Digital Watermarking Using Least Significant Bit Algorithm

Neha Jadhav, Suverna Kharat, Punam Nagare.
Guided By Prof. Harsha Sarode
Nutan Maharashtra Institute of Engineering and Technology, Pune.

ABSTRACT:
Digital watermarking is one of the types of digital signal which hidden directly in digital content. It helps to make the distribution of digital material more secure. Digital watermarking has the properties like strongness, security, transparency, complexity, capacity, and verification. A Digital Watermarking is a form of steganography in which copy-move and other source information is hidden inside a document, image or sound file without the user’s knowledge. Many companies involved in digital watermarking activities with different types of watermarks. It discusses different techniques for images, text and other applications of digital watermarking.

KEYWORDS: Digital watermarking, LSB

1. INTRODUCTION:
Steganography is a method of hiding digital information. Steganography can be applied to many types of data, like audio, video, and images and can hide any kind of digital information. For security steganography consists of a significant challenge as it hides the act of communication; LSB steganography, in which the lowest bit plane of a bitmap image is used to convey the secret data, has long been known to steganographers. Because the eye cannot detect the very small perturbations it introduces into an image and because it is extremely simple to implement,1 LSB methods are commonly used among the many free steganography tools available on the internet. There are two types of LSB steganography: LSB replacement and LSB matching. In the LSB matching first split the RGB channel of an input image into LSB and non LSB(MSB). Then calculate the parity of non LSB. Then set digital data(0,1) for even parity or odd parity. Then in last compare the LSB with the calculated part of non-LSB. And detect the hidden part of an image. LSB replacement is very similar, except that the LSBs of the cover pixels are simply overwritten by the secret bit stream.

2. PREVIOUS SYSTEM:
In this section a literature survey of digital Watermarkings technique used for images is presented. It shows the previous work which had been done on digital watermarks and their results.
1] Ersin Elbasi et al enclosed the watermark in the Discrete Wavelet Transform domain. For watermark enclosing, the two level DWT decomposition of an NxN gray scale image I is computed.
2] Gil-Je Lee et al , represented a simple and strong watermarking technique by using random mapping function. The proposed algorithm is watermark enclosing which can be very strong than the simple watermarking algorithm.
3] Saeid Fazli et al , searched the trade-off between unobservable and strongness of LSB watermarking. In this algorithm, instead of lower bit planes significant bit-planes of the watermark image are put in picture. So, they analyse the effect of image compression on the watermark, and estimate the strongness and unobserveability by calculating the distortion occurs due to watermarking.
4] Gaurav Bhatnagar et al , represented a new semiblind reference watermarking scheme based on discrete wavelet transform (DWT) and singular value decomposition (SVD) for copyright protection and authenticity.

3. PROPOSED SYSTEM:
We proposed a new digital algorithm depends on LSB techniques. Most of authors has proposed the third and forth LSB but our proposed watermarking algorithm is using first LSB for hiding the data for security purpose. So, no one will know that there is some data is hidden in the image. To hide information in a cover images, least significant bit technique is used. In LSB techniques, pixels are changed by bits of hidden message inside the image. To hide the message inside image least bits needed to be changed from eight bytes of grids. Only few bits needed in an image to modify or hide a secret message. Because the quality of the Watermarked image is very low, less than 4-bit LSB. While changing the LSB of a pixel it results in small changes in the intensity of the colors. So these changes cannot be visible for naked human eye. Only professional tracker solve which type of information hidden inside the image. For example, Figure 1 shows the 1-bit LSB. In Figure 1, the pixel value of the cover image is (11000101)₂ and the secret data is 0. It is stored into LSB-1 therefore, the changed pixel value of the pixel is (11000100)₂. LSB can store 1-bit in each pixel. If the cover image size is 256 x 256 pixel image, it can thus store a total amount of 65,536 bits or 8,192 bytes of hidden data in an image.

![Fig.1. An example of 1 bit LSB](image)

3.1 **BLOCK DIAGRAM OF LSB WATERMARKING:**

3.2 **WORKING OF LSB WATERMARKING:**
1. Take color image as an input.
2. Separate RGB values of image.
3. Separate MSB and LSB of input image.
4. Calculate parities from MSB.
5. For even parity set ‘1’ into LSB and for odd parity set ‘0’ into LSB.
6. Compare LSB.
7. If any change occurs then forgery detected.

3.3 **FLOWCHART OF LSB WATERMARKING:**

![Fig.2. Block Diagram Of LSB Watermarking](image)
4. RESULTS:

Modified image

Output image

Modified image

Output image

Modified image

Output image

Modified image

Output image

5. CONCLUSION:

For secure intellectual property is currently a very important topic for media, for university administrators and for the publishing industries. In digital watermarking robustness describes whether the watermark can be reliably detected after any changes in the original image like rotation, scaling or cropping. It exists for entertainment companies and libraries because it offers the promise of better protecting their multimedia content from piracy. It is transparent in use, does not increase files sizes, and yet is highly robust and secure. The understanding of the theory behind digital watermarking will lead to the design of more reliable systems for more applications. LSB may be detected simply through visual inspection of an image and its bit-planes, or more reliably through methods which use statistical metrics to identify the likelihood an image contains hidden data. Steganography proves to be a significant technique for detection when communicating. The detection issues with steganography create challenges for security systems in attempting to prevent the transmission of steganographic content.

REFERENCES: