



Separable Reversible Data Hiding For Digital Images Using Dual Watermarking

Sneha Kumbhar, Jyoti Bhogade, Monika Kadhane
Dept. of IT, Pune University, Pune,
Maharashtra, India

Abstract: This paper presents a new method for embedding data into an image called "A Block Complexity based Data Embedding" (ABCDE). The principle of the method is the same as that of BPCS-Steganography. Embedding is performed by replacing pixel data of noisy regions in an image with another noisy data obtained by converting data to be embedded. A complexity measure is defined in BPCS-Steganography for discriminating noisy regions in an image. In the proposed system, a Dual Watermarking Scheme based on DWT-SVD with chaos encryption algorithm, will be developed to improve the robustness and protection along with security. DWT and SVD have been used as a mathematical tool to embed watermark in the image. Two watermarks are embedded in the host image. The secondary is embedded into primary watermark and the resultant watermarked image is encrypted using chaos based logistic map. This provides an efficient and secure way for image encryption and transmission.

Keywords— Bit-plane blocks, Wavelet watermarking, Alpha-Channel Masking.

I. INTRODUCTION

Reversible data hiding (RDH) in images is a technique, by which the original cover can be losslessly recovered after the embedded message is extracted. This important technique is widely used in medical imagery, military imagery and law forensics, where no distortion of the original cover is allowed. Since first introduced, RDH has attracted considerable research interest.

Here we are investigating the data hiding technique which is reversible in nature. Thus it is termed as Reversible data hiding technique. Using the encrypted image as a cover data in which the data is embedded. In separable reversible data hiding technique firstly a content owner encrypts the original uncompressed image then a data hider compress the image to create space to accommodate some additional data. At the receiver side there are three possibilities to retrieve the embedded data and get covering data; this is the basic theme of this concept[7].

The process of embedding information into another object/signal can be termed as watermarking. Watermarking is mainly used for copy protection and copyright-protection. Historically, watermarking has been used to send "sensitive" information hidden in another signal. Watermarking has its applications in image/video copyright protection. The characteristics of a watermarking algorithm are normally tied to the application it was designed for. Digital watermarking is the process of embedding information into a digital signal which may be used to verify its authenticity or the identity of its owners, in the same manner as paper bearing a watermark for visible identification. In digital watermarking, the signal may be audio, pictures, or video. If the signal is copied, then the information also is carried in the copy. A signal may carry several different watermarks at the same time[1].

In visible digital watermarking, the information is visible in the picture or video. Typically, the information is text or a logo, which identifies the owner of the media. The image on the right has a visible watermark. When a television broadcaster adds its logo to the corner of transmitted video, this also is a visible watermark[1].

In the invisible digital watermarking, information is added as digital data to audio, picture, or video, but it cannot be perceived as such (although it may be possible to detect that some amount of information is hidden in the signal). The watermark may be intended for widespread use and thus, is made easy to retrieve or, it may be a form of Steganography, where a party communicates a secret message embedded in the digital signal. In either case, as in visible watermarking, the objective is to attach ownership or other descriptive information to the signal in a way that is difficult to remove. It also is possible to use hidden embedded information as a means of covert communication between individuals [5].

One application of watermarking is in copyright protection systems, which are intended to prevent or deter unauthorized copying of digital media. In this use, a copy device retrieves the watermark from the signal before making a copy; the device makes a decision whether to copy or not, depending on the contents of the watermark [3]. Another application is in source tracing. A watermark is embedded into a digital signal at each point of distribution. If a copy of the work is found later, then the watermark may be retrieved from the copy and the source of the distribution is known. This technique reportedly has been used to detect the source of illegally copied movies. Annotation of digital photographs with descriptive information is another application of invisible watermarking. While some file formats for digital media may contain additional information called metadata, digital watermarking is distinctive in that the data is carried right in the signal[6].

A) Primary Watermark

Primary watermark shall contain the author and copyright information of the image. This information will be embedded on original image so that an image shall always carry its copyright information with it. We shall achieve this using BPCS Steganography[3].

