Manit Kumar al. International Journal of Recent Research Aspects ISSN: 2349-7688, Vol. 2, Issue 2, June 2015, pp. 137-142

Digital image watermarking: a review

Manit Kumar[1], Mohinder Paul Malhotra[2]

[1]M.Tech Student, BIMT Panipat

[2]Assosiate Professor, BIMT Panipat

Abstract: **Digital watermarking is the act of hiding a message related to a digital signal (i.e. an image, song, video) within the signal itself. It is a concept closely related to steganography, in that they both hide a message inside a digital signal. However, what separates them is their goal. Watermarking tries to hide a message related to the actual content of the digital signal, while in steganography the digital signal has no relation to the message, and it is merely used as a cover to hide its existence. Watermarking has been around for several centuries, in the form of watermarks found initially in plain paper and subsequently in paper bills. However, the field of digital watermarking was only developed during the last 15 years and it is now being used for many different applications. This paper deals with the development of watermarking schemes for digital images stored in both, spatial and transformed domain. In this paper, we mainly focus on the Discrete Cosine Transform (DCT) and Discrete Wavelet Transform (DWT) based development.**

Keywords: DWT-DCT-PBFO, Watermarking.

I. INTRODUCTION

Digital watermarking is similar to watermarking physical objects except that the digital watermarking technique is used for digital content instead of physical objects. In digital watermarking a low-energy signal is imperceptibly embedded in another signal. The low energy signal is called watermark and it depicts some metadata, like security or rights information about the main signal. The main signal in which the watermark is embedded is referred to as cover signal since it covers the watermark. The cover signal is generally a still image, audio clip, video sequence or a text document in digital format. The digital watermarking system essentially consists of a watermark embedder and a watermark detector (See Figure 1). The watermark embedder inserts a watermark onto the cover signal and the watermark detector detects the presence of watermark signal. Note that an entity called watermark key is used during the process of embedding and detecting watermarks. The watermark key has a one-to-one

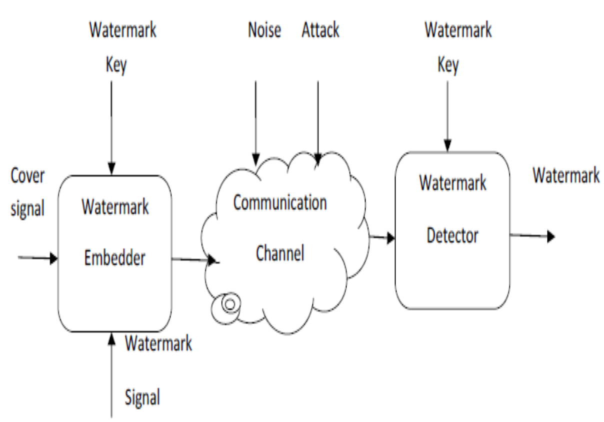

Figure 1: Generic digital watermark embedding and detection scheme

correspondence with watermark signal (i.e., a unique watermark key exists for every watermark signal). The watermark key is private and known to only authorized parties and it ensures that only authorized parties can detect the watermark. Further, note that the communication channel can be noisy and hostile (i.e., prone to security attacks) and hence the digital watermarking techniques should be resilient to both noise and security attacks. Watermark can be a number, text or image. Secret/public key is used to enforce security of watermarked content. For secure transport of watermarked data encryption/decryption is used. Watermark can be recovered by an authorized agency having secure key, watermark and / or original data. Watermarking process consists of 3 parts:

- Watermark
- Embedding Algorithm
- Extraction/Detection Algorithm

Digital Watermarking techniques can be classified in a number of ways depending on different parameter like cover medium, embedding domain, perception and application domain.

- According to type of Document or by Media: Text, Image, Video, Audio
- According to Human Perceptibility: Visible and Invisible.
- By goals and Imperceptibility: Robust, Fragile and Semi-fragile.
- By requirement of original for Extraction: Blind, Non-Blind, Public and Private.
- By embedding or according to Watermarking: Spatial domain and Transform domain.
- According to Application: Source based and Destination based.

