc digital watermarks are hard to sense for the human eye, still are durable and furnish images with a persistent personality. In order to hide the watermark, Digimarc changes the energy of watermark within the image so that it stays imperceptible in both flat as well as detailed areas. The watermark is robust, surviving typical image alters and file format conversions, staying with the image in printed and digital form-and is yet detectable on printing an image and after that checked once more into a PC. In this paper, a system of twofold security is presented, where a unique password (key) is send in advance utilizing text stenography, and after that real information is send as watermarked image, and actual information can only be recovered with the use of the key.

II. RELATED CONCEPTS AND METHODS

A. Text steganography

On the basis of the cover medium, the modern day methodology, steganography can be divided into five types:

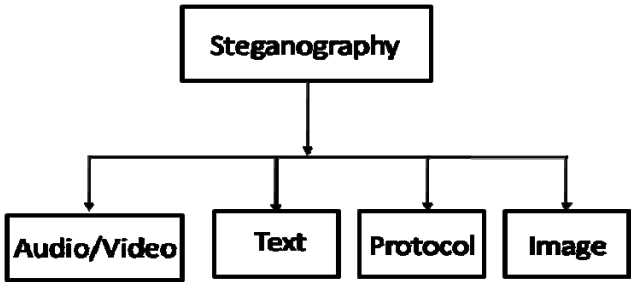


Fig. 1 Types of Stenography

As far as our work is concerned, text steganography is used by us. Images are used as the prevalent cover medium for steganography. A message is embedded in a digital image utilizing an embedding algorithm. This is done by making use of the secret key. The resultant stego-image is then received by the receiver. On the other side, the extraction algorithm processes it using the same key. Unauthenticated persons can simply see the transmission of an image during the transmission of stego-image yet can't notice the vicinity of the concealed message.

The bit of minimum significance (i.e. the 8th bit) of all or some of the bytes within an image is changed into a bit of the secret message. The two main types of Digital images are 24 bit and the 8 bit images [1-2]. In 24 bit images, three bits of information could be installed in each pixel, one in each LSB position of the three eight bit values. The appearance of the image is not changed by the LSB with the increase or decrease of the value; much so the resultant stego image appears almost similar as the cover image. While on the other hand, one bit of information can be covered up in 8 bit images [1-3].

To get rid of the concealed image from the stego-image, the inverse process is applied. For the situation the LSB of the cover image pixel value $C(i, j)$ is equivalent to the message bit 'm' of secret massage to be embedded, $C(i, j)$ does not change; if not, set the LSB of $C(i, j)$ to m. The message embedding procedure is given as under:

$S(i,j) = C(i, j) - 1$, if LSB $(C(i, j)) = 1$ and $m = 0$
$S(i,j) = C(i, j)$, if LSB$(C(i, j)) = m$
$S(i,j) = C(i, j) + 1$, if LSB $(C(i, j)) = 0$ and $m = 1$

where LSB ($C(i, j)$) stands for the LSB of cover image $C(i, j)$ and m is the next message bit to be embedded. $S(i,j)$ is the stego image. The flow chart of the process is shown in Fig. 2.

For the successful insertion of the character in this case we have to change just four bits. It is very difficult for a human eye to perceive the resulting changes that are made to the slightest significant bits as they are too small, consequently the message is hidden in an adequate way [4]. The advantage of LSB embedding is its simplicity and numerous techniques use these techniques. Moreover, it also allows the transparency of high perceptual.

