International Journal of Electronics and Electical Engineering

Volume 3 | Issue 3 Article 10

January 2015

GENERIC LOSSLESS VISIBLE WATERMARKING BY USING TRANSLUCENT AND MONOCHROME METHOD

Vijaya Kumar Talluri
Dept. of ECE, Loyala Institute of Tech and Management, Guntur, AP, India, vktalluri@gmail.com

M. Lakshmi Narayana
Dept. of ECE, Loyala Institute of Tech and Management, Guntur, AP, India, laksminm@gmail.com

Dr. S.Siva Reddy
Dept. of ECE, Loyala Institute of Tech and Management, Guntur, AP, India, sreddy@gmail.com

Recommended Citation

Talluri, Vijaya Kumar; Narayana, M. Lakshmi; and Reddy, Dr. S.Siva (2015) "GENERIC LOSSLESS VISIBLE WATERMARKING BY USING TRANSLUCENT AND MONOCHROME METHOD," *International Journal of Electronics and Electical Engineering*: Vol. 3 : Iss. 3 , Article 10.
DOI: 10.47893/IJEEE.2015.1154
Available at: https://www.interscience.in/ijeee/vol3/iss3/10

GENERIC LOSSLESS VISIBLE WATERMARKING BY USING TRANSLUCENT AND MONOCHROME METHOD

Vijaya Kumar Talluri[1], M. Lakshmi Narayana[2], Dr. S.Siva Reddy[3]
1PG Student, Dept. of ECE, Loyala Institute of Tech and Management, Guntur, AP, India
2Assistant Professor, Dept. of ECE, Loyala Institute of Tech and Management, Guntur, AP, India
3 Professor & HOD, Dept. of ECE, Loyala Institute of Tech and Management, Guntur, AP, India

***Abstract*-** Images make up a major component of multimedia content. Digital arts, illustrative diagrams, cultural heritage paintings in digitized for and digital photographs are examples of images. Advances in computing hardware, software, and computer networks have created threats to copyright protection and content integrity. In this paper, a new method for lossless visible watermarking is proposed by using appropriate compound mappings that allow mapped values to be controllable. The mappings are proved to be reversible for lossless recovery of the original image. The approach is generic, leading to the possibility of embedding different types of visible watermarks into cover images. Two applications of the proposed method are demonstrated, where opaque monochrome watermarks and non uniformly translucent full-color ones are respectively embedded into color images.

Keywords- *Fuzzy transportation; Trapezoidal fuzzy numbers; Optimal solution.*

I. INTRODUCTION

Digital watermarking is the process of embedding information into a digital signal in a way that is difficult to remove. The signal may be audio, pictures or video, for example. If the signal is copied, then the information is also carried in the copy. A signal may carry several different watermarks at the same time.

Digital watermarking methods for images are usually categorized into two types: invisible and visible. The first type aims to embed copyright information imperceptibly into host media such that in cases of copyright infringements, the hidden information can be retrieved to identify the ownership of the protected host. It is important for the watermarked image to be resistant to common image operations to ensure that the hidden information is still retrievable after such alterations. Methods of the second type, on the other hand, yield visible watermarks which are generally clearly visible after common image operations are applied. In addition, visible watermarks convey ownership information directly on the media and can deter attempts of copyright violations.

Embedding of watermarks, either visible or invisible, degrade the quality of the host media in general. A group of techniques, named reversible watermarking , allow legitimate users to remove the embedded watermark and restore the original content as needed. However, not all reversible watermarking techniques guarantee lossless image recovery, which means that the recovered image is identical to the original, pixel by pixel. Lossless recovery is important in many applications where serious concerns about image quality arise. Some examples include forensics, medical image analysis, historical art imaging, or military applications.

Research in digital watermarking covers almost all media forms. Examples include audio, video, image, text, 3-D model, and software codes. Digital watermarks are signals embedded imperceptibly into the media and can be detected under specific conditions.

The meaning and purpose of the earliest watermarks are uncertain. They may have been used for practical functions such as identifying the molds on which sheets of papers were made, or as trademarks to identify the paper maker. On the other hand, they may have represented mystical signs, or might simply have served as decoration. By the eighteenth century, watermarks on paper made in Europe and America had become more clearly utilitarian. They were used as trademarks, to record the date the paper was manufactured and to indicate the size of original sheets. It was also about this time that watermarks began to be used as ant counterfeiting measures on money and other documents.

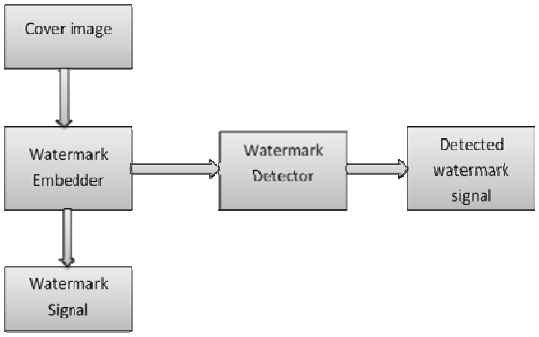


Figure 1 A Generic Watermarking System

In the remainder of this paper, the proposed method for deriving one-to-one compound mappings is described in Section II. Related lemmas and theorems are also proved and security protection measures described. Applications of the proposed method for embedding opaque monochrome and translucent color watermarks into color images are also described in Sections II. In Section III, the implementation methods for visible

watermarks are described. In Section IV, experimental results are presented to demonstrate the effectiveness of the proposed method. Finally, a conclusion with some suggestions for future work is included in Section IV.

II. EXISTING VS PROPOSED METHOD

Digital watermarking methods for images are usually categorized into two types, one is visible and another one is invisible. The first type aims to embed to copyright information imperceptibly into host media such that in cases of copyright infringements, the hidden information can be retrieved to indentify the ownership of the protected host. It is important for the watermarked image to be resistant to common image operations to ensure that the hidden information is still retrievable after such alternations. Methods of the second type, on the other hand, yield visible watermarks which are generally clearly visible common image operations are applied. In addition, visible watermarks convey ownership information directly on the media and can deter attempts of copyright violations.

Embedding of watermarks either visible or invisible, degrade the quality of the host media in general. A group of techniques named reversible watermarking, allow legitimate users to remove the embedded watermark and restore the original content as needed. However, not all reversible watermarking techniques guarantee lossless image recovery, which means that the recovered image is identical to the original, pixel by pixel.

Digital watermarking aims at hiding data directly into media contents. Originally, watermarking was designed to meet copyright protection requirements. It soon proved to be attractive to convey metadata, enabling content indexing, management and tracing . This technique has also been extended to control content integrity and authentication. It is then referred to as fragile watermarking. The use of a watermark for authentication purposes raises an important problem: as the watermark modifies pixel values, it also prevents strict integrity control. To circumvent the problem, the watermarking process has to be reversible, i.e. it must be possible to recover the original image from the watermarked one. In that sense, reversible watermarking is a lossless process. Besides enabling strict integrity control, lossless watermarks also enlarge the scope of watermarking based systems to any visual content stored or transmitted in a lossless(or reversible or noiseless) fashion. Lossless image processing is required in applications where pictures are subject to further processing, e.g. to extract specific information through extreme zoom. It is also desired for images obtained at great cost, or in applications where the quality desired for the rendering is still unknown. Medical imaging, prepress industry, image archival systems, precious artworks, military images, and remotely sensed images are all candidates for lossless processing, and in particular for lossless watermarking.

The additional functionality offered by digital watermarks, however, often comes at the expense of image fidelity. Most watermarking techniques modify, and hence distort, the host signal in order to insert the authentication information, and furthermore, the watermarked image rather than the original is authenticated. The distortion induced on the host image by the watermarking procedure is called the embedding distortion. Often, the embedding distortion is small and bounded, yet irreversible, i.e. it cannot be removed to recover the original host image. In many applications, the loss of image fidelity is not prohibitive as long as original and modified images are perceptually equivalent.

On the other hand, in medical, military and legal imaging applications, images are often enlarged, enhanced or further processed by image processing algorithms. Potential sensitivity of post processing operations to the embedding distortion and mission critical nature of these applications prohibit the permanent loss of image fidelity during watermarking. The loss of signal fidelity can be remedied by the use of Lossless Authentication (also referred as reversible, invertible or distortion-free authentication watermarks) techniques. These methods, like their lossy counterparts, insert authentication information by modifying the host signal, thus induce an embedding distortion. Nevertheless, they also enable the removal of such distortions and the exact lossless restoration of the original host signal. In this paper, after reviewing earlier methods, we propose a novel lossless authentication framework, which provides greater flexibility and improved computational performance. The new framework, in contrast with the earlier methods, verifies the authenticity and integrity before recovering the original, un watermarked image.

