Comparison of SVD-Watermarking and LSB-Watermarking Techniques

Anupma Yadav #1, Anju Yadav #2

#1 computer science, ITM University, Gurgaon
#2 Computer Science, Rewari

1 anupmayadav90@gmail.com, 2 anjucuty@gmail.com

Abstract—Watermarking, belongs to the data hiding field, has gain lot of attention and interest of researcher. There is work going on in this field. There are various use of watermarking algorithms that includes content protection, tamper detection, and copyright protection. In this paper, we presented two well known watermarking technique SVD and LSB in terms of image. When we compared them, earlier one shows better result as compared to the former.

Key Words: digital watermarking, SVD, LSB, PSNR, MSE

I. INTRODUCTION

Watermarking refers to the process of protecting our essential information in digital means like image, audio, video etc. In other terms, we can say watermark is kind of a signature that tells about the true owner of the multimedia object. The information send over network needs to be protected by one way or other. In order to secure our information, insert watermark in it. Digital watermarking technology promises the data security, copyright protection and authentication. Digital watermarking can refer to the embedding of watermark in images, video, audio, and signals. Watermarking consist of two sections watermark embedding and watermark extraction. In watermark embedding we use to embed the information, while in extraction, the embedded watermark is extracted and compared with the original. In this paper our main focus will be on two technologies one is least significant bit watermarking and other is singular value decomposition watermarking.

The paper is organized as follow: section II consist of digital watermarking technique in detail, section III consist of utilization and application of watermarking technology, section IV discuss the LSB watermarking and SVD watermarking technique, section V show the comparison of LSB and SVD in terms of PSNR, MSE etc. section VI discuss about the possible attacks and section VII conclusion.
II. DIGITAL WATERMARKING TECHNIQUE

Watermarking is defined as a technique to hide secret information termed as watermark inside any multimedia object. For example we can say the watermark is considered as a signature that reveals the proof of owner identity. Watermark is broadly categories into two parts: visible and invisible. Name itself explain them, the visible watermark, is visible to the human eye in the cover object, while, the invisible is hidden inside the cover object and no human can tell by just seeing it, that, watermark is there. Mainly the watermarking technique consist of two parts: watermark embedding and watermark extracting. In watermark embedding, the process of hiding a watermark in cover image is explained, as shown in fig.1, the step by step explanation. In watermark extraction, the receiver of watermarked image tries to recover the watermark form it. The extracted watermark possibly suffered some attack during sending. Hence to validate the recovered watermark we can adopt any of the two methods i.e. non-blind watermarking and blind watermarking. In non-blind watermarking, the original watermark is used to compare with the extracted watermark and the difference is measured. In blind watermarking, the strength of extracted watermark is detected through a correlation measure.

III. APPLICATION AND REQUIREMENT OF WATERMARKING TECHNIQUE

There are three main requirements of the watermarking i.e. transparency, robustness and capacity. Transparency means the percentage of similarity between the original and extracted watermark. Robustness means the detection of watermark after applying some common operations. Broadly attacks are classified into four types: attacks that aim to remove the complete watermark, attacks that try to violate the synchronization of embedder and detector, protocol attacks and last one is cryptography attacks. Capacity means within a unit of time, no. of bit encoded by watermark. This property tells how much data to be encoded so that it can be successfully recovered by the extractor.

There are various applications of watermarking. Some of them are discussed below.

A. Copyright protection

While sharing data over internet, we need a protected way to distribute over information. In this case the watermarking techniques are quite beneficial. In this type of applications the non-blind schemes are appropriate for watermark recovery.

B. Fingerprinting

To detect the true owner of digital content, we can use the concept of fingerprinting. Every user of digital content has its unique identity as fingerprint. A single digital object may consist of many fingerprints as it belongs to many users.
C. Fraud detection

When we use multimedia content for legal purposes, then it is important to protect information from being tampered. If the receiver discovers the change or degradation in watermark then the document cannot be trusted. Fraud detection is important in terms of the security for some applications for e.g. medical records.

D. Id card verification

To verify the identification of a person through id-card, the watermarking technique can be used by embedding the information on the person photo and at the time of identification the hidden information is compared with the detail present on the id-card. Hence it is quite efficient to reveal the true identity of a person. This approach can be used by company to verify its employee, passport authority for the identity of the person, or many more.

IV. COMPARISON OF LSB AND SVD WATERMARKING TECHNIQUE

A. LEAST SIGNIFICANT BIT WATERMARKING

LSB is a spatial domain watermarking technique. In spatial domain watermarking techniques, we have to work directly on the pixels. In least significant bit(LSB) watermarking techniques simple operations used for embedding information in cover image. Following are the steps followed in the traditional LSB watermarking techniques:

1. Convert RGB image to gray scale image.
2. Make double precision for image.
3. Shift most significant bits to low significant bits of watermarked image.
4. Make least significant bits of host image to zero.
5. Add shifted version (step 3) of watermarked image to modified (step 4) host image.

