OPTIMIZED EMBEDDING OF PERCEPTUAL HASH FOR IMAGE AUTHENTICATION IN DIGITAL CAMERAS

Sami-ud-Din[1]

Abstract

Combination of watermark and cryptographic hash function has been used in prevailing research for the authentication, tamper proofing and copy right protection of digital images. The key elements in such schemes are the robustness of watermark, reliability of authentication mechanism and the quality of the watermarked image. Most of the algorithms proposed compromise on one of above factors. This paper attempts to optimize the balance between these three factors by first quantifying these qualitative factors and then using optimization technique to find an efficient balance between these key factors. The perceptual hash function is utilized to enhance the security and reliability of digital images. This algorithm has been tested on a large database of images and the results are shown.

Keywords Optimal Wavelets, Image Security, Perceptual Hash, Watermarking, Multiresolution Analysis.

Introduction

The rapid growth and popularity in the field of digital photography and the use of communication networks for distribution of digital media has prompted the imminent need of copyright and ownership authentication [1],[2]. Digital watermarking, steganography and data hiding are promising methods for protection against piracy and malicious manipulations of original media contents [3]. *Robust*, *fragile* and *semi-fragile* authentication schemes are commonly used depending upon the nature of the applications. Small changes in digital contents due to lