Available Online at www.ijcsmc.com

International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

ISSN 2320–088X

IJCSMC, Vol. 4, Issue. 6, June 2015, pg.632 – 636

REVIEW ARTICLE

A Review on Watermarking & Image Encoding

Narinder Singh, Deepak Sharma

Department of Computer Science and Engineering, Guru Kashi University Talwandi Sabo, Bathinda(pb)

narindersidhu11@gmail.com

Abstract: ***Today, exchange of information is been held electronically. Digital data can be stored efficiently with a very high quality and it can be manipulated very easily using computers. Digital media offer several distinct advantages over analog media. Therefore, we have great need of secure transmission of the concerned data. Watermarking is used as a key solution to make the data transferring secure from illegal interferences. A watermark is a secondary image, which is overlaid on the host image, and provides a means of protecting the image. Watermark techniques are used in various areas such as copyright protection, broadcast monitoring and owner identification. Continuous efforts are being made to device an efficient watermarking scheme and this paper conducts a literature survey of watermarking. It describes the early work carried out on digital watermarks, including the brief analysis of various watermarking schemes and its potential applications.***

Keywords: " Watermarking techniques, watermarking attributes, applications, image compression, RLE, LZW, HUFFMAN, Transformation, Fractal coding"

1. INTRODUCTION

In multimedia, everyday tons of data is embedded on digital media or distributed over the internet. This data, which include still images, video, audio, or text are stored and transmitted in a digital format can be easily copied without loss of quality and efficiently distributed. Thus the protection of intellectual property rights has become increasingly important. Information stored in digital format because of ease of reproduction, retransmission and even manipulation allows a pirate either to remove a watermark and violate a copyright or to cast the same watermark after altering the data to forge the proof of authenticity. Publishers, artists, and photographers, however, may be unwilling to distribute pictures over the Internet due to a lack of security, images can be easily duplicated and distributed without the owner's consent. Watermarking have been proposed as a way to tackle this tough issue. Watermark is a code that is embedded inside an image. Watermarking however adds the additional requirement of robustness. Now digital image watermarking is increasing attention due to the fast developing in the internet traffic. It is inserted invisible in host image so that it can be extracted at later times for the evidence of rightful ownership [1]. The main purpose of watermarking is to embed information imperceptibly and robustly in the host data. Typically the watermark contains information about the origin, ownership, destination, copy control, transaction etc[2].

2. CLASSIFICATION OF WATERMARKING TECHNIQUES

a) *Visible Watermarks:* Visible watermarks are those watermarks which can be easily perceived by the viewer, and clearly identify the owner. The visible watermarks are viewable to the normal eye such as bills, company logos and television channel logos etc. Such watermarks cannot be removed by cropping the center part of the image[3]

b) Invisible watermark: Invisible watermark is hidden in the content. It can be detected by an authorized agency only. While the obviousness of visible watermarking makes distinguishing legitimate and illegitimate versions easy, its conspicuousness makes it less suitable for all applications. [3]Such watermarks are used for content and author authentication and for detecting unauthorized copier.

c) *Fragile watermarks:* Fragile watermark are also known as tamper-proof watermarks. Such watermark are destroyed by data manipulation or in other words it is a watermarks designed to be destroyed by any form of copying or encoding other than a bit-for-bit digital copy. [4]They lose their mettle when they are subject even to the smallest changes.

3. ATTRIBUTES OF WATERMARKING

a) *Transparency:* The watermark that is been embedded should not degrade the original image quality. And in rare case if any distortions are visible in the image it tends to degrade the commercial value of the image. [5]

b) *Robustness:* Robustness is the ability to detect the embedded watermark after common image processing operations like compression, filtering, geometric distortion etc. Robustness is application dependent and it is not necessary that all the applications require robustness against all the operations. For example, in broadcast monitoring the robustness is required only against the communication related manipulations. In fragile watermarking, robustness is undesirable.

c) *Capacity or Data Load:* This quantity describes the maximum amount of data that can be embedded into the image to ensure correct removal of watermark during extraction. The number of bits, a watermarking scheme encodes within a cover work is referred to as data payload and is application dependent. For *N* bits watermark, the system can encode any of *2N* different messages. Increasing the watermark payload will affect the fidelity of the system and vice versa. [5]Thus, it is very important for the researchers to make trade-off between contradicting properties of the watermarking while developing the watermarking systems.

d) *Computational Complexity* :Computational complexity indicates the amount of time watermarking algorithm takes to encode and decode. To ensure security and validity of watermark, more computational complexity is needed. [6]Conversely, real-time applications necessitate both speed and efficiency.

