Neural, Parallel, and Scientific Computations 18 (2010) 357--364

SIMULATING CONVOLUTED DIGITAL WATERMARKING HIDDEN MESSAGE ALGORITHMS USING QUANTIZED INDEX MODULATED BEZIER AND HERMITE SPLINES

ROBERT S. OWOR, KHALIL F. DAJANI, AND ZEPHYRINUS OKONKWO
Department of Math and Computer Science, Albany State University, Albany GA 31705

ABSTRACT: This paper briefly surveys the landscape of digital watermarking. Our goal is to understand the general principles that could lead to successful watermarking methods. Whereas cryptography is a relatively mature area of information security, serious study of digital watermarking began only recently, and much is yet unknown. Digital Piracy poses an unprecedented array of threats, ranging from intellectual property violations; to military, industrial and economic espionage; to outright despicable theft of works available in digital format.

Digital watermarking while nascent is a promising technology that offers protection of unencrypted or decrypted digital content. The three main technical challenges faced by watermarking algorithms are fidelity, robustness and security. Current watermarking methods while offering acceptable fidelity and robustness against certain types of processing, fail to overcome data compression and noise addition challenges. Further difficulties are encountered when robust geometric transformations such as scaling, rotation and cropping of still and moving images takes place. Theoretical approaches have been developed that could lead to secure watermarking methods, but substantial gaps remain between theory and practice. The merging of computation and communication, as embodied in the myriad of digital devices and communications systems present substantial new challenges and opportunities for the processing and distribution of valuable digital creations such as audio tracks, still images, and movies for commercial, military and educational purposes. At the same time, new technology has opened the Pandora's Box of cheap, easy copying and distribution of pirated material. A standard and well-understood technical approach to reducing piracy is to use cryptography, where, only authorized users have the decryption keys. Cryptography is useful so long as the authorized user has no intention of making free copies of protected material and distributing them to friends or relatives. A complementary approach that offers protection of unencrypted material is digital watermarking to effectively limit illegal copying and distribution.

We conclude the paper by presenting a digital water marking algorithm based on Quantized Index Modulated Convoluted Bezier and Hermite Splines. Using this technique, vital data can be hidden and transmitted using random phase carrier techniques. The theory behind this method is reviewed and shown to hide both pictorial and non-pictorial data with fidelity, robustness and security. The details of the procedures used for design, possible optimization, message extraction, optimization, synchronization, rotation and scaling are also discussed. Simulation and experimental evaluation of the model will be the next step in the research.

1. INTRODUCTION

An increasing number of cases involving fake currency, phishing scams, illegal copying of digital content and accelerated attacks on electronic systems such as credit cards have renewed and revamped interest in digital water marking technology. Traditionally, a watermark was a form,

Received April 25, 2010

image or text that was impressed onto paper, to provide evidence of its authenticity. Digital watermarking is an extension of this concept into the electronic arena. The phenomenal growth of the Internet has highlighted the need for mechanisms to protect, access, own, authenticate, copy and distribute digital media. Identical copies of digital information in image, text or audio/video format can be produced and distributed easily. Digital watermarks are pieces of information added to digital data (text, audio, video, or still images) that can be detected or extracted later to make an assertion about the data. Watermarks may be visible or invisible, in either case their use is two-fold: first, to discourage unauthorized usage, and second, to act as an authenticator of genuineness. Watermarks may also be classified as robust or fragile. Robust watermarks are those which are difficult or impossible to remove from the object in which they are embedded. Fragile watermarks are those that are easily removed by simple extraction algorithms. For a digital watermark to be effective, it must be robust, recoverable, original, reliable, non-intrusive authoritatively removable and un-authoritatively intractably un-removable. Three main processes occur in watermarking namely: insertion of a watermark, detection of a watermark, and extraction of a watermark. Extracting the watermark can be divided into two phases, locating the watermark, and recovering the watermark information. Watermark extraction may be done with or without the original document. Detection involves the extraction and comparison of the watermark with the original, to determine authenticity. Two main techniques are currently used in digital watermarking namely spatial and frequency based embedding of bit patterns.

1.1 Spatial based Watermarking

Spatial bit embedding involves the selection of the pixels to be modified based on their location within the data. Spatial bit embedding is very susceptible to cropping and other mosaic attacks. One such susceptible algorithm is the Least Significant Bit (LSB) Algorithm. A modification of this method uses a secret key to choose a random set of bits, and replaces them with the watermark. The watermark is invisible, as changes are made to the LSB only; still it is not robust. Image manipulations, such as re-sampling, rotation, format conversions and cropping, invalidate the hidden watermark in many cases.