The concept of using a lossless data embedding method for authentication watermarking has been proposed earlier in the literature. and is commonly referred as invertible or reversible authentication . A general block diagram which is representative of the prior techniques is seen in Fig.2 All these methods are based on calculating the authentication information, and inserting this information using a lossless (reversible) data embedding method. The authentication information may be a hash, message authentication code, or digital signature computed over the un watermarked image. The methods are differentiated by the particular reversible data embedding scheme used. In particular, Fridrich . propose substituting least significant bit (LSB) plane(s) of the image by a bit-string containing the authentication information and the compressed form of the original LSBs. In this method, additional capacity is created through the lossless compression of the LSBs, which also allows for reconstruction of the original LSBs, thus the original image

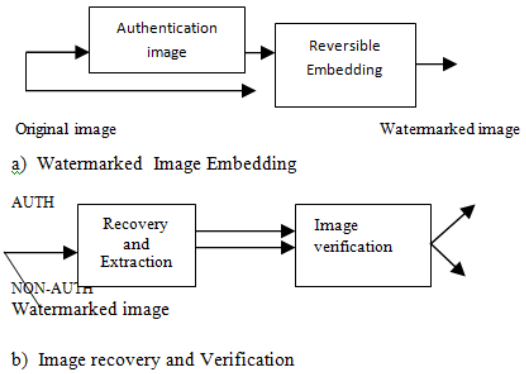


Figure 2 Prior lossless authentication watermarking methods

This method is later replaced with the RS-Embedding scheme, which improves the capacity or equivalently reduces the embedding distortion—in comparison with the earlier. Honsinger proposed using an additive spread spectrum watermark for data embedding. Reversibility of the scheme is guaranteed through the use of modulo arithmetic.

Recently, Tian explored the integer wavelet transform. In his method, called difference expansion, detail coefficients of the transform are modified in an invertible manner. In these methods, the integrity and authenticity of the image is verified by

i) extracting the embedded authentication information,
ii) reversing the watermarking procedure, thus reconstructing the original image,
iii) comparing the reconstructed image

with the extracted signature. If the extracted signature matches to the signature that is calculated from the reconstructed image, the image is deemed authentic. Note that the image reconstruction, which often is the most computation intensive process, is required for verification, even when the image is not authentic. Dittmann proposed an alternative protocol for the LSB compression technique. They replace the signature of the whole image with two signatures that are computed from the most significant bits (MSB) of the image and the compressed version of the LSBs, respectively. Their approach allows for validation before image reconstruction. In addition, encryption of the compressed LSBs facilitates reconstruction of the original by authorized parties who hold the secret key only, without affecting the public key validation process. Nevertheless, the protocol is dependent on the particular reversible data embedding mechanism and is not compatible, for instance, with Honsinger's method. Moreover, a second signature consumes additional capacity and thus increases embedding distortion. Note also that none of the lossless authentication methods in the literature offers tamper localization capability, which is one of the major advantages of authentication watermarks over conventional digital signatures.

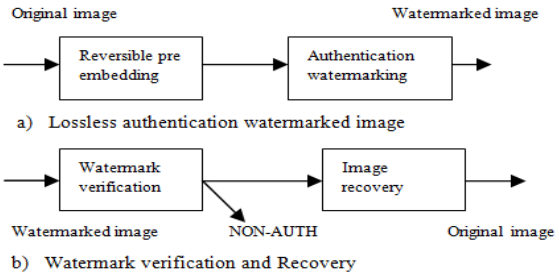


Figure 3 Prior lossless authentication watermarking methods

The lossless authentication framework proposed herein provides an alternative construction for authentication watermarking with lossless (reversible) data embedding.

As seen in Fig. 3, our approach differs from the prior techniques in the order of authentication and lossless data embedding phases. The prior schemes calculate the authentication information first, and then embed this information with a reversible data embedding method.

III. DESIGN ARCHITECTURE OF LOSSLESS WATERMARK SYSTEMS

As to lossless visible watermarking, the most common approach is to embed a monochrome watermark using deterministic and reversible mappings of pixel values or DCT coefficients in the watermark region. Another approach is to rotate consecutive watermark pixels to embed a visible watermark. One advantage of these approaches is that watermarks of arbitrary sizes can be embed into any host image. However, only binary visible watermarks can be embedded using these approaches, which is too restrictive since most company logos are colorful.