4. WATERMARKING APPROACHES

Various watermarking system can be classified into two main domains i.e. Spatial domain techniques and Frequency domain techniques.

a) Spatial Domain Techniques: In this technique, the watermark is inserted in the cover image changing pixels or image characteristics. Some common spatial-domain algorithms include Least Significant Bit (LSB) Modification, Patchwork, Texture Block Coding, etc. The most serious drawback of spatial-domain technologies is that it tends to provides limited robustness. It is complex for spatial-domain watermarks to subsist under attacks such as lossy compression and low-pass filtering.[7] Also the amount of information that can be embedded in spatial domain is also very limited. The algorithm should carefully weight the number of changed bits in the pixels against the possibility of the watermark becoming visible.

b) *Frequency-Domain Technologies :*In comparison to spatial-domain watermark, watermarks in frequency domain are more robust and much more compatible to popular image compression standards. Thus, frequency-domain methods are more widely applied. To embed a watermark, a frequency transformation needs to be applied to the host data. [8]Then, modifications are made to the transform coefficients. Possible frequency image transformations include the Discrete Fourier Transform (DFT), Discrete Cosine Transform (DCT) and others. In recent years they are becoming generally desolated.

5. APPLICATION OF WATERMARKING

a) ***Copyright Protection****:* Watermarking is essentially applied for copyright protection. The aim is to evade other parties from claiming the copyright by embedding the information that identifies the copyright owner of the digital media. The application must make certain that embedded watermark cannot be eliminated without causing a noteworthy deformation in digital media though maintaining a high level of robustness. [9]When a new work is produced, copyright information can be inserted as a watermark.

b) ***Authentication:*** In some cases we have need to identify the ownership of the contents. All this can be done by embedding a watermark and providing the owner with a private key that gives him an access to the message. ID cards, ATM cards, credit cards are all examples of documents that require authentication. In an image authentication application the intent is to detect modifications to the data. The characteristics of the image, such as its edges, are

inserted and compared with the current images for differences. [9]If any part of the content is modified, its summery, the signature, will change making it possible to detect that some kind of tampering has taken place.

c) ***Publication Monitoring and Copy Control:*** The watermark contains owner data and specifies the corresponding amount of copies allowed. This presupposes hardware and software able to update the watermark at every use .[10] It also allows copy tracking of unauthorized distribution since owner data is recorded in the watermark.

d) *Convert Communication:* The embedded signal is employed in the transmission of secret information from one person (or computer) to another, devoid of anyone along the way becoming aware that this information is being transmitted. It includes exchange of messages secretly inserted within images.

e) *Digital Fingerprinting:* This is a process that is been used for detecting the owner of the content. This is so because every fingerprint is the unique characteristics of the owner.

f) *Medical Application:* Name of the patients can be printed on the X-ray reports and MRI scans using techniques of visible watermarking. The medical reports play a very important role in the treatment offered to the patient. [11]If there is a mix up in the reports of two patients this could lead to disaster.

6. IMAGE COMPRESSION

Image compression is an application of data compression that encodes the original image with few bits. The objective is condense the number of bits obligatory to digitally symbolize an image while maintaining its apparent visual excellence. Image compression is a procedure that is very vastly used for the integral and resourceful convey of data. It not only reduces the dimension of realistic file to be transferred but at the equivalent time reduces the storage space requirements, cost of the data transferred, and the time required for the transfer.

A common characteristic of most images is that the neighbouring pixels are correlated and therefore contain redundant information. The foremost task then is to find less correlated representation of the image. Two fundamental components of compression are redundancy and irrelevancy reduction. Redundancies reduction aims at removing duplication from the signal source[12].Irrelevancy reduction omits parts of the signal that will not be noticed by the signal receiver, namely the Human Visual System. In an image, which consists of a sequence of images there are three types of redundancies in order to Compress file size. They are:

a. *Coding redundancy:* Fewer bits to represent frequently occurring symbols.

b. *Interpixel redundancy:* Neighbouring pixels have almost same value.

c. *Psycho visual redundancy:* Human visual system cannot simultaneously distinguish all colors.

Types Of Compression

Compression can be divided into two categories, as Lossless and Lossy compression. In lossless compression, the reconstructed image after compression is numerically identical to the original image . In lossy compression scheme, the reconstructed image contains degradation relative to the original. Lossy technique causes image quality degradation in each compression or decompression step. [12]The following are the some of the lossless and lossy data compression techniques:

- Lossless coding techniques

1. Run length encoding
2. Huffman encoding
3. LZW coding
4. Area coding

- Lossy coding techniques

1. Transformation coding
2. Fractal coding
3. Block Truncation Coding

Run Length Encoding: Run-length encoding (RLE) is a very simple form of data compression in which runs of data (that is, sequences in which the same data value occurs in many consecutive data elements) are stored as a single data value and count, rather than as the original run. This is most useful on data that contains many such runs: for example, simple graphic images such as icons, line drawings, and animations. It is not useful with files that don't have many runs as it could greatly increase the file size[13].Run-length encoding performs lossless data compression and is well suited to palette-based bitmapped images such as computer icons. RLE can compress any type of data regardless of its information content, but the content of data to be compressed affects the compression ratio. Consider a character run of 15 'P' characters which normally would require 15 bytes to store : PPPPPPPPPPPPPPP is stored as 15P .With RLE, this would only require two bytes to store, the count (15) is stored as the first byte and the symbol (P) as the second byte.

Huffman encoding: A more sophisticated and efficient lossless compression technique is known as "Huffman coding", in which the characters in a data file are converted to a binary code, where the most common characters in the file have the shortest binary codes, and the least common have the longest.[14]To see how Huffman coding works, assume that a text file is to be compressed, and that the characters in the file have the following frequencies: The first step in building a Huffman code is to order the characters from highest to lowest frequency As long as bits constitute legitimate Huffman codes, and a bit doesn't get scrambled or lost, the decoder will never lost.

LZW coding: LZW is a statistics solidity method that takes benefit of duplication. The innovative description of the method was created by Lempel and Ziv in 1978 (LZ78).[15]It is dynamic compression method, the inspiration is to first start with an original model, secondly read statistics portion by portion and lastly revise the model and encode the statistics as one go along. LZW is a "phrase book"-based compression algorithm, this means that instead of tabularizing temperament counts and building trees, as done in case of Huffman encoding.Thus, to encode a substring, only a single code number, analogous to that substring's catalog in the phrase book ,needs to be printed to the output file. A large English text file can typically be compressed via LZW to about half its original size.

Area coding: In area coding procedure unique codeword's are used to categorize huge areas of adjacent 1's or 0's. In this method the entire image is alienated into blocks of size m*n pixels, which are confidential as block having only white pixels, chunk having only black pixels or chunk with varied intensity. The most recurrent happening grouping is then assigned the 1-bit codeword 0, and the remaining other two categories are assigned with 2-bit codes 10 and 11. The code assign to the assorted concentration grouping is used as a prefix, which is followed by the mn-bit pattern of the chunk. When principally white text credentials are being compressed, a vaguely simpler approach called white block skipping is mature to cipher the solid white areas as 0 and all other blocks including the concrete black blocks are coded as 1 followed by the bit blueprint of the block. This approach takes improvement of the projected structural patterns of the image to be compress.

Lossy coding techniques

Transformation coding: Transform field coding is been used to transform the pixels in the inventive image into regularity field coefficients called convert coefficients. These coefficients have numerous pleasing properties.[14]Transform coding techniques uses a reversible, linear mathematical alter to plot the pixel values onto a position of coefficients, which are then quantized and encoded. The key aspect following the success of transform-based coding schemes depends on many of the consequential coefficients for most expected images which have small magnitudes and can be quantized without causing significant deformation in the decoded image.