In another technique, the pixels are divided into 2 equal sets X and Y randomly by a secret key. A small integer d is added to the intensity of each pixel in set X, and subtracted from each pixel in set Y. If the integer d is small, the changes made by the additions and subtractions are visibly imperceptible. To detect if the image is watermarked, a simple calculation of the average intensities of the two areas is done. If the two values differ by a value of 2d, the image is watermarked. If they differ by 0, the image is not watermarked.

Yet another technique uses superimposition of bits to create a watermark. A watermark symbol is selected and either scaled and/or the canvas enlarged; so that the two images i.e. the watermark and the original image, have the same dimensions. The two images are then added together as follows. For each pixel making up the watermark symbol, a fixed intensity is added to the corresponding pixel in the original image. The resulting watermark may be visible or invisible, depending on the intensity chosen. Superimposition is robust in the face of most common geometric transformations but may be defeated by rotation operations. Furthermore, the simplicity of this technique is no match for the processor power available today to manipulate, text, audio, video and graphics formats.

1.2 Frequency based Watermarking

Watermarking in the frequency domain involves the selection of the pixels to be modified based on the frequency of occurrence of that particular pixel. The purpose of this approach is to convolute the susceptibility to cropping algorithms. Common transforms, such as Fast Fourier Transforms, alter the value of pixels within the original image based on their frequencies. The

watermark is more commonly applied to the lower frequencies within an image as higher frequencies are usually lost when an image is compressed; moreover higher frequencies tend to be imperceptible to the human senses. Frequency based techniques result in a watermark that is dispersed throughout the image and is therefore, less susceptible to attack by cropping. However, these techniques are susceptible to standard frequency filters and frequency based compression algorithms, which tend to filter out less significant frequencies.

Techniques used for efficient bandwidth utilization such as compression, sampling, re-sampling, bit rate adjustment, filtering, bit shuffling, error correction, and re-transmission often interfere with digitally watermarked content. Compression in particular renders un-intended attacks during data transmission in low bandwidth channels. High quality images are often converted to JPEG to reduce their size; thereby invalidating watermarked content. Another un-intended attack method is the deletion or shuffling of blocks (Fabien A. P. Petitcolas, Ross J. Anderson, Markus G. Kuhn, 1998). In audio data, small blocks may be deleted or shuffled with no noticeable decrease in quality in order to better utilize available bandwidth. In images rows or columns of pixels may be deleted or shuffled without a significantly noticeable degradation in image quality. Other common unintended attacks include horizontal and/or vertical flipping, small angle rotation and cropping [9]. All these changes may render an existing watermark undetectable. It is therefore imperative that this matter be brought to the attention of standards bodies implementing various conflicting objectives. The security of information is a critical, necessary and vital part of the equation of modern communications networks.

These weaknesses and conflicting objectives existent in communications networks have been exploited by attackers almost with little or no resistance (Fabien A. P. Petitcolas, Ross J. Anderson, Markus G. Kuhn, 1998). Often attackers are only interested in a small subsection of an image, a piece of text, an audio track or series of video frames. A watermark at the edge of an image can often easily be cropped out of the picture without any significant loss. The mosaic attack is an extreme form of this method. In a mosaic attack, the attacker breaks up the entire watermarked image into many small parts. For example, a watermarked image on a web page can be cut up and reassembled as a whole using tables in HTML (Barni M., Bartolini F., 2007). The only defense against this attack is to tile a very small watermark all over the image, and allow retrieval of the watermark from any of the small subsections of the fragmented image. However, the attacker can always create smaller blocks, and the watermarked image also has to be large enough to be distinguishable. Watermarking is not restricted to just images. Audio watermarking uses the time and frequency masking properties of the human ear to conceal the watermark, and make it inaudible. One of the most frequently techniques used is echo-hiding. It involves hiding information within recorded sound by introducing very short echoes; relying on the fact that the human auditory systems cannot perceive echoes shorter than a few milliseconds. Information is embedded into audio data by introducing two types of echoes, characterized by their duration and relative amplitude. One echo type represents zeros while the other ones. This allows the encoding of watermarks within the audio data.

1.2.1 Spread Spectrum Frequency Method

Video watermarking is accomplished by using two main frequency based watermarking techniques namely: Spread Spectrum and Quantization Index Modulation. Spread Spectrum is a frequency-domain method where the watermark is placed only in perceptually significant portions of an image. Any attempt to remove the watermark would severely corrupt the original image data unless an exact inverse algorithm which extracts the original data is used. To embed a watermark in significant regions inconspicuously, a spread spectrum technique is used. Spread spectrum is a method whereby a narrowband signal is spread across a signal of much larger bandwidth. The total energy of the narrowband signal at any particular frequency is very low, and thus is imperceptible to the casual observer.

1.2.2 Quantization Index Modulation

Quantization Index Modulation relies on the quantization of the selected original data coefficients by means of a quantizer chosen among a set of quantizers based on the characteristics of data to be embedded. In a sense, QIM achieves the same results as, and even exceeds the Spread Spectrum technique by spreading the energy of the watermark across the entire data set. QIM is an efficient watermarking method which embeds an *N*-ary message by quantizing the signal using one of *N* quantizers. Dithering, chosen from a uniform distribution improves the security and efficiency of the system even further. A number of modifications have been proposed for QIM based watermarking algorithms. These adaptations however trade-off robustness against noise particularly in smooth image regions. Connected piecewise segments of curves distributed across the image is a possible QIM based algorithm. Bezier and Hermite Splines provide an interesting case to study. In the next section, we discuss the use of Bezier and Hermite Splines in the implementation of Quantization Index Modulated based watermarking.

2. HERMITE AND BEZIER SPLINES

A good class of equations representing geometric shapes is those describing curves and surfaces. Parametric curves are very flexible. They are not required to be functions. Curves can be multi-valued with respect to any coordinate system. A Parametric representation of curves and surfaces can be used to describe the geometric shapes and plot them on a graphics based system. The *X, Y* and Z coordinates can be expressed as shown below:

$$(X(u,v), y(u,v), z(u,v)) \tag{1}$$

This representation is functions independent.

2.1 Hermite Splines

We can represent an arbitrary length curve as a series of curves pieced together using their turning points as connection points. A Polynomial equation can be specified by the position of, and gradient at, each endpoint of curve.
Thus we can determine: $x = X(t)$ in terms of x_0, x_0', x_1, x_1'.
Consider

$$X(t) = a_3t^3 + a_2t^2 + a_1t + a_0$$
and $$X'(t) = 3a_3t^2 + 2a_2t + a_1.$$

Substituting for t at each endpoint:

$$x_0 = X(0) = a_0$$
$$x_0' = X'(0) = a_1$$
$$x_1 = X(1) = a_3 + a_2 + a_1 + a_0$$
$$x_1' = X'(1) = 3a_3 + 2a_2 + a_1$$

The solution can be shown to be

$$a_0 = x_0$$
$$a_1 = x_0'$$
$$a_2 = -3x_0 - 2x_0' + 3x_1 - x_1'$$
$$a_3 = 2x_0 + x_0' - 2x_1 + x_1'$$

The resultant polynomial can be expressed in matrix form as

$$X(t) = t^T M_H q, \tag{2}$$

where q is the control vector.

We can now define a parametric polynomial for each coordinate required independently, i.e. ***X(t),*** ***Y(t)*** and ***Z(t)*****.** The algorithm shown below plots the curve.

(1) Loop through t – select step size to suit.
(2) Plug x values into the geometry matrix.
(3) Evaluate P(t) $\rightarrow$ x value for current position.
(4) Repeat for y & z independently.
(5) Draw line segment between current and previous point.

Figure 1 below shows possible Hermite Spline graphs.

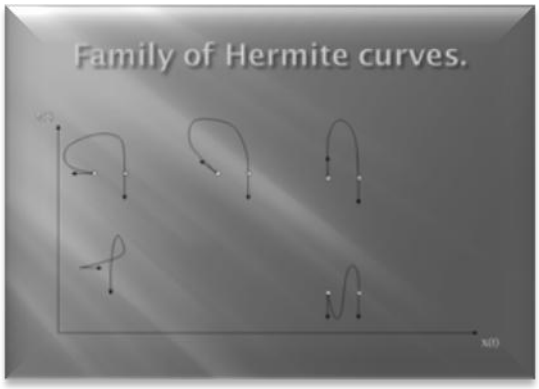

Fig. 1 Hermite Curves

2.2 Bézier Curves

In certain cases, Hermite cubic curves are difficult to model because there is always a need to specify need to specific coordinate points and gradients. It is possible to improve the system by specifying only points. Bezier Curves are more intuitive because of this. Bézier specify 2 endpoints and 2 additional control points to describe the gradient at the endpoints. A Bezier Matrix can be derived from a Hermite matrix. The cubic form of the Bezier Matrix is the most popular, i.e.

$\boldsymbol{X(t) = t^T M_B q}$ ……. (3), where M_B is the Bézier matrix.

Figure 2. below shows an example of a Bezier curve.