A. Database management systems:

As any other watermark, a lossless watermark conveys metadata information, which enables a range of applications such as IPRs identification, content indexing, management and usage or history tracing. The reversibility feature extends the scope of these applications to lossless systems.

B. Authentication systems

In a strict authentication system, the change of a single bit invalidates the integrity control, making no difference between malevolent and non-malevolent content manipulations. Strict authentication systems based on watermarking are only possible using lossless watermarks. Such systems can be either symmetric or

$$q = F_b^{-1}(F_a(p)) = F_b^{-1}(p-a) = F_b^{-1}(\varepsilon) = \varepsilon + b = \varepsilon + l$$

asymmetric. It is worth noting that for both systems the input image might be either the whole image or part of it. Independent authentication of non-overlapping regions, e.g. blocks, of the image provides localized detection of image modifications.

Reversible watermarking, also called lossless data hiding, embeds the watermark data into a digital image in a reversible manner, i.e. one can restore the original image without and degradation. Many techniques, focusing on

capacity-distortion improvement, have been proposed during the last decade. In most of the previous work, channel degradation is not allowed; as a result, such schemes are highly fragile. This limits the usability of reversible watermarking only in lossless environments.

The advance of computer technologies and the proliferation of the internet have made reproduction and distribution of digital information easier than before. Copyright protection of intellectual properties has, therefore, become an important topic. One way for copyright protection is digital water marking, which means certain specific information about the copyright holder in to the media to be protected.

Based on Lemma 1, we will now derive the proposed generic lossless visible watermarking scheme in the form of a class of one-to-one compound mappings, which can be used to embed variety of visible watermarks into images. The embedding is reversible, that is, the watermark can be removed to recover the original image losslessly. For this aim, a preliminary lemma is first described as follows.

Lemma 1 (Preference of Compound-Mapped Value):

It is possible to use the compound mapping

$$q = F_b^{-1}\left(F_a\left(p\right)\right)$$

to convert a numerical value to another value close to a preferred value .

Proof: Let

$$F_x\left(p\right) = p - x$$

Wherex is the parameter for F. Then

$q = F_b^{-1}\left(F_a\left(p\right)\right)$=$F_b^{-1}(p-a) = F_b^{-1}(\mathcal{E})$

$= \mathcal{E} + b = \mathcal{E} + l$

$F_x^{-1}(p') = p' + x$

Also, let

a= p- $\mathcal{E}$and b = l

where l is a small value. Then, the compound mapping $F_b^{-1}\left(F_a\left(p\right)\right)$means that the value is close to the preferred value. The above lemma relies on two assumptions. The first is that 'a' is close to 'p' or equivalently, that a=p- $\mathcal{E}$.

The reason why we derive the above lemma for a=p- $\mathcal{E}$ instead of a=p is that in the reverse mapping we want to recover from without knowing, which is a requirement in the applications of reversible visible watermarking investigated in this study.

Although the value of 'a'cannot be known in advance for such applications, it can usually be estimated, and we will describe some techniques for such estimations in the subsequent sections. The second assumption is that $F_x\left(p\right)$ yields a small value if x and p are close. Though the basic difference function

$$F_x\left(p\right) = p - x$$

used in the above proof satisfies this requirement for most cases, there is a possible problem where the mapped value may exceed the range of valid pixel values for some values of p and$x$. For example, whena=255,b=255and p=253 we have, q=255-253+255=257>255. It is possible to use the standard modulo technique (i.e., taking q = 257mod256 = 1) to solve this issue; however, such a technique will make q far from the desired target value which is 255. Nevertheless, we will show in Section III that using such a standard modulo function, $F_x\left(p\right) = p - x$ mod256, can still yield reasonable experimental results. Furthermore, we show earlier a more sophisticated one-to-one function that is free from such a wraparound problem. By satisfying the above two requirements, the compound mapping yields a value q that is close to the desired value. We now prove a theorem about the desired lossless reversible visible watermarking in the following.

Theorem1 (Lossless Reversible Visible Watermarking):

There exist one-to-one compound mappings for use to embed into a given image a visible watermark Q whose pixel values are close to those of a given watermark, such that the original image can be recovered from Q losslessly.