B) Secondary Watermark

We will use intermediate image data (grayscale component of the intermediate image) itself as the data to be watermarked on the intermediate image. This data will help us determine if there is any modification or damage done to the original image and also reconstruct the original image to some extent. We shall do this using Alpha Channel / Transparency Channel masking [5].

II. PROBLEM STATEMENT

Digital Watermarking is used for copyright protection and authentication. In the proposed system, a Dual Watermarking Scheme based on BPCS Algorithm and Alpha Channel /Transparency Channel Masking Algorithm will be developed to improve the robustness and protection along with security [2]. Two watermarks will be embedded in the host image. The secondary is embedded into primary watermark and the resultant watermarked image can then be transmitted over a non secure channel. This provides an efficient and secure way for image security and transmission. The watermarked image is decrypted and a reliable watermark extraction scheme can be developed for the extraction of the primary as well as secondary watermark from the image.

III. RELATED WORK

A) Embedding Techniques:

Inputs: - Text file, cover image 1, cover image 2 and secret key.

Output: - Stego image

Begin

1. Select a text file, convert it into binary form and calculate the number of bits in it.

2. Select a carrier image (cover image 1) for hiding purpose, find the number of pixels, convert it into RGB image and calls the compression function.

3. If bits calculated are compatible with the image resolution, then

Start sub iteration 1

Replace red component of the first pixel with first character. Replace green component of the second pixel with second character. Replace blue component of the third pixel with third character. And repeat iterations until pixels get exhaust.

Stop sub iteration 1

Else

Repeat sub iteration 1

Finds necessary compression ratio and perform sub iteration 2.

Sub iteration 2

Replace necessary bits as defined by the compression ratio in immediate component of each pixel. Store the information about bits embedded in a binary address file.

Stop sub iteration2

4. Provide a security key as encryption completes.

5. Select 2nd cover image to hide the distorted stego image.

End

B) Extraction technique:

Input:- Stego image and secret key.

Output:-secret text file.

Begin

1.Browse the stego image.

2.Choose the folder in which you want to extract the hidden text file.

3.Provide necessary security key.

4.convert the binary file into human readable form.

End

C) Block Complexity Measure:

The new embedding method ABCDE is based on the principle introduced in BPCS.A resource file is converted into noisy data, and is replaced with the pixel data in noisy regions of a container image. We have to locate noisy regions appropriately to embed the resource file secretly. If not, informative regions of the container image would be disordered by the embedded resource file and noticeable changes would be left after embedding.

In BPCS the noisy region of an image is

located on each bit-plane as small pixel blocks those have noisy patterns. Each bit-plane of a container image is regularly divided into small square binary pixel blocks a illustrated in Figure 1.A binary pixel block can be regarded as one in a noisy region if it has a complex black-and-white pattern. Only such complex blocks are used for embedding.

On embedding the blocks on the lowest bit-plane (the LSB plane) is used first. The blocks in a container image are examined one by one from those on the LSB plane through up to those on the highest bit-plane (the MSB plane). A resource file is embedded piece by piece as a complex block is found on a bit-plane. This way of embedding is preferable, because changes in lower bit-planes would not spoil the quality of a container image greatly.