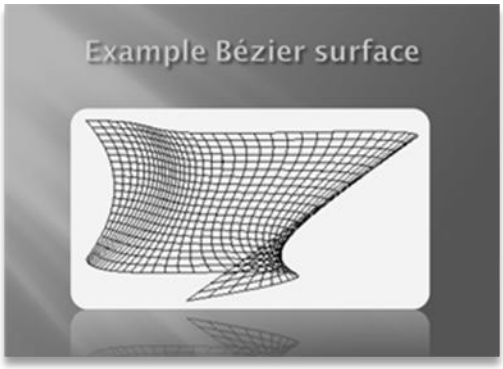

Fig. 2. Bezier Curve

3. THE QUANTIZED INDEX MODULATED HERMITE-BEZIER MODEL

Let ***O[M×N]*** denotes the original image with dimensions ***[M × N].***
Define a Transformation Function ***T*** over ***O[MxN]*** such that the resultant image

$$E[MxN] = T(O[MxN]).$$

The Transformation function ***T*** is a Bezier or Hermite Spline Function which introduces a watermark into ***O[MxN].***
The Transformation Function ***T*** also acts as a Quantization Matrix. ***T*** can be defined to meet a set of constraints ***C*** defined by the vector ***C[K]*** mapped to a vector of Stability Conditions ***S[K]***. The choice of constraints depends on the specific water marking application in question. Among the common Stability Conditions are: compression, cropping, rotation, translation, scaling, shearing, filtering, interference, time, frequency, phase shift, wavelength, amplitude, FFT operations (Owor, R., Dajani, K., Okonkwo, Z., Hamilton, J., 2008).

Mathematically, it is possible to show that given the original image matrix O, a transformation function T can be found such that, constrained by a vector C of constraints, satisfying a set of stability conditions S, the water marked image is guaranteed to enforce the constraint. The advantage of using Bezier and Hermite curves lies in their wide spread use in graphics systems. Further, these equations can be implemented to meet the stability requirements listed above without creating large matrices. Approximations of infinite Bicubic splines can also be done using Discrete Fourier Transform functions in the case of audio, video and animation signals based on time and frequency. The energy of the transformation matrix can be spread across the entire image of choosing the right parameters to enable the Bezier curves to cover the entire image.

4. CONCLUSION

Despite the vulnerability of current QIM techniques, watermarking remains important as long as it hinders the task of copyright infringement and the production of fake documents and currencies. Digital Watermarking is still in the infant stages of research (Bishop, M. 2000, Bansal, A.; Singh Bhadouria, S. 2007). Digital watermarking has not provided anything near the level of security provided by encryption schemes. In recent years, there has been a growing interest in this field (Mihcak, M. Kivanc, Venkatesan, Ramarathnam, Jakubowski, Mariusz H.**,** 2009)**.** Much work remains to be done. We hope to make a number of contributions to this new and vital area of research.

ACKNOWLEDGEMENTS

This work was partially supported under National Science Foundation Grants NSF-DUE-0621307 and NSF-DUE-0516432. We thank our colleagues at Auburn University for being such outstanding academic partners.

5. REFERENCES

1. Daly S. J., Squilla J R, Denber M, Honsinger C. W., Hamilton J., (1999), "Method for embedding digital information in an image", U.S. Patent 5,859,920, 1999.
2. Fabien A. P. Petitcolas, Ross J. Anderson, Markus G. Kuhn, (1998), Attacks on copyright marking systems, in David Aucsmith (Ed), Information Hiding, Second International Workshop, IH'98, Portland, Oregon, U.S.A., April 15-17, 1998, Proceedings, LNCS 1525, Springer-Verlag, ISBN 3-540-65386-4, pp. 219-239.

3. Barni M., Bartolini F., Data hiding for fighting piracy, (2007), Signal Processing Magazine, 21(2):28–39,
4. Bishop, M. (2000). Academia and Education in Information Security: Four Years Later. In Proceedings of the Fourth National Colloquium on Information System Security Education.
5. Chen B., (2000) "Design and analysis of digital watermark, information embedding, and data hiding systems," Ph.D. dissertation, MIT, Cambridge, MA, June 2000.
6. Bogumil, D., (2006), An asymmetric image watermarking scheme resistant against geometrical distortions, SP:IC(21), No. 1, January 2006, pp. 59-66.
7. Bansal, A.; Singh Bhadouria, S. (2007), Network Security and Confidentiality with Digital Watermarking, Digital EcoSystems and Technologies Conference, 2007. DEST apos;07. Inaugural, IEEE-IES Volume, Issue, 21-23 Feb. 2007 Page(s):325 – 328
8. Owor, R., Dajani, K., Okonkwo, Z., Hamilton, J., (2008) "A Hybrid Discrete Fast Fourier Transform Elliptical Cryptographic Algorithm for Portable Wireless Devices and Distributed Networks". ACM Huntsville Simulation Conference 2008, October 2123 2008.
9. Mihcak, M. Kivanc, Venkatesan, Ramarathnam, Jakubowski, Mariusz H., (2009), Assignee: Microsoft Corporation, US Patent 7634660 - Derivation and quantization of robust non-local characteristics for blind watermarking. http://www.patentstorm.us/patents/7634660/claims.html, last accessed Jan. 8th 2010