Proof: This is a consequence of Lemmas 1 and 2 after regarding the individual pixel values in I, L and Q respectively as those p,l and q mentioned in Lemma 2. And it is clear by Lemma 1 that the value can be recovered losslessly from the mapped value which is derived in Lemma 2. The above discussions are valid for embedding a watermark in a gray scale image. If color images are used both as the cover image and the watermark, we can apply the mappings to each of the color channels to get multiple independent results. The resulting visible watermark is the composite result of the color channels. Based on Theorem 1, the proposed generic lossless reversible visible watermarking scheme with a given image and a watermark L as input is described as an algorithm as follows.

Algorithm 1:Generic Watermark Embedding

Input: An image I and a watermark W.

Output: Watermarked image W.

Steps:

1) Select a set P of pixels from I where L is to be embedded and call P a watermarking area.

2) Denote the set of pixels corresponding to Pin W by Q.

3)For each pixel X with value p in P, denote the corresponding pixel in Q as Z and the value of the corresponding pixel Y in L as *l*and conduct the following steps.

a) Apply an estimation technique to derive to be a value close to *p*, using the values of the neighboring pixels of X (excluding itself X).

b) Set *b* to be the value *l*.

c) Map p to a new value

$$q = F_b^{-1}\left(F_a\left(p\right)\right.$$

d) Set the value of Z to be *q*.

4) Set the value of each remaining pixel in W, which is outside the region P, to be equal to that of the corresponding pixel in I.

Note that we do not use the information of the original image pixel value of itself for computing the

parameters and for X. This ensures that identical parameter values can be calculated by the receiver of a watermarked image for the purpose of lossless image recovery.

Algorithm 2: Generic Watermark Removal for Lossless
Image Recovery

Input: A watermarked image W and a watermark L.
Output: The original image R recovered from W.
Steps:

1) Select the same watermarking area Q in W as that selected in Algorithm 1.
2) Set the value of each pixel in R, which is outside the region Q, to be equal to that of the corresponding pixel in W.
3) For each pixel Z with value q in Q, denote the corresponding pixel in the recovered image R as X and the value of the corresponding pixel Y in L as *l*, and conduct the following steps.
a) Obtain the same value *a* as that derived in Step 3a of Algorithm 1 by applying the same estimation technique used there.
b) Set *b* to be the value *l*.
c) Restore *p* from *q* by setting

$$p = F_a^{-1}(F_b(q))$$

d) Set the value of X to be p.

IV. RESULTS AND CONCLUSION

A series of experiments implementing the proposed methods were conducted using the MATLAB software. To quantitatively measure the effectiveness of theproposed method, we define a set of performance metrics here. First, the quality of a watermarked image W is measured by the peak signal-to-noise ratio (PSNR) of W with respect to the non-recoverable watermarked image B in the following way

$$\mathrm{PSNR_w} = 20 \times \log_{10} \frac{255}{\sqrt{\frac{1}{w \times h}\sum_{y=1}^{h}\sum_{x=1}^{w}(W(x,y)-B(x,y))^2}}$$

Also, the quality of a recovered imageR is measured by the PSNR of R with respect to the original image I in a similar way

$$\mathrm{PSNR_R} = 20 \times \log_{10} \frac{255}{\sqrt{\frac{1}{w \times h}\sum_{y=1}^{h}\sum_{x=1}^{w}(R(x,y)-I(x,y))^2}}$$

It is desired to have the value of the$\mathrm{PSNR_w}$ to be as high as possible, so that the watermarked image can be visually as close to the benchmark image as possible.

For illicit recoveries, the $\mathrm{PSNR_R}$ should be as low as possible to make the recovered image visually intolerable (e.g., very noisy). In particular, we want the region obscured by the watermark to be as noisy as possible in an illicitly recovered image. For this purpose, we introduce an additional quality metric for an illicitly recovered image that only takes into account the region Q covered by the watermark. Specifically, we measure the quality of the recovered image Q by the following PSNR measure:

$$\mathrm{PSNR_Q} = 20 \times \log_{10} \frac{255}{\sqrt{\frac{1}{|Q|}\sum_{y=1}^{h}\sum_{x=1}^{w} SE_Q(x,y)}}$$

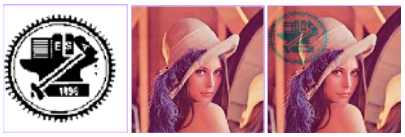
Table 1 gives the information about the average values of the $\mathrm{PSNR_w}$ obtained after embedding a particular watermark in the six test images, as wellas the average corresponding values of the $\mathrm{PSNR_R}$ and $\mathrm{PSNR_Q}$ obtained when incorrect keys were used for image recoveries. If the watermark coverage increases $\mathrm{PSNR_W}$ will decrease gradually. Table 1(a) and Table 1(b) are obtained by parameter and mapping randomization respectively. $\mathrm{PSNR_W}$ by the mapping randomization is low compared to parameter randomizationwith the same watermark coverage.

Table 1(a): PSNR values obtained by parameter randomization method

Watermark Coverage	$\mathrm{PSNR_R}$	$\mathrm{PSNR_Q}$	$\mathrm{PSNR_W}$
16%	24	14	33
22%	22.5	18	31.25
28%	26	20	32
34%	26.5	22	32

Table 1(b): PSNR values obtained bymapping randomization method

Watermark Coverage	$\mathrm{PSNR_R}$	$\mathrm{PSNR_Q}$	$\mathrm{PSNR_W}$
16%	20	12	32
22%	21	12	31
28%	18	11.5	30.32
34%	15	11	29



a) b) c)
Watermark image Original image Watermarked image

Fig. 5:Opaque monochrome watermarking method

a) b) c)
Watermark image Original imageWatermarked image

Fig. 6Translucent colour watermarking method

The image in Fig. 5(a) is taken as a watermark image and Fig. 5(b) is original image. By using opaque monochrome method these two images are embedded then watermarked image as shown inFig. 5(c)is obtained.

The image in Fig. 6(a) is taken as a watermark image and Fig. 6(b) is an original image. By using translucent

watermarking method these two images are embedded then watermarked image as shown in Fig. 6(c) is obtained. In this paper, a new method for reversible visible watermarking with lossless image recovery capability has been proposed. The method uses one-to-one compound mappings that can map image pixel values to those of the desired visible watermarks. Relevant lemmas and theorems are described and proved to demonstrate the reversibility of the compound mappings for lossless reversible visible watermarking. The compound mappings allow different types of visible watermarks to be embedded, and two applications have been described for embedding opaque monochrome watermarks as well as translucent full-color ones. A translucent watermark is clearly visible and visually appealing, thus more appropriate than traditional transparent binary watermarks in terms of advertising effect and copyright declaration. The two-fold monotonically increasing property of compound mappings was defined and an implementation proposed that can probably allow mapped values to always be close to the desired watermark if color estimates are accurate. The parameter randomization and mapping randomization techniques are also described, which can prevent illicit recoveries of original images without correct input keys. Experimental results have demonstrated the feasibility of the proposed method and the effectiveness of the proposed security protection measures.

The proposed methods can be extended to other data types other than bitmap images Like DCT coefficients in JPEG images and MPEG videos.

REFERENCES

[1] Y. Hu and S.Kwong,"Wavelet domain adaptive visiblewatermarking," Electron. Lett., vol. 37, no. 20, pp. 1219–1220, Sep. 2001.

[2] S. P. Mohanty, K. R. Ramakrishnan, and M. S. Kankanhalli, "A DCT domain visible watermarking technique for images," in Proc. IEEE Int. Conf. Multimedia and Expo, Jul. 2000, vol. 2, pp. 1029–1032.

[3] G. Braudaway, K. A. Magerlein, and F. Mintzer, "Protecting publicly available images with a visible image watermark," in Proc. SPIE Int. Conf. Electronic Imaging, Feb. 1996, vol. 2659, pp. 126–133.

[4] Y. J. Cheng and W. H. Tsai, "A new method for copyright and integrity protection for bitmap images by removable visible watermarks and irremovable invisible watermarks," presented at the Int. Computer Symp.—Workshop on Cryptology and Information Security, Hualien, Taiwan, R.O.C., Dec. 2002.

[5] F. A. P. Petitcolas, R. J. Anderson, and M. G. Kuhn, "Information hiding—A survey," Proc. IEEE, vol. 87, no. 7, pp. 1062–1078, Jul. 1999.

[6] N. F. Johnson, Z. Duric, and S. Jajodia, Information Hiding. Steganography and Watermarking—Attacks and Countermeasures. Boston, MA: Kluwer, 2001.

[7] I. J. Cox, J. Kilian, F. T. Leighton, and T. Shamoon, "Secure spread spectrum watermarking for multimedia," IEEE Trans. Image Process., vol. 6, no. 12, pp. 1673–1687, Jun. 1997.