© 2014 IJRRA All Rights Reserved

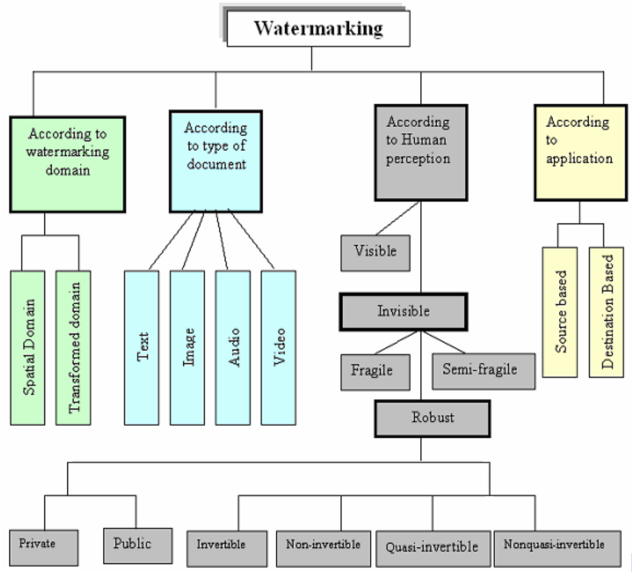

Figure 2: Classifications of Watermarking

1) Visible Watermarking: In it, visible watermarks are an extension of the concept of

logos. Such watermarks are applicable to images only. These logos are inlaid into the image but they are transparent. Such watermarks cannot be removed by cropping the center part of the image. The drawbacks of visible watermarking are degrading the quality of image and detection by visual means only. Such watermarking has applications in maps, graphics and software user interface.

2) Invisible Watermarking: In it, invisible watermark is hidden in the content. It can be detected by an authorized agency only. Such watermarks are used for content and or author authentication and for detecting unauthorized copier. Invisible watermarks do not change the signal to a perceptually great extent i.e. there are only minor variations in the output signal. An example of an invisible watermark is when some bits are added to an image modifying only its least significant bits. Invisible watermarks that is unknown to the end user. While the addition of the hidden message to the signal does not restrict that signal's use, it provides a mechanism to track the signal to the original owner.

3) Fragile Watermarking: In it, watermark embedded is known as fragile watermark or tamper-proof watermark. The fragile watermark is embedded in such a way that any manipulation or modification of the image would alter or destroy the watermark that is such watermarks are destroyed by data manipulation.

4) Asymmetric & Symmetric Watermarking: Asymmetric watermarking (also called asymmetric key watermarking) is a technique where different keys are used for embedding and detecting the watermark. In symmetric watermarking (or symmetric key watermarking) the same keys are used for embedding and detecting watermarks.

5) Steganographic & Non-Steganographic watermarking: Steganographic watermarking is the technique where content users are unaware of the presence of a watermark. In non-steganographic watermarking, the users are aware of the presence of a watermark. Steganographic watermarking is used in fingerprinting applications while non-steganographic watermarking techniques can be used to deter piracy.

6) Text document watermarking: Text document is a discrete information source. In discrete sources, contents cannot be modified. Thus, generic watermarking schemes are not applicable. The approaches for text watermarking are hiding watermark information in semantics and hiding watermark in text format.

   a) In Semantic-based watermarking, the text is designed around the message to be hidden. Thus, misleading information covers watermark information. Such techniques are known as scientific approach.

   b) In Text format watermarking, by text format mean layout and appearance. Commonly used techniques to hide watermark information are line shift coding, word shift coding and feature coding.

      - In line shift coding, single lines of the document are shifted upward or downward in very small amounts. The watermark information is encoded in the way lines are shifted upward or downward. Watermark recovery is simple because a line space in normal text is uniform.
      - In word shift coding, words are shifted horizontally in order to modify the spacing between consecutive words. While detecting the watermark, the original word spacing data is required because normally word spacing is variable.
      - In feature coding, feature of some characters are modified. In a typical case, the lengths of end lines to characters like b, d, h are modified. While detecting the watermark, the original lengths are known.

7) Spatial Domain Watermarking: Watermarking schemes that directly perform some transformation on the image pixels are called spatial domain watermarks. In a spatial domain watermarking scheme, the watermark is embedded by direct modifying the pixel value of an image. No transforms are applied to the host signal during watermark embedding. These spatial domain watermarking schemes are simple and less robust to common signal processing operations, since the watermark doesn't spread all over the image and some common signal processing easily erase the embedded watermark without affecting the quality of the watermarked image.

