Review of different parameters for Digital Reversible Watermarking

Geeta Sharma
Associate Professor
Jagannath Institute of Management Sciences,
JIMS, Rohini, Delhi

Prof.Dr. Vinay Kumar
Ph.D. (Comp. Sc.) MCA, M.Sc(Maths)
Ex Scientist & Professor,
NIC, GOI

Abstract
Reversible digital watermarking is majorly used for authentication and copyright management. Researches generally revolved around the invisible, robust and less complex algorithm. A watermark that can store more data always prioritized over others. In this paper, Iconsidered the various type of digital watermarking and the type of cover data. A watermarked data can be sent over the open network due to imperceptibility feature. Thus it can attract various attacks and must be robust. I also stated the objective of my research work that will form the base for further research.

Keywords: watermarking, steganography, algorithm, histogram

INTRODUCTION

Steganography is used to hide the secret data in the cover (that can be text, audio, video or images) in such a manner that it is not perceivable to human eye. On the other side, digital watermarking is a process to embed a mark or piece of information to acknowledge the ownership and to avoid unauthorized use of data. According to Wikipedia, *"A digital watermark is a kind of marker covertly embedded in a noise-tolerant signal such as an audio, video or image data".*Digital Watermarking can be broadly classified as follows:

- **Visible/Invisible Watermark:**Watermarks are kept visible to ensure authenticity like impressions on currency note (used as one of the major measure). It can be used to identify the owner of some intellectual work like paintings. A visible watermark can be perceived by human eyes with some or no efforts. The embedding of visible watermark is comparatively easy but it is more prone to external attacks. Whereas an invisible watermark cannot be perceived by human eye. An intruder cannot simply crop it from the image. The watermarked signal is almost similar to the original signal. [8] The quality of the image is not much affected with watermark.

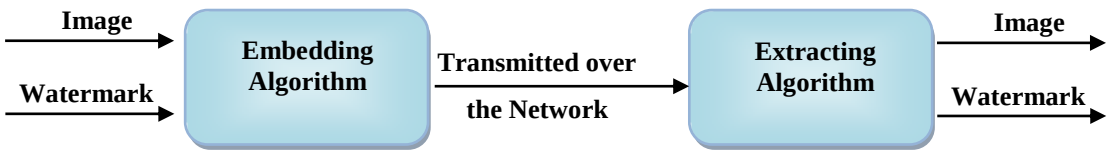
- **Fragile/Semi-Fragile/Robust Watermark:** If a watermark gets destroyed with a small change to the cover, then it is called fragile watermark. On the other hand, a robust watermark is intact of the changes made to the cover. That is, the changes made the quality of the cover image very poor and unauthorized access can be easily identified. A watermark is said to be semi-fragile if the changes exceed the limit (threshold) set by the sender. If the threshold is set to zero, then it operates as a fragile watermark.[8]

- **Public/Private Watermarking:**If a secret key is generated and used for the both the operation embedding and extracting, then it is called private key watermarking. Whereas in public watermarking two keys are generated public and private. Public key is used for the embedding and a receiver can extract the watermark only with private key.

- **Spatial/Transform Domain watermarking:**When some pixel values of the image are modified directly to store the watermark then it is known as spatial watermarking. Transform domain watermarking use some transformation algorithms and do not change the pixel values directly.

- **Type of Cover:**Watermarking is also classified according to the cover or medium that carries the watermark. Some examples are Text watermarking, Image watermarking, Audio watermarking, Video Watermarking etc.

- **Reversible Digital Watermarking:**In digital watermarking, the watermark must be embedded in such a way that the cover image can be extracted without any distortion at the receiver's end. This is known as reversible digital watermarking. Since the digital watermark is meant to protect the original digital content (i.e. image in our case), thus retrieval of original data is also required. One of the major measures to analyze an algorithm is the quality of the original data after the extraction of the watermark. Here, in this paper, we will work on invisible reversible digital watermarking. The digital medium that we chose is image. The process of digital watermarking can be understood well with following steps:



- **Embedding:** Embedding is the process of hiding the watermark in the original image. It takes original message, watermark and a secret key as the input and results in watermarked image.

- **Transmission:** This watermarked image can be used and transmitted over the network. As the watermark is invisible and not perceivable to human eye, less number of attacks is expected.

- **Extraction:** The authenticity of the image can be verified by extracting the watermark from the image. Then it is compared with the original to recognize the attacks.