Fractal Image Coding: Fractal compression is a lossy compression method for digital images, based on fractals. The method is best suited for textures and natural images, relying on the fact that parts of an image often resemble other parts of the same image. Fractal algorithms convert these parts into mathematical data called "fractal codes" which are used to recreate the encoded image. Fractal image compression techniques work by attempting to look for possible self-similarities within the image. [16]If aspects of the image can be self-predicted the entire image can be generated using a few image seed sections with appropriate transformations to create other areas of the image.

Block truncation coding : Block truncation coding (BTC) is a straightforward and swift lossy compression technique planned for digitized gray scale images. It was initially introduced by Delp and Mitchell. The solution behind BTC is to execute instant preserving (MP) quantization for blocks of pixels so that the superiority of the image will continue adequate and at the same time the storage space stipulate also remains decreased.

CONCLUSION

Watermarking is a rapidly growing area of research and development. The problem which we face today is the development of truly robust, transparent and secure watermarking technique for different digital media including images, video and audio. It is concluded that watermarking technique is very impressive for image authentication and for protection against attacks. Watermarking defines methods and technologies that hide information. In this paper we are briefly defining the concepts of watermarking as well as an application of watermarking and compression is discussed. In this image has been watermarked along compression algorithm that is based on encoding. And finally watermarking combined with image compression is been presented to enhance the level of security for the data to be transmitted. The experiment proves that compressed image watermarking can well withstand a variety of image processing and other attacks. It is concluded that, we have developed a general compressed image-watermarking framework, by jointly considering watermarking and compression reduces the system's complexity. The amount of compression achieved depends upon the characteristics of the source to a great extent. So the resultant images will not much blurred or not lost their information after compression.

REFERENCES

[1] F. Hartung and M. Kutter,Stefan Katzenbeisser and FabienA. P. Petitcolas, editors, Information Hiding Techniques for Steganography and Digital watermarking ,Artech House, 2000 .

[2] Juergen Seitz, Digital Watermarking for Digital Media,Information Science Publishing, 2005.

[3] D. Kundur, D. Hatzinakos, Digital Watermarking for Telltale Tamper Proofing and Authentication, in proceeding of the IEEE, (1999),pp. 1167-1180.
[4] M. El-Gayyar and J. von zur Gathen, "Watermarking techniques spatial domain", University of Bonn Germany, Tech. Rep., 2006.
[5] M. Arnold, M. Schmucker, and S. D. Wolthusen, Techniques and Applications of Digital Watermark and Content Protection, Artech House, 2003.
[6] J.Liu and X.He, "A review study on digital watermarking", 1st International Conference on Information and Communication Technologies, pp. 337-341, 2005.
[7] Edin Muharemagic and Borko Furht "A survey of watermarking techniques and applications" 2001.
[8] J. Fridrich, "Image watermaking for tamper detection", in Proc. IEEE International Conference Image Processing, Chicago, IL, Oct. 1998, pp. 404-408.
[9] Edin Muharemagic and Borko Furht "Survey of watermarking Techniques and Applications".
[10] Katzenbeisser S. and Petitcolas F.A.P., "Information Hiding Techniques for Steganography and Digital Watermarking", Aetech House, UK, 2000.
[11] B. Chen and G.W. Wornell. Achievable performance of digital watermarking systems. IEEE International Conference on Multimedia Computing and Systems, 1:13–18, 1999.
[12] Vartika Singh "A Brief Introduction on Image Compression Techniques and Standards" International Journal of Technology and Research Advances Volume of 2013 issue II.
[13] www.ehow.comInterne
[14] www.wisegeek.com/what-islosslesscompression.html
[15] www.pcmag.com/encyclopedia/term/46335/lossy-compression
[16] searchciomidmarket.techtarget.com/definition/image-compression
[17] www.rimtengg.com/coit2007/proceedings/pdfs/43.pdf "A STUDY OF VARIOUS IMAGE COMPRESSION TECHNIQUES

