SURVEY ON DIGITAL IMAGE WATERMARKING TECHNIQUE USING IMAGE PROCESSING

D.Napoleon
Assistant Professor
Department of Computer Science
Bharathiar University
Coimbatore

R.Saikumar
Research Scholar
Department of Computer Science
Bharathiar University
Coimbatore

M.Sivaranjani
Research Scholar
Department of Computer Science
Bharathiar University
Coimbatore

Abstract—In recent days, there was a security glitches are increased through the transmission of digital data over internet. There is an alternative and best solution in the field of image processing is digital image processing which can be applied for secure transmission of the digital data with the help of images. Digital watermarking can be used to hide the information inside the signal which cannot be accessed by the third party. It can be used for security purpose for securing the information in image. Water marking is the most secured method for encryption and decryption of the information within an image. There are only two methods are used as data embedding into the image and extraction of embedding data from the image. In this paper, there are some new techniques using watermarking in the research field of image processing have been discussed.

Keywords: Watermarking, Digital data, Embedding, Extraction, Image processing.

1. INTRODUCTION

In digital world, it’s very difficult to secure the data of an individual whose data have been transferred through the internet. There are lot of glitches for digital data transmission. Different types of attackers are growing day by day and there are lot of ways to depredating the digital data while transferring it over internet. Digital watermarking is the best technology for providing security to the data validation and copy right protection of the digital data. Watermarking is the method of securing the information by embedding into an images, videos, audios as well as text for security persistence. Water marking is the way of hiding the information of ownership and it can be accessed only by administrator not by third party. The embedded digital data can be accessed only by extracting it from the image with the help of key generation method. Key generation is nothing but the digital data can be embedded into the image with generating the key. The same key can be used for extracting the embedded image. The digital data which can be hidden inside the image cannot accessed without the presence of key. Digital watermarking is the technology which have many applications for protecting the digital data, certificate distribution over the digital media and tag the user information. Hiding an information in an image has become an important area for hiding the information. The proposed work analyse the key generation method of digital image watermarking and explore its applications and uses several methods for security purposes.

2. INITIAL STAGE OF WATERMARKING

There are two basic steps have been used for data watermarking using digital data are as follows:

i. Data Embedding
ii. Data Extraction

The above mentioned two methods are basic steps for hiding the data from glitches in the proposed system. The below figure shows that how the data have been hidden inside the image and how it can be accessed by extracting the hidden digital data.

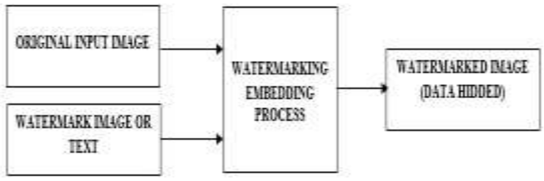

ORIGINAL INPUT IMAGE
WATERMARK IMAGE OR TEXT
WATERMARKING EMBEDDING PROCESS
WATERMARKED IMAGE (DATA HIDDED)

Fig 1. Embedding Process of Watermarking

Fig 1. Says that, the original image have been given along with the watermark image or text which needs to embedded into the original image. And the data can be embedded into the image and the digital data can be hided. It cannot be accessed by any other third parties.

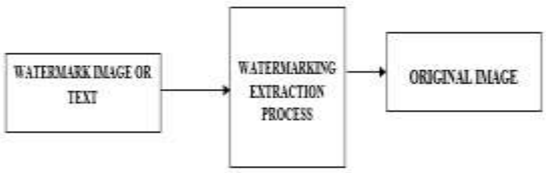


Fig 2. Extracting Process of Watermarking

Fig 2. Says that the process of extracting the hidden digital data from the watermarked image for accessing that data. Only the administrator can be accessed the data which is extracted from the image. The embedding is the process of hiding an information which can be processed from sender's side. A receiver only receive the watermarked image from the sender. The receiver can access that watermarked image only with the help of watermark image or text. It can be also said like key generation method. Without accessing the key the receiver cannot access the image with digital data received from the data. And the key can be known by the sender and receiver only, no other third parties can use or attack our digital information transferred over an internet for communication.

3. REQUIREMENTS OF DIGITAL WATERMARKING

Digital image watermarking concerns to solve some issues properly, thus, this paper highlights the main requirements of watermarked image as following:

i. *Robustness:*

The robustness is the ability of detecting the watermark after some signal processing modification such as spatial filtering, scanning and printing, lossy compression and so.In addition to that, not all the watermarking algorithms have the same level of robustness, some techniques are robust against some manipulation operations they fail against other stronger attacks.

- The robust is nothing but protecting the data of copyright information protection and broadcast monitoring. There are two more steps under the robust technique named as fragile and semi-fragile.
- Where the fragile can be described as the image can be destroyed at any time detection of any illegal accessing of data to be manipulate or to access by the third parties. It can be mostly used under the protection of content authentication.
- The semi-fragile are incidental attack where the fragile are malicious attack. And it can be used for image authentication.

ii. *Imperceptibility:*

- Imperceptibility is the method of verifying the original image with watermarked image for authentication.
- In other words, the watermark image can looks similar to the original image and the watermark is invisible to small degradation in contrast or brightness of an image.
- Besides that, the watermark is not always preferred to be invisible, sometimes, it is preferred to have visible watermark into the image.

iii. *Data payload:*

- Data payload is nothing but the number of bits are embedded into the original image. And it is the highest quality of an information which can be hidden without modifying the quality of an image. The quality of an image can be calculated by the amount of information hidden in the original data. It predict that the how much of data have been embedded into the original image for watermarking, so that they can be effectively detected the extraction process.

iv. *Security:*

- Watermark system is said to be one of the secured method for data transmission, the unauthorized person cannot remove the watermark from the original image without having any general knowledge about watermarking and embedding algorithm.
- Security is the important factor of watermarking system and only the authorized persons can detect the watermark from an image where others can't. The copyright protection can accomplish in the watermarking system.

v. *Computational complexity:*

- The method called Computation complexity is defined as the amount of time taken by the watermarking algorithm for embedding and extraction process of hiding the data into the image.
- More computational difficulty is needed for the strong security and validity of the watermark. On the other hand, real-time applications require both speed and efficiency.

vi. *Inevitability:*

- Inevitability is the method to produce the original data during the extraction of watermark. The optimization of the parameters is mutually competitive and cannot be simply done simultaneously.
- A rational concession is always a requirement. Alternatively, if robustness to strong warp is an issue, the message that can be frequently hidden must not be too long.

vii. Low complexity:

- The cost is the reason behind studying the complexity, so it should be at a reasonable cost. It describes the economics of using watermark embedders and detectors, because it can be very complicated and depends on business model that is used.
- The main two issues of complexity are the speed of embedding and detection, and the number of embedders and detectors.

4. WATERMARKING APPLICATIONS

There are lot of applications in digital water marking system. Only few are listed below,

i. *Copyright Protection:*

- The one of the most important application of watermarking is copyright protection from the unauthorized user.
- Ownership of digital media can be established in the case of a copyright dispute by using the embedded data as a proof.

ii. *Broadcast monitoring:*

- This application is used to monitor unauthorized broadcast station. It can verify whether the content is really broadcasted or not.

iii. *Authentication and Integration verification:*

- The watermark is embedded in the image for detecting if the image has customized or not, this process can be used for verification.
- Integrity verification can be achieved by using fragile or semi fragile watermark which has low robustness to modification in an image.

iv. *Fingerprint:*

- The main purpose of fingerprinting is to protect clients. If someone got a legal copy of a product, but redistributed illegally, fingerprinting can prevent this.
- This can be achieved by tracing the whole transaction by embedding single robust watermark for each receiver.

v. *Medical application:*

- In medical field, watermarking plays an important role for the purpose of protecting the hospital's information from unauthorized persons such as patient's report etc.
- Security and verification of such data are now becoming very significant in medical field where the digital data are easily distributed over the internet.

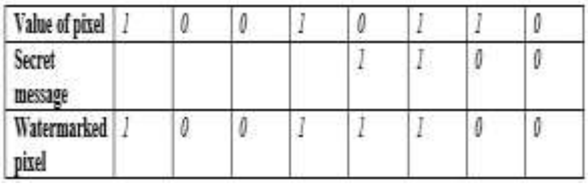
5. DIGITAL IMAGE WATREMARKING TECHNIQUES:

i. *Spatial Domain:*

Spatial domain is the main method for embedding the information directly into an image. And there are lot of techniques and algorithms are used for embedding this type of watermarking as Least Significant Bit (LSB), Intermediate Significant Bit (ISB), patchwork, etc.

A. *Least significant bit (LSB):*

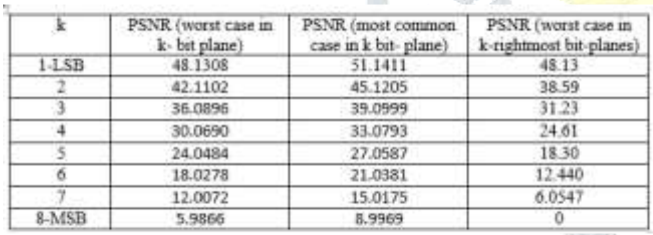
Least significant bit is a simple method for digital image watermarking because the least significant bit carry less information and their effect does not cause visible changes. And it can be used for simple operation to embed an information in the original image. An idea theme behind the LSB is a simple one as, the pixels of original image are changed by no. of bits of secret message. As like, the number of 8byte pixels was embedded into the image. Where the 1 to 4 least bits needed to modify according to embedded secret message. And only half of the bits in an image will need to change for hiding the secret information into the original image. Because the watermarked image quality is very low, it can be less than 4 least significant bit, changing the LSB of a pixels have changes in color change in pixel intensity. This change cannot be recognized by human, where the attacker can easily extract the changed bits due to its simple operation. For example, the below shown figure explains that the 4 bit LSB operation. The pixel value of an image is 150 (10010110) and the secret data is 1100. The secret data need to be watermarked with original image. Now the pixel value have been changed to 156(10011100). LSB method can store the 4-bit value in each pixel of an image with the size of 256 x 256, finally it stores the total amount of 65,536 bits of embedded data into the original image.



Value of pixel	1	0	0	1	0	1	1	0
Secret message					1	1	0	0
Watermarked pixel	1	0	0	1	1	1	0	0

Fig 3. Digital watermarking with 1-bit LSB technique

The worst case in the simple LSB substitution method occurs when the watermark bit and original bit are different all the time. In other words, the difference between the original pixel and watermarked pixel is (2k-1), where k is the level of different bit-planes. The PSNR for the worst case of embedding one bit within k bit-plane and embedding the watermark within krightmost of host image are presented in Table 1, in addition to most common distribution embedding for k bitplane.The first is the worst case by embedding in the k bit-plane only. The second is for embedding the watermark into the k bit-plane, only for the most common case and the third is for embedding the worst case in the krightmost bit-planes. It could be seen that the image quality of the watermarked image had been drastically degraded when k > 4, in case of using one bit-plane only for hosting the watermark. In case of k right-most bit2013 IEEE 9th International Colloquium on Signal Processing and its Applications, 8 - 10 Mac. 2013, Kuala Lumpur, Malaysia 237 planes, the image quality of the watermarked image was drastically degraded when k > 3.



k	PSNR (worst case in k- bit plane)	PSNR (most common case in k bit- plane)	PSNR (worst case in k-rightmost bit-planes)
1-LSB	48.1308	51.1411	48.13
2	42.1102	45.1205	38.59
3	36.0896	39.0999	31.23
4	30.0690	33.0793	24.61
5	24.0484	27.0587	18.30
6	18.0278	21.0381	12.440
7	12.0072	15.0175	6.0547
8-MSB	5.9866	8.9969	0

Table 1. PSNR values of worst embedding case and the most common one for different bit planes using LSB method.

B. Intermediate significant Bit (ISB):

The embedding watermark, within LSB gives the best image quality, embedding within the Most Significant Bit MSB gives the worst image quality. When starting from the MSB towards the LSB, embedding will improve the quality of watermarked image.Improved LSB to a new technique called intermediate significant bit (ISB). In the new method, the watermark pixel's location has been tested according to the range of each bit-plane.If the pixel value is located at the edges of the ranges, any small change caused by attacks will move the pixel from a range to other range, and the watermark cannot be extracted.

The below figure shows that, the original image can be used for visible water marking that shows the watermarked content to be visible for the viewers. The lenaimage have been taken from the Matlab source image and the logo of some institute have chosen as a watermarked information. The watermarked image can be fetched with original image and the data can be visible to the viewers. From the below figured image, the first image shows the original image and the second shows the logo which can be embedded into the source image and the third shows the logo can be embedded into the source image which is visible for the users and the final image shows only the original image and the logo have been disappeared. It's because of the information hidden inside the data which cannot visible to the viewer as well as there is less possible for attackers in stealing the digital data. The data which can be embedded into the original image it can be accessed only by the authenticated user with the knowledge of decoding the encrypted information.

The watermarking not only applied to the image also to the video, text, audio, graphics and so. The information to be hide in the video can need the real time extraction and robustness for the problems. In the audio the watermarked are done in tunes and mp3 also. The text plays a very good role for watermarking which can be done between the space between the characters and the in the text the information can be embedded. The graphics watermarking to the 2D or 3D file for mentioning the copyrights.

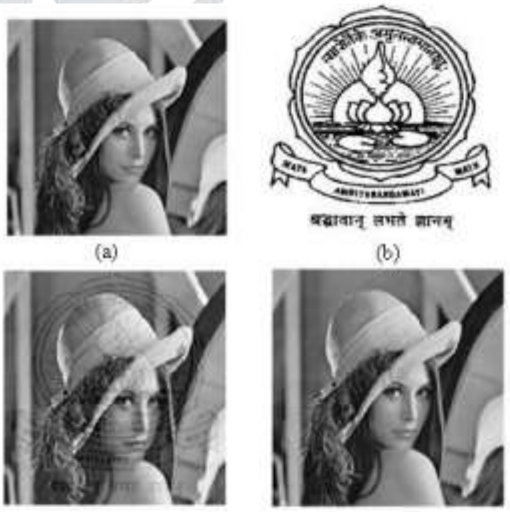


Fig 4. (a) Original Lena image (b) Logo to be watermarked (c) Visible watermarked image and (d) Invisible watermarked image

6. CONCLUSION

In this survey paper, we provided a recent research in the watermarking field. We have offered various characteristics for digital watermarking like basic of watermarking, techniques, applications about watermarking system. Copying photos from the Internet is just a matter of right clicking on a photo and saving it on the computer hence the security and authenticity of the image or data are cracks. The watermark is required to prevent the original images and other documents over the internet.

REFERENCES

[1] M. L. M. Ingemar J. Cox, Jeffrey A. Bloom, Jessica Fridrich, and Ton Kalker, Digital Watermarking and Steganography: Morgan Kaufmann Publishers, 2008.

[2] Y. Yusof and O. O. Khalifa, "Digital watermarking for digital images using wavelet transform," in Telecommunications and Malaysia International Conference on Communications, 2007. ICT-MICC 2007. IEEE International Conference on, 2007, pp. 665-669. V1 H1 H2 V2 H3 V3 D3 D2 D1 64 32 64 16 2013 IEEE 9th International Colloquium on Signal Processing and its Applications, 8 - 10 Mac. 2013, Kuala Lumpur, Malaysia 239

[3] Z. Yanqun, "Digital Watermarking Technology: A Review," in Future Computer and Communication, 2009. FCC '09. International Conference on, 2009, pp. 250-252.

[4] R. F. Olanrewaju, "Development of Intelligent Digital Watermarking via Safe Region," PHD, Electrical and Computer Engineering, International Islamic University Malaysia, Kulliyyah of Engineering, 2011.

[5] J.-S. Pan, H.-C. Huang, and l. C. Jain, Eds., Intelligent Watermarking Techniques (Series on Innovative Intelligence. World Scientific, 2004, Pages.

[6] L. Jian and H. Xiangjian, "A Review Study on Digital Watermarking," in Information and Communication Technologies, 2005. ICICT 2005. First International Conference on, 2005, pp. 337-341.

[7] N. Cvejic, "Algorithms for Audio Watermarking and Steganography," Department of Electrical and Information Engineering, University of Oulu, 2004.

[8] A. G. Charles Fung, Walter Godoy Junior, "A Review Study on Image Digital Watermarking," presented at the The Tenth International Conference on Networks, St. Maarten, The Netherlands Antilles, 2011.

[9] S. Jun and M. S. Alam, "Fragility and Robustness of BinaryPhase-Only-Filter-Based Fragile/Semifragile Digital Image Watermarking," Instrumentation and Measurement, IEEE Transactions on, vol. 57, pp. 595-606, 2008.

[10] C. De Vleeschouwer, J. F. Delaigle, and B. Macq, "Invisibility and application functionalities in perceptual watermarking an overview," Proceedings of the IEEE, vol. 90, pp. 64-77, 2002.

[11] Xia, X.G., C. Boncelet, and G. Arce, 1998. Wavelet transform based watermark for digital images. In the International Online Journal of Optics.

[12] Santa Agreste, Guido Andaloro, Daniela Prestipino, LuigiaPuccio, 2007. An image adaptive, wavelet-based watermarking of digital images. In Elsevier Journal of Computational and Applied Mathematics.

[13] M. L. M. Ingemar J. Cox, Jeffrey A. Bloom, Jessica Fridrich, and. Ton Kalker, 2008. Digital Watermarking and Steganography: Morgan. In Kaufmann Publishers.

[14] Jeng-Shyang Pan, Hsiang-Cheh Huang, Lakhmi C. Jain, and Wai-Chi Fang, 2004.Intelligent Multimedia Data Hiding. In Springer.

[15] Jain Liu, and Xiangjain, 2005. A review study on Digital Watermarking. In International Conference on Information and Communication Technologies.