8) Frequency Domain Watermarking: It is also known as Transform Domain watermarking. On the other hand, frequency domain watermarking schemes involve embedding the watermark by modifying the transform co-efficient, after the image has been transformed to the transform domain or watermarking schemes that transform the image in the frequency domain and then modify the transform coefficients are called Transform domain.
9) Invisible-Robust Watermarking: In it, watermark is embedded in such a way that alternations made to the pixel value are perceptually not noticed and it can be recovered only with appropriate decoding mechanism. The robust watermark is specially designed to detect a wide range of "attacks", which basically are trying to remove the watermark, but without destroying the image/video.
10) Invisible-Fragile Watermarking: In it, watermark is embedded in such a way that any manipulation or modification of the image would alter or destroy the watermark. The fragile watermark is used for detecting even the smallest alteration of an image.
11) Source-based Watermarking: Source-based watermark are desirable for ownership identification or authentication where a unique watermark identifying the owner is introduced to all the copies of a particular image being distributed. A source-based watermark could be used for authentication and to determine whether a received image or other electronic data has been tampered.
12) Destination-based Watermarking: The watermark could also be destination-based where each distributed copy gets a unique watermark identifying the particular buyer. The destination-based watermark could be used to trace the buyer in the case of illegal reselling.

II. DISCRETE WAVELET TRANSFORM

In numerical analysis and functional analysis, a discrete wavelet transform (DWT) is any wavelet transform for which the wavelets are discretely sampled. As with other wavelet transforms, a key advantage it has over Fourier transforms is temporal resolution: it captures both frequency *and* location information (location in time). The discrete wavelet transform has a huge number of applications in science, engineering, mathematics and computer science. Most notably, it is used for signal coding, to represent a discrete signal in a more redundant form, often as a preconditioning for data compression. Practical applications can also be found in signal processing of accelerations for gait analysis, in digital communications and many others. It is shown that discrete wavelet transform (discrete in scale and shift, and continuous in time) is successfully implemented as analog filter bank in biomedical signal processing for design of low-power pacemakers and also in ultra-wideband (UWB) wireless communications.

Definition

One level of the transform

The DWT of a signal x is calculated by passing it through a series of filters. First the samples are passed through a low pass filter with impulse response g resulting in a convolution of the two:

$$y[n] = (x * g)[n] = \sum_{k=-\infty}^{\infty} x[k]g[n-k].$$

The signal is also decomposed simultaneously using a high-pass filter h. The output is the detail coefficients (from the high-pass filter) and approximation coefficients (from the low-pass). It is important that the two filters are related to each other and they are known as a quadrature mirror filter. However, since half the frequencies of the signal have now been removed, half the samples can be discarded according to Nyquist's rule. The filter outputs are then sub sampled by 2 (Mallat's and the common notation is the opposite, g- high pass and h- low pass):

$$y_{\mathrm{low}}[n] = \sum_{k=-\infty}^{\infty} x[k]h[2n-k]$$

$$y_{\mathrm{high}}[n] = \sum_{k=-\infty}^{\infty} x[k]g[2n-k]$$

This decomposition has halved the time resolution since only half of each filter output characterises the signal. However, each output has half the frequency band of the input so the frequency resolution has been doubled.

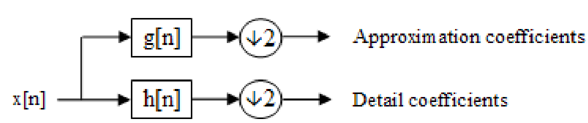

Figure 3: Block diagram of filter analysis

With the sub sampling operator $\downarrow$

$$(y \downarrow k)[n] = y[kn]$$

the above summation can be written more concisely.

$$y_{\mathrm{low}} = (x * g) \downarrow 2$$

$$y_{\mathrm{high}} = (x * h) \downarrow 2$$

However computing a complete convolution $x * g$ with subsequent downsampling would waste computation time.

Cascading and Filter banks

This decomposition is repeated to further increase the frequency resolution and the approximation coefficients decomposed with high and low pass filters and then down-

© 2014 IJRRA All Rights Reserved

sampled. This is represented as a binary tree with nodes representing a sub-space with a different time-frequency localisation. The tree is known as a filter bank.

At each level in the above diagram the signal is decomposed into low and high frequencies. Due to the decomposition process the input signal must be a multiple of 2^n where n is the number of levels.

In image analysis 2D DWT is used which breaks the image into four different coefficients named approximation, horizontal, vertical and diagonal coefficient. Maximum energy is lying with the approximation coefficient as shown in figure 4.

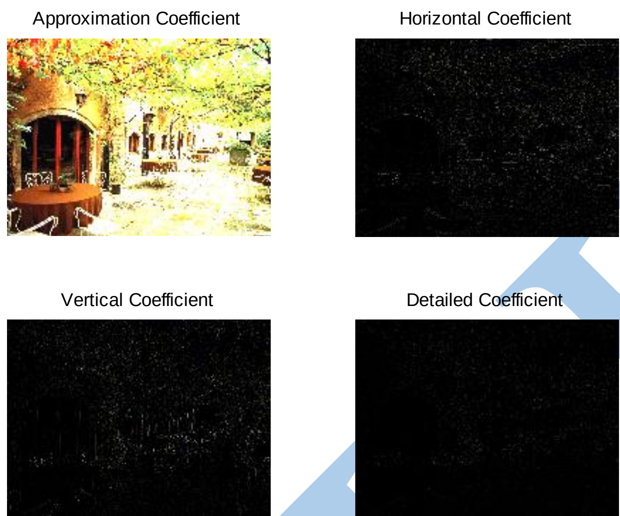

Figure 4: DWT2 transform on an image

III. DISCRETE COSINE TRANSFORM

DCT breaks the image into two different frequency components: low frequency and high frequency. Low frequency component contains high energy and can be considered as luminance part of image whereas reflectance is constituted by high frequency component as it contains the low energy. A discrete cosine transform (DCT) expresses a finite sequence of data points in terms of a sum of cosine functions oscillating at different frequencies. DCTs are important to numerous applications in science and engineering, from lossy compression of audio (e.g. MP3) and images (e.g. JPEG) (where small high-frequency components can be discarded), to spectral methods for the numerical solution of partial differential equations. The use of cosine rather than sine functions is critical for compression, since it turns out (as described below) that fewer cosine functions are needed to approximate a typical signal), whereas for differential equations the cosines express a particular choice of boundary conditions. In particular, a DCT is a Fourier-related transform similar to the discrete Fourier transform (DFT), but using only real numbers. DCTs are equivalent to DFTs of roughly twice the length, operating on real data with even symmetry (since the Fourier transform of a real and even function is real and even), where in some variants the input and/or output data are shifted by half a sample. There are eight standard DCT variants, of which four are common. The most common variant of discrete cosine transform is the type-II DCT, which is often called simply "the DCT", its inverse, the type-III DCT, is correspondingly often called simply "the inverse DCT" or "the IDCT".

The discrete cosine transform (DCT) helps separate the image into parts (or spectral sub-bands) of differing importance (with respect to the image's visual quality). The DCT is similar to the discrete Fourier transform: it transforms a signal or image from the spatial domain to the frequency domain.

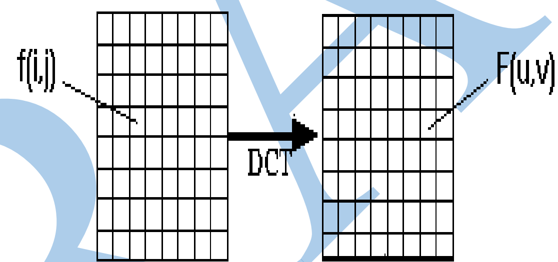

Figure 5: Discrete cosine transform

The general equation for a 2D (N by M image) DCT is defined by the following equation:

$$B_{pq} = \alpha_p \alpha_q \sum_{m=0}^{M-1} \sum_{n=0}^{N-1} A_{mn} cos \frac{\pi(2m+1)p}{2M} cos \frac{\pi(2n+1)q}{2N}$$

$$\alpha_p = \begin{cases} \frac{1}{\sqrt{M}}, p = 0 \\ \sqrt{\frac{2}{M}}, 1 \le p \le M-1 \end{cases}$$

$$\alpha_q = \begin{cases} \frac{1}{\sqrt{N}}, q = 0 \\ \sqrt{\frac{2}{N}}, 1 \le q \le N-1 \end{cases}$$

and the corresponding ***inverse*** 2D DCT transform is.:

$$B_{pq} = \alpha_p \alpha_q \sum_{m=0}^{M-1} \sum_{n=0}^{N-1} A_{mn} cos \frac{\pi(2m+1)p}{2M} cos \frac{\pi(2n+1)q}{2N}$$

$$A_{mn} = \sum_{m=0}^{M-1} \sum_{n=0}^{N-1} \alpha_p \alpha_q cos \frac{\pi(2m+1)p}{2M} cos \frac{\pi(2n+1)q}{2N}$$

The low frequency component of dct contains the maximum information about an image whereas high frequency component only has fine details as shown in figure 6.