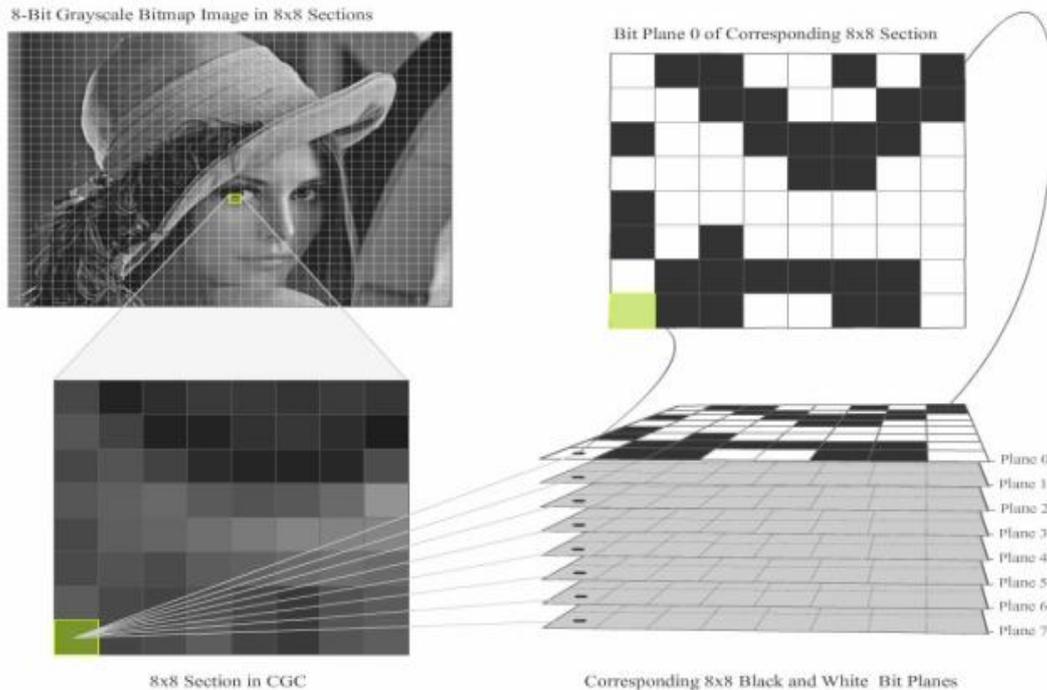


Figure 1: Binary pixel blocks on bit-planes

D) Black & White Border Complexity Measures:

We find that a block is simple when it is entirely or almost entirely in black or white. Figure 2 shows an 8x8 block. It looks simple. There are $(8-1) \times 8 \times 2 = 112$ pixel borders inside, but only eight out of them lie between black and white pixels. The others lie between the same color pixels, i.e., either between two white pixels or between two black pixels. A block can thus be regarded as simple when it has a few black-and white borders in it.

This observation leads us to the definition of a complexity measure of a block based on the total length of black-and-white borders in it, which is employed in BPCS. Suppose that k out of M pixel borders lie between black and white pixels in a block, the complexity measures is then given by

$$\alpha = k/M.$$

E) α Channel Masking:

The length of the black-and-white border in a binary image is a good measure for image complexity. If the border is long, the image is complex, otherwise it is simple. The total length of the black-and-white border equals to the summation of the number of color-changes along the rows and columns in an image. For example, a single black pixel surrounded by white background pixels has the boarder length of 4. We will define the image complexity α by the following.

$$\alpha = k / (\text{The max. possible B - W changes in the image})$$

(1) Where, k is the total length of black-and-white border in the image. So, the value ranges over $0 \leq \alpha \leq 1$. (2)

(1) is defined globally, i.e., α is calculated over the whole image area. It gives us the global also use α for a local image complexity (e.g., an 8×8 pixel-size area). We will use such α as our local complexity measure in this paper.

IV. PROPOSED SYSTEM

Dual watermarking scheme based on DWT and Singular Value Decomposition (SVD) along with the chaos based encryption technique is proposed. After decomposing the cover image into four bands (LL, HL, LH, and HH), we apply the SVD to each band, and modify the singular values of the cover image with the singular values of the watermarked primary watermark. When the primary watermark image is in question, the invisible secondary watermark can provide rightful ownership. Modification in all frequencies allows the development of a watermarking scheme that is robust to a wide range of attacks. SVD transform is performed on all the images and sum up the singular values to find the new singular values. Both the watermarks are embedded in the same manner and the watermarked primary watermark is encrypted using chaos encryption.