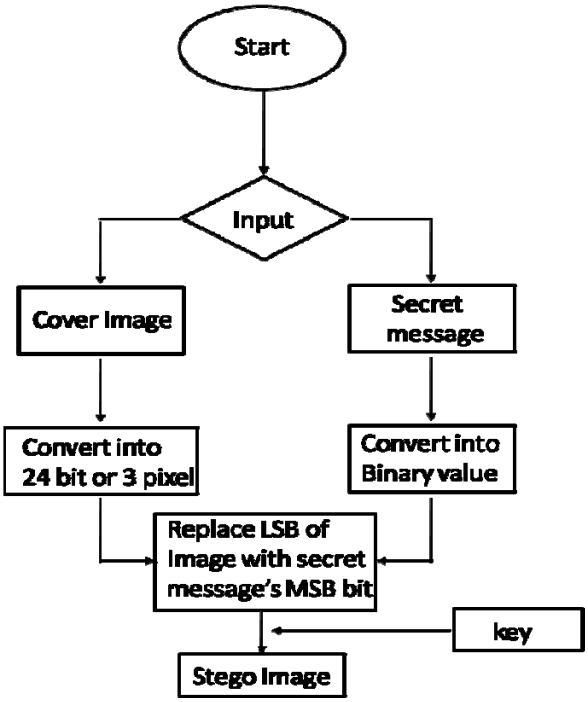


Fig. 2 Flow chart description of LSB Steganography

B. Transform Domain Technique

The Frequency domain the message is enclosed into transformed coefficients of image providing some additional information concealing capacity along with more firmness to deal with attacks. Transform domain embedding can be termed as a domain of embedding techniques.

Discrete Cosine Transform

The next step after color coordinate conversion is of separating the three image color components into various 8×8 block. The Forward DCT and the Inverse DCT could be mathematically defined as under:

Forward DCT

$$F(u,v)=\frac{2}{N}C(u)C(v)\sum_{x=0}^{N-1}\sum_{y=0}^{N-1}f(x,y)\cos\left[\frac{\pi(2x+1)u}{2N}\right]\cos\left[\frac{\pi(2y+1)v}{2N}\right] \quad (1)$$

for $u=0,...,N-1$ and $v=0,...,N-1$

where $N=8$ and $C(k)=\begin{cases}1/\sqrt{2} & \text{for } k=0\\ 1 & \text{otherwise}\end{cases}$

Inverse DCT

$$f(x,y)=\frac{2}{N}\sum_{u=0}^{N-1}\sum_{v=0}^{N-1}C(u)C(v)F(u,v)\cos\left[\frac{\pi(2x+1)u}{2N}\right]\cos\left[\frac{\pi(2y+1)v}{2N}\right] \quad (2)$$

for $x=0,...,N-1$ and $y=0,...,N-1$ where $N=8$

In the selected 8×8 block, the $f(x,y)$ is the each pixel value and the $F(u,v)$ is the DCT coefficient after transformation. The transformation of the 8×8 block is also a 8×8 block composed of $F(u,v)$.

The first frequency-domain watermarking scheme was developed by Cox. After that considerable measures of watermarking algorithms have been proposed in frequency domain [5] [6]. A broadly accepted point now is the frequency-domain watermark should be embedded into the mid-band of the transformed host image. In high frequency band, Watermarks tend to have less impact on the nature of original image, while in low band will accomplish a superior robustness and the mid-bind scheme is right a tradeoffs between the imperceptibility and robustness [6].

III. Proposed Methodology

In this work a twofold security system is presented, where a password (key) is send in advance using text stenography. There after a watermarked image is send which contain embedded message or image. Watermarked image is first encrypted before it is transmitted in the network. On the receiver end image can be decrypted to recover original image, but hidden data will only be retrieved when key is provided to the system send in advance.

The above idea is depicted in figure 3. In the analysis for watermark DCT is considered. In the previous system (Fig. 4) PSNR is considered to be the main parameter in image quality measurements.