© 2014 IJRRA All Rights Reserved

Figure 6(a) Original Image

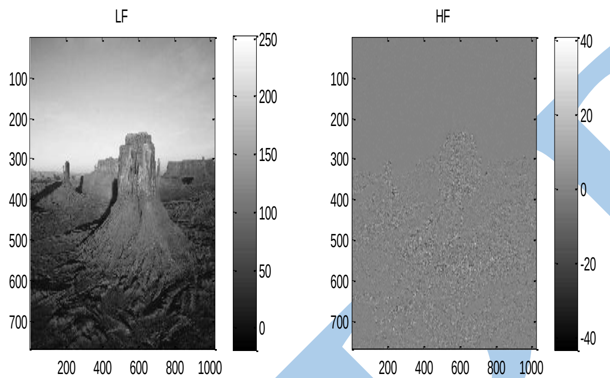

Figure 6 (b) Low frequency coefficients, high frequency coefficient

As, is clear from the above figure that after converting the original image into gray scale low frequency coefficient shows the maximum information whereas high frequency coefficient depicts nothing.

IV. LITERATURE REVIEW

Ray-Shine (2012) proposed two methods to improve the reliability and robustness. To improve the reliability, for the first method, the principal components of the watermark are embedded into the host image in discrete cosine transform (DCT); and for the second method, those are embedded into the host image in discrete wavelets transform (DWT). To improve the robustness, the particle swarm optimization (PSO) is used for finding the suitable scaling factors. The experimental results demonstrate that the performance of the proposed methods outperforms than those of the existing methods.

Sonil Sood (2014) proposes a novel method for watermarking relational databases based on hybrid model optimization in which the embedding and extracting algorithms of watermarking in discrete wavelet transform (DWT) are combined with Genetic Algorithm (GA)-Bacterial Foraging Algorithm (BFO) based optimization techniques for watermarking. We use the 5-level DWT for the spatial transform; because of this we get the more accurate watermark. Identification of owner is cryptographically made secure and used as an embedded watermark. Strength of BFA is explored to make the technique robust, secure and imperceptible.

Hsiang-Cheh Huang (2010) presented the optimization of robust watermarking using bacterial foraging optimization algorithm. By finding tradeoffs among different watermark robustness and imperceptibility, and considering the adaptive tuning of weighting factors, we design a practical fitness function for optimization. Simulation results depict the better performances over existing implementations with GA, and hence fuzzy-based BF can be considered to be another practical optimized watermarking scheme.

Sonil Sood (2014) provides a survey of various optimization techniques for watermarking databases. The Genetic Algorithm (GA) is a class of optimization algorithm that mimics the process of natural evolution. Genetic algorithm helps in searching appropriate locations in cover images to insert watermark. Also its hybridization with other nature inspired algorithms can further improve the process of watermarking.

P. Surekha (2011) proposes a new optimization method for digital images in the Discrete Wavelet Transform (DWT) domain. Digital image watermarking has proved its efficiency in protecting illegal authentication of data. The amplification factor of the watermark is the significant parameter that helps in improving the perceptual transparency and robustness against attacks. The tradeoff between the transparency and robustness is considered as an optimization problem and is solved by applying Genetic Algorithm. The experimental results of this approach prove to be secure and robust to filtering attacks, additive noise, rotation, scaling, cropping and JPEG compression. The Peak Signal to Noise Ratio (PSNR), Mean Square Error (MSE), and computational time are evaluated for a set of images obtained from the Tampere University of Technology, Finland using the MATLAB R2008b software.