In this algorithm, nearly half of the bit is needed to be modified to embed the secret data or information. The change in the last 4 bit that is least significant produces the small change in intensity which is not detected by human eye.

![Watermarking Process on Image](image)

As you can see in the fig2 image, the difference between the two images is not quiet predictable. They seem similar to the viewer. Lots of research work has been done in this field. Bamatraf et al. [1] purposed, a new LSB watermarking technique that is better than the traditional LSB watermarking algorithm. In this approach, they purposed a model based on LSB watermarking that embed the two watermark bit on the cover image $3^{rd}$ and $4^{th}$ LSB. The result is more robustness than the traditional and the image quality of watermarked image is better than earlier. Sudhir et al [2] purposed a new watermarking algorithm that is the combination of LSB technique and MPFRFT technique. In this approach, two watermarks are used for embedding in one cover image i.e. dual watermarking technique. The parameter involved in MPFRFT is considered as the secret keys. The purposed algorithm produces good result in term of robustness and imperceptibility. Alam et al. [3] purposed a new approach
focused on the increment of the amount of data that we can embed in cover image. They propose two approaches both of them increment the watermark size i.e. 3×3-2 approach gives 33% of size increment and 4×4-4 approach that gives 50% size increment with some limitation. Chopra et al. [4] present the implementation of invisible LSB watermarking and visible LSB watermarking technique. The effect of various attack has been shown too.

B. SVD WATERMARKING TECHNIQUE

SVD is a numerical method used to diagonalizable matrices in numerical analysis. It is an algorithm developed for a variety of applications. The main properties of SVD from the viewpoint of image processing applications are:

1) The singular values (SVs) of an image have very good stability, that is, when a small perturbation is added to an image, its SVs do not change significantly; and

2) SVs represent intrinsic algebraic image properties.

SVD mathematical properties provide an elegant way to extract the feature from the digital data i.e. image, audio etc. Ruizen Liu et.al [5] proposed a novel watermarking algorithm based on SVD. The purpose of this technique is to provide solution to the problem of copyright protection of multimedia documents. In the proposed method, he used the property of SVD to hide the watermark. The Singular values have good stability and it represents image properties in terms of intrinsic algebraic. They explained watermarking casting and detection scheme based on SVD. The proposed method provides good result in terms of security and robustness. Ghazy et.al [6] proposed the improved SVD watermarking based on block based methods. In proposed method, the watermark embedding is done in SVs of each block separately. This technique makes watermark more robust to attacks. Watermark detection is done by extracting the watermark from SVs of the watermarked blocks. The proposed methodology results in fidelity and robustness in resistance to JPEG compression, Gaussian noise and cropping. Wang et al [7] proposed a new watermarking technique based on DCT, DWT and SVD. The proposed algorithm is compare with SVD and DCT+SVD. They proposed non-blind watermarking technique and make improvement by Arnold transformation to watermarked image. The results are better than both algorithm used for comparison. It provided stronger robustness and faster speed in watermarking and recovering. Zhu et al [8] proposed the improved watermarking algorithm on traditional W-SVD algorithm. The W-SVD is DWT based classic wavelet-based watermarking approach.

V. EXPERIMENTAL RESULT

TABLE 1: CALCULATION B/W ORIGINAL AND WATER MARKED IMAGE

<table>
<thead>
<tr>
<th>IMAGE</th>
<th>SVD-WATERMARKING</th>
<th>LSB-WATERMARKING</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>PSNR</td>
<td>MSE</td>
</tr>
<tr>
<td>TUSKUBA IMAGE</td>
<td>44.4398</td>
<td>2.3578</td>
</tr>
<tr>
<td>AERIAL IMAGE</td>
<td>44.2564</td>
<td>2.5394</td>
</tr>
</tbody>
</table>

To compare both the algorithm, we have taken two image of different size. First is Tuskuba image of size (384 X 288) and second is Aerial image of size (450 X 650). The result in case of LSB watermarking is better than that of SVD watermarking technique. The SVD watermarking is comparatively robust than LSB watermarking.

VI. CONCLUSION

This paper introduces SVD and LSB algorithm in watermarking. These two are the popular watermarking algorithm. In this paper, comparison of these two algorithms is shown with various measuring parameters. These comparison table shows that the both algorithm have their own advantage. Using SVD however a better option.
REFERENCES