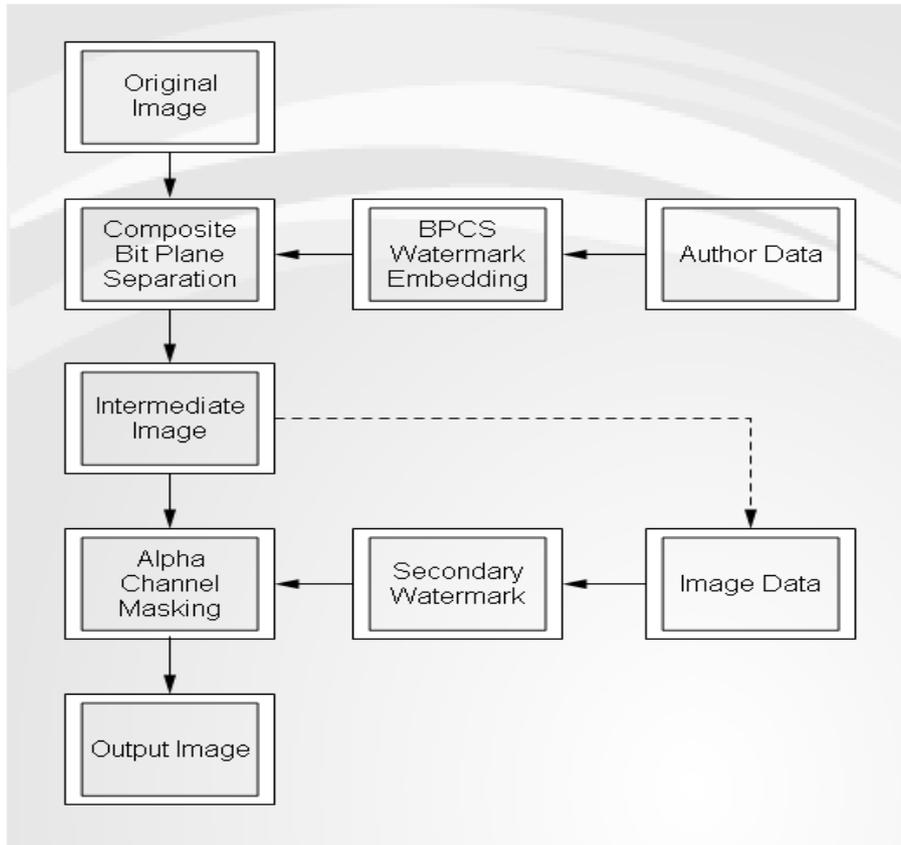


Figure 2: Block Diagram of Proposed System

A) MODULES:

In the proposed system, there are four modules, they are as follows:

1. Embedding secondary watermark into primary.
2. Encryption of watermarked primary image and embedding in the host image.
3. Attacks
4. Extraction of primary and secondary watermark from the host image.

A. Embedding secondary watermark into primary watermark

In two-dimensional DWT, each level of decomposition produces four bands of data denoted by LL, HL, LH, and HH. The LL subband can further be decomposed to obtain another level of decomposition. This process is continued until the desired number of levels determined by the application is reached. In DWT-SVD based watermarking, the singular values of the detail and approximate coefficients are extracted. The extracted singular values are modified to embed the watermark data.

LL2	HL2	HL1
LH2	HH2	
LH1		HH1

Figure 3: DWT

Let A be a general real matrix of order $m \times n$. The singular value decomposition (SVD) of A is the factorization:

$$A = U * S * V^T \quad (1)$$

where U and V are orthogonal(unitary) and $S = \text{diag}(\sigma_1, \sigma_2, \dots, \sigma_r)$, where $\sigma_i, i = 1(1)r$ are the singular values of the matrix A with $r = \min(m, n)$ and satisfying :

$$\sigma_1 \geq \sigma_2 \geq \dots \geq \sigma_r \quad (2)$$

The first r columns of V the right singular vectors and the first r columns of U the left singular vectors.

Use of SVD in digital image processing has some advantages. First, the size of the matrices from SVD transformation is not fixed. It can be a square or a rectangle. Secondly, singular values in a digital image are less affected if general image processing is performed. Finally, singular values contain intrinsic algebraic image properties.