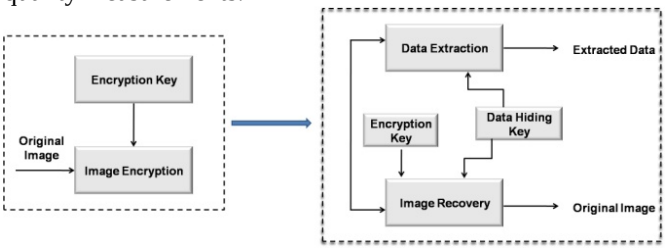


Fig.3: Schematic of proposed work

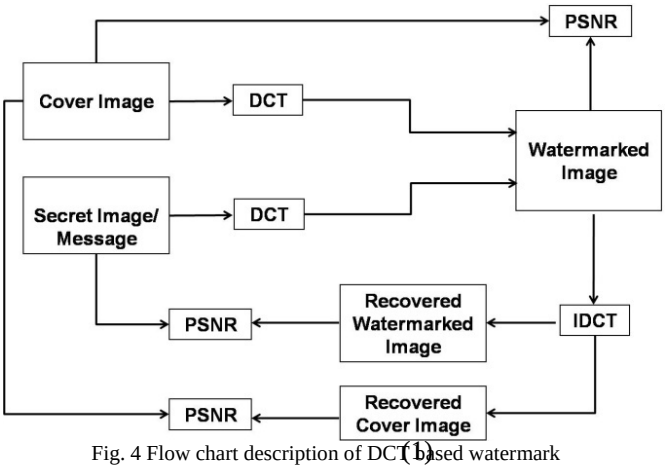


Fig. 4 Flow chart description of DCT based watermark

A. Peak Signal to Noise Ratio (PSNR)

As a performance measure for image distortion due to hiding of message, the well-known peak-signal-to noise ratio (PSNR), which is categorized under difference distortion metrics, can be applied to stego images. It is defined as:

$$PSNR(dB) = 10\log\frac{\left(C_{\max}\right)^2}{MSE} \quad (3)$$

MSE = mean square error;
which is given as:

$$MSE = \frac{\left(S-C\right)^2}{MN} \quad (4)$$

With $C_{\max} = 255$:

Where M and N are the dimensions of the image,
S is the resultant stego-image, and C is the cover image.

The PSNR for the retrieved image is defined as

$$PSNR(dB) = 10\log\frac{\left(C_{\max}\right)^2}{MSE} \quad (5)$$

$MSE = \frac{R^2}{MN}$, where *R* is retrieved image.

B. Structural Similarity Image Metrics

The base of the Structural Similarity is on the concept that the visual system of humans is deeply adapted to process structural information and the algorithm attempts to measure the change in this information between and reference and distorted image. In view of various tests, SSIM improves work at quantifying subjective quality of image than MSE or PSNR.

At a high level, attempts are made by SSIM to measure the alteration in luminance, contrast along with the structure in an image. Average pixel intensity is termed as Luminance, contrast by the fluctuation between the reference and distorted image, and structure by the cross-correlation between the 2 images [7].

$$SSIM(x,y) = \frac{\left(2\mu_x\mu_y + c_1\right)(2\sigma_{xy} + c_2)}{\left(\mu_x^2 + \mu_y^2 + c_1\right)\left(\sigma_x^2 + \sigma_y^2 + c_2\right)} \quad (6)$$

$$MSSIM = \frac{1}{T}\sum_{j=1}^{T} SSIM_j \quad (7)$$

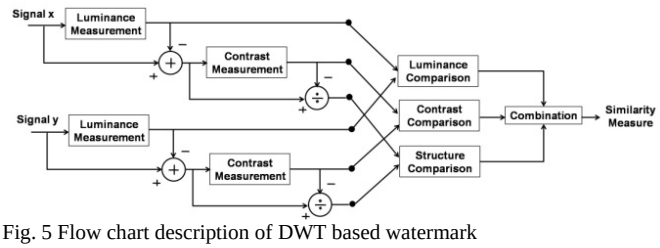


Fig. 5 Flow chart description of DWT based watermark

IV. Simulation Results

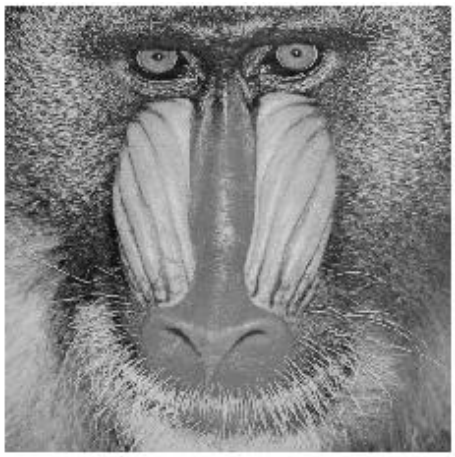
In the first phase, a key '3774' is send to the receiver using text steganography, and is successfully decoded at the receiver. For watermark embedding standard image, Lena, Baboon, Boat, Barbara and peppers is considered. Each image is in pgm format of size 512x512. Embedding depth for digital watermarking is considered to be 0.01.

A. DCT Results

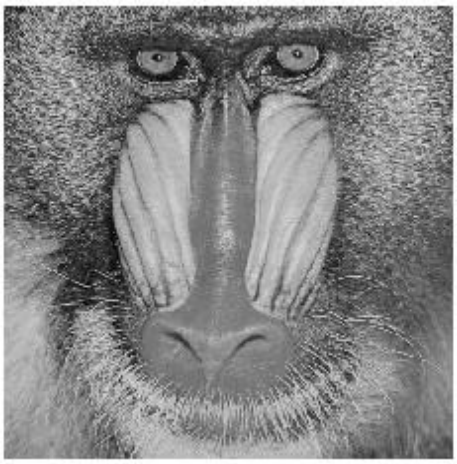
In table 1, results obtain under DCT is presented. Here, it can be observed that the PSNR of the considered images is nearly around 40 dB, and for most of the images, SSIM varies from a minimum value of 0.8644 for peppers to a maximum for Baboon with value 0.9239. For the illustration of results image of Baboon are shown in the paper. For the image of Lena PSNR is 41.0595 with SSIM is 0.8807.

TABLE I
PSNR AND SSIM FOR DIFFERENT IMAGES

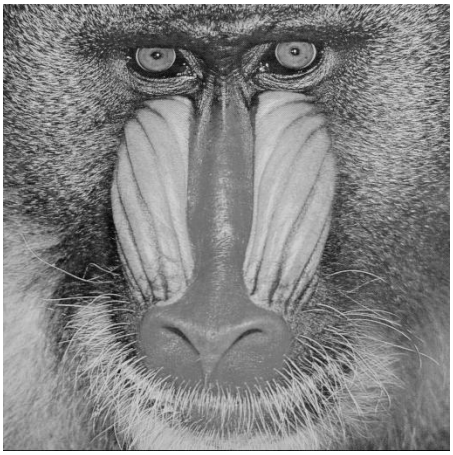
Performance Metrics		
Image	**PSNR**	**SSIM**
LENNA	41.0595	0.8807
BABOON	40.5107	0.9239
BOAT	40.8441	0.8802
BARBARA	41.0948	0.9146
PEPPERS	40.4979	0.8644



(a) Original Image



(b) Watermarked Image



(c) Retrieved Image

(d) SSIM Index Map Image

Fig. 6 (a),(b),(c),(d) Results (DCT)

In figure 6 (a-d), results for DCT are shown. In figure (a) original Baboon image is shown, and obtained watermarked image is shown in figure (b). In figure (c) retrieved image is shown, which is very much similar to the original and watermarked image. It is difficult for human eye to detect difference among these three images. To quantify the quality of image PSNR is obtained and shown in Table 2. The obtained SSIM map is shown figure (d).

V. CONCLUSIONS

This paper presents the detailed analysis of two fold secure online transmission system with basic steganography and watermarking techniques. The main aim of the paper is to analyse that DCT scheme are presented in terms of PSNR, and SSIM. The PSNR results are nearly same for various images however, SSIM varies significantly. Thus it is obvious that that PSNR alone cannot be considered as good quality measures for images. The two way protection scheme makes information transfer more secure and robust.

REFERENCES

[1] Chan, C.K. and L.M. Cheng, “Hiding data in images by simple LSB substitution, “Pattern Recognit., Vol. 37, pp. 469-474, 2001.

[2] R. Anderson and F. Petitcolas, "On the limits of steganography" IEEE Journal of Selected Areas in Communications, Vol. 16, No. 4, 1998.

[3] Adrian G. Boris and Ioannis Pitas, “Image watermarking using block site selection and DCT domain constraints”, Optics Express, Vol. 3, No. 12, pp.512-523,1998..

[4] Fridrich, J., M. Goljan and R. Du, “Detecting LSB steganography in color and gray-scale images,” IEEE Multimedia, Vol.8: pp.22-28,2001.

[5] Provos, N. and P. Honeyman, “Hide and seek: An introduction to steganography,”IEEE Secur. Privacy, 1: 32-44, 2003.

[6] Qin, J., X. Xiang and M.X. Wang, “A review on detection of LSB matching steganography, “Inform. Technol. J., 9: 1725-1738, 2010

[7] Wang, Z.; Bovik, A. C.; Sheikh, H. R. & Simoncelli E. P. “Image quality assessment: From error visibility to structural similarity,” *IEEE Trans. Image Processing*, Vol. 13, No. 4, pp. 600-612,2004.