Khaled Loukhaoukha (2011) suggested a new optimal watermarking scheme based on lifting wavelet transform (LWT) and singular value decomposition (SVD) using multi-objective ant colony optimization (MOACO) is presented. The singular values of the binary watermark are embedded in a detail subband of host image. To achieve the highest possible robustness without losing watermark transparency, multiple scaling factors (MSF) are used instead of a single scaling factor (SSF). Determining the optimal values of the multiple scaling factors (MSF) is a difficult problem. However, to determine these values, a multi-objective ant colony-based optimization method is used. Experimental results show much improved performances in terms of transparency and robustness for the proposed method compared to other watermarking schemes. Furthermore, the proposed scheme does not suffer from the problem of high probability of false positive detections of the watermarks.

© 2014 IJRRA All Rights Reserved

V. REFERENCES

[1]. Abdelaziz I. Hammouri, Basem Alrifai and Heba Al-Hiary," An Intelligent Watermarking Approach Based Particle Swarm Optimization in Discrete Wavelet Domain" IJCSI International Journal of Computer Science Issues, Vol. 10, Issue 2, No 1, March 2013

[2]. Ray-Shine Run, Shi-Jinn Horng, Jui-Lin Lai, Tzong-Wang Kao, Rong-Jian Chen," An improved SVD-based watermarking technique for copyright protection" Expert Systems with Applications 39 (2012)

[3]. Sonil Sood, Ajay Goyal," Watermarking Relational Databases using Genetic Algorithm & Bacterial Foraging Algorithm" International Journal of Information & Computation Technology, Volume 4, Number 17 (2014)

[4]. Hsiang-Cheh Huang, Yueh-Hong Chen, Ajith Abraham," Optimized Watermarking Using Swarm-Based Bacterial Foraging" Journal of Information Hiding and Multimedia Signal Processing, Volume 1, Number 1, January 2010.

[5]. Sonil Sood," Digital Watermarking Using Hybridization of Optimization Techniques:A Review" International Journal of Computer Science and Information Technologies, Vol. 5 (4) , 2014.

[6]. P. Surekha and S. Sumathi," Implementation Of Genetic Algorithm For A Dwt Based Image Watermarking Scheme" Ictact Journal On Soft Computing: Special Issue On Fuzzy In Industrial And Process Automation, July 2011, Volume: 02, Issue: 01.

[7]. Zhicheng Wei, Hao Li, Jufeng Dai ,Sashuang Wang," Image Watermarking Based On Genetic Algorithm" IEEE 2006

[8]. Mahmoud Elnajjar, A.A Zaidan, B.B Zaidan, Mohamed Elhadi M.Sharif and amdan.O.Alanazi," Optimization Digital Image Watermarking Technique for Patent Protection" Journal Of Computing, Volume 2, Issue 2, February 2010.

[9]. Khaled Loukhaoukha," Optimal Image Watermarking Algorithm Based on LWT-SVD via Multi-objective Ant Colony Optimization" Journal of Information Hiding and Multimedia Signal Processing, Volume 2, Number 4, October 2011.

[10]. Mona M. Soliman, Aboul Ella Hassanien, Neveen I. Ghali and Hoda M. Onsi," An adaptive Watermarking Approach for Medical Imaging Using Swarm Intelligent" International Journal of Smart Home Vol. 6, No. 1, January, 2012.

[11]. V. Aslantas," Optimal SVD based Robust Watermarking using Differential Evolution Algorithm" Proceedings of the World Congress on Engineering 2008 Vol I.

[12]. S.Veeramani, Y.Rakesh," An Optimization Technique for Image Watermarking Scheme" International Journal of Computer Trends and Technology (IJCTT) – volume 5 number 3 –Nov 2013.

[13]. Krati vyas, B.L.Pal," Proposed Method In Image Steganography To Improve Image Quality With Lsb Technique" International Journal of Advanced Research in Computer and Communication Engineering Vol. 3, Issue 1, January 2014.

[14]. Parisa Gerami, Subariah Ibrahim, Morteza Bashardoost," Least Significant Bit Image Steganography using Particle Swarm Optimization and Optical Pixel Adjustment" International Journal of Computer Applications (0975 – 8887) Volume 55– No.2, October 2012.

[15]. Navdeep Kaur," Steganography Using Particle Swarm Optimization-A Review" International Journal Of Engineering Sciences & Research Technology, November, 2013.

[16]. Aisha Fernandes, Wilson Jeberson," A Simple Steganographic Technique with a Good Embedding Capacity" International Journal of Darshan Institute on Engineering Research and Emerging Technology Vol. 2, No. 2, 2013, pp. 56-61

© 2014 IJRRA All Rights Reserved