B. Encryption

Chaos theory is a branch of mathematics which studies the behavior of certain dynamical systems that may be highly sensitive to initial conditions. This sensitivity is popularly referred to as the butterfly effect. As a result of this sensitivity, which manifests itself as an exponential growth of error, the behavior of chaotic systems appears to be random. That is, tiny differences in the starting state of the system can lead to enormous differences in the final state of the system even over fairly small timescales. This gives the impression that the system is behaving randomly.

Chaos-based image encryption techniques are very useful for protecting the contents of digital images and videos. They use traditional block cipher principles known as chaos confusion, pixel diffusion and number of rounds. The complex structure of the traditional block ciphers makes them unsuitable for real-time encryption of digital images and videos. Real-time applications require fast algorithms with acceptable security strengths. The chaotic maps have many fundamental properties such as ergodicity, mixing property and sensitivity to initial condition/system parameter and which can be considered analogous to some cryptographic properties of ideal ciphers such as confusion, diffusion, balance property.

A chaos-based image encryption system based on logistic map, in the framework of stream cipher architecture, is proposed. This provides an efficient and secure way for image encryption and transmission.

C. Attacks

To investigate the robustness of the algorithm, the watermarked image is attacked by Average and Mean Filtering, JPEG and JPEG2000 compression, Gaussian noise addition, Resize, Rotation and Cropping. After these attacks on the watermarked image, we compare the extracted watermarks with the original one. The watermarked image quality is measured using PSNR (Peak Signal to Noise Ratio).

D. Extraction of watermarks

Decryption is the reverse iteration of encryption.

After decryption of the watermarked primary image, the extraction process takes place.

V. RESULT ANALYSIS

Experiment is performed in five stages. In first stage the cover image is divided into 8 bits plane block using BPCS algorithm and set the threshold value using alpha channel masking algorithm. In second stage primary watermark is done on the cover image. In third stage secondary watermark is done. In fourth stage there is extraction of data and recovery of cover image. In last stage there is verification of original image. If any damage or modification in the original image it can be reconstruct using alpha channel masking.



Figure.4 Cover Image Before Watermarking



Figure.5 Stego-Image After Watermarking

VI. CONCLUSION

This paper discussed the possibility of hiding text file, image, short audio and video messages inside digital images. This paper provides an efficient and secure way for image encryption and transmission. It also deals with a novel dual watermarking scheme, which include encryption, to improve rightful ownership, protection and robustness.

REFERNCES

- [1] Dual Watermarking Scheme with Encryption *Proceedings of the Int. Conf. on Information Science and Applications ICISA 2010 Chennai, India. 6 February 2010.*
- [2] Wu J, Zhang R et al. Reliable Detection of BPCS Steganography[J]. *Journal of Beijing University of Posts and Telecommunications*, 2009, 32(4): 113-121
- [3] Mussarat Abdullah, and Fazal Wahab “Key Based Text Watermarking of E-Text Documents in an object based Environment using Z-axis for Watermark Embedding”, *world academy of engg and technology* 46, 2008
- [5] Mohamed Saehab, Elisa Bertino, Arif Ghafoor “Watermarking Relational Databases Using Optimization-Based Techniques” 2011

- [6] Copyright Protection of Online Application using Watermarking, march 2011
- [7] “Reversible data hiding in encrypted images by reserving room before encryption” IEEE Transactions On Information Forensics And Security, Vol. 8, No. 3, March 2013.
- [8] Proceedings of the 2013 International Conference on Pattern Recognition, Informatics and Mobile Engineering (PRIME) February 21-22 ©2013 IEEE “Separable Reversible Data Hiding Using Rc4 Algorithm”
- [9] Rakhee Lakhera , Shital Behare , Alka Gulati, - A Novel Approach for Watermarking using Dual Watermarking Technique, IJCEM International Journal of Computational Engineering & Management, Vol. 15 Issue 4, July 2012