RELATED WORK

Digital watermarking can be classified in variety of ways, as we have seen in previous section. Our area of concern is Reversible Digital Watermarking. It can be achieved with variety of methods including lossless compression, difference expansion and histogram bin shifting techniques. The first method is using the concept of lossless compression of the images. Celiket. Al. had proposed a method in 2005[1] that used code redundancy. The compressed original image consumed less space and that freed space was further used for hiding the watermarked message. The major disadvantage of this method was very less capacity that is directly dependent on freed space. Also the complexity of computing this space is also very high. Another method consider the difference expansion technique. It was offered by Tian in 2003[2] where two adjacent pixels are compared and the difference is expanded further to hide the message. This process is also known as interpixel redundancy elimination. This method have reduced the computational complexity while capacity is higher than the lossless compression.

Ni et. al. [3] had embedded histogram shifting method in Reversible Digital Watermarking for the first time in 2006. This method produced very effective results, although the computational complexity was reduced drastically. The common feature of the different variants of the basic technique is to take advantage of a pixel value for which there are no corresponding pixels in the image[4]. Generally, in a 8-bit image(grayscale) the values of pixel varies from 0 to 255 where the highest value 255 is not used and known as zero point. The disadvantage of this method is poor capacity. Some researchers had introduced blend of two methods that is difference expansion and histogram bin shifting (HBS) lead to overflow/underflow condition. Kim et al used the 64 modulo addition to avoid the anomaly but still suffered with noise. Luo et al[5] proposed a better solution and pixels at the boundary ie 0 and 255 were not used for hiding the pixel information. This technique is also known as pixel prediction or interpolation.

OBJECTIVE OF RESEARCH

The objective of the study is to provide security while sending the information using steganography. The requirements for a secure communication system are as follows:

- The fact that secret information is being communicated should be concealed and communication should take place in an unremarkable manner.
- The confidentiality of secret information should be ensured, even under the suspicion that secret information is being communicated. It ensures the protection of the interest of investor.
- Steganography helps in establishing authenticity of a piece of information. Watermarks establish ownership of an artifact. Digital watermarking is the technique of adding identifying information to digital artifacts using steganographic principles i.e. hiding the information cleverly so that extraction is difficult by any adversary. Applications of watermarking include copyright protection, data monitoring, and data tracking.
- Generally the cover used in steganography is left unwanted after the retrieval of the hidden message. Here, complexity of the problem lies in the fact that cover must be in usable condition after the execution of extraction algorithm. Watermarking helps in identification of the origin of object. The cover must be available for editing, copying, compression etc.
- Intellectual Property Right (IPR): Area where such work is required to protect IPR of digital data. Here, Intellectual property (IP) refers to creations of the mind, such as inventions; literary and artistic works; designs; and symbols, names and images used in commerce. IP is protected in law by, for example, patents, copyright and trademarks, which enable people to earn recognition or financial benefit from what they invent or create. By striking the right balance between the interests of innovators and the wider public interest, the IP system aims to foster an environment in which creativity and innovation can flourish [6].

PARAMETERS

A digital watermark is based on three quality measures: robustness, imperceptibility, and capacity. When optimize on quality criteria of the information hiding, one need to compromise on other. So, balance need to be maintained, while implementing an algorithm. These are the pillars of any information hiding algorithm and need to be understood in detail.

2.1. Robustness

A digital watermark is called *robust* with respect to transformations if the embedded information may be detected reliably from the marked signal, even if degraded by any number of transformations. Typical image degradations are JPEG compression, rotation, cropping, additive noise, and quantization. For video content, temporal modifications and MPEG compression often are added to this list [7]. If a digital watermark resists a chosen class of transformations then it is called robust. These watermarks are used for protecting the copyright applications and no access control information.

2.2. Imperceptibility

A digital watermark is called imperceptible if the watermarked content is perceptually equivalent to the original, not watermarked. A digital watermark that is perceptual, on the other hand, is imperceptible. It works context-sensitive/adaptive [7]. Generally, creation of robust and imperceptible watermark is considered quite challenging. There are various tests to measure like:

a.) **MSE:** Mean Squared Error is used to check the similarity between two images. According to Wikipedia, this difference is then squared. Here Y_i is the pixel position in original image and Y_i is the pixel value at same position in watermarked image. Then the difference is squared to compute the MSE value.

$$\mathrm{MSE} = \frac{1}{n}\sum_{i=1}^{n}(Y_i - \hat{Y}_i)^2$$

b.) **PSNR:** Peek Signal to Noise Ratio is used to check and compute the strength of the signal. Following is the fuction to compute PSNR:

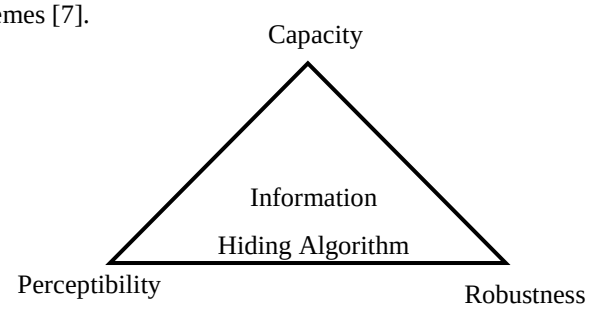
$$PSNR = 10.\log_{10}\left(\frac{MAX_I^2}{MSE}\right)$$

2.3. Capacity

The length of the embedded message determines two different main classes of digital watermarking schemes:

1. The message is conceptually zero-bit long and the system is designed in order to detect the presence or the absence of the watermark in the marked object. This kind of watermarking scheme is usually referred to as *zero-bit* or *presence watermarking schemes*. Sometimes, this type of watermarking scheme is called 1-bit watermark, because a 1 denotes the presence (and a 0 the absence) of a watermark [7].

2. The message is an n-bit-long stream $(m = m_1 \ldots m_n,\ n \in \mathbb{N}$, with $n = |m|)$ or $M = \{0,1\}^n$ and is modulated in the watermark. These kinds of schemes usually are referred to as multiple-bit watermarking or non-zero-bit watermarking schemes [7].



CHALLENGES

1. **Retrieval:** In reversible watermarking, the cover data need to be restored in the form it was sent. The cover is useful and bit by bit it must be same as the original data. Location map is used identify the difference between the original image and the image after embedding the watermark. The major challenge is to improve the watermark embedding capacity.
2. **Reduced FRR:** In reversible watermarking the cover image need to be recovered at receiver's end. The hash is thus matched with cover image and if there is any ambiguity, the cover get rejected summarily. Even a single bit mismatch can cause this rejection. So it is a challenge to reduce the False Rejection Rate. The solution can be the local tamporization, rejection of tampered area only and/or retransmission of tampered image only.
3. **Overhead Data:** The information required for data retrieval and authentication, often add an overhead to the cover image eg. thresholds, location map, pixel frequency histogram's information etc.
4. **Embedding Capacity:** Capacity of any cover image is dependent on the technique used for the information hiding. Thus it is a challenge to select an algorithm that is less complex and can store more data.

CONCLUSION

This paper highlight the various aspects of the information hiding including the basic concept of digital watermarking, classification of the digital watermarking, various parameters and objective of the research. The literature review revolved around the reversible digital watermarking, and more specifically the histogram shifting variations of reversible digital watermarking. This lead to the further implementation of the novel algorithm based on the histogram shifting algorithm.

REFERENCES

[1] M.U. Celik, G. Sharma, A.M. Tekalp and E. Saber, “Lossless generalized-LSB data embedding”, IEEE Transactions on Image Processing, 2005

[2] J. Tian, “Reversible data embedding using a difference expansion”, IEEE Transactions on Circuits Systems and Video Technology, 2003

[3] Z. Ni, Y.Q. Shi, N. Ansari and W. Su, “Reversible data hiding”, IEEE Transactions on Circuits and Systems for Video Technology, 2006

[4] P. Nagarju, R. Naskar and R. S. Chakraborty, " Improved histogram bin shifting based reversible watermarking", International Conference on Intelligent Systems and Signal Processing, 2013

[5] L. Luo, Z. Chen, M. Chen, X. Zeng and Z. Xiong, “Reversible image watermarking using interpolation technique”, IEEE Transactions on Information Forensics and Security , 2010

[6]”What is Intellectual Property?” World Intellectual Property Organization. 12 February, 2014 <http://www.wipo.int/about-ip/en/>

[7] “Digital Watermarking.” Wikipedia: The Free Encyclopedia. Wikimedia Foundation, Inc. 3rd March, 2014. Web. November, 2013. <http://en.wikipedia.org/wiki/Digital_watermarking>

[8] Bender, W., Gruhi, D., Morimota, N. and Lu, A. (1996), “Techniques for Data Hiding”, IBM Systems Journal, Vol. 35, No. 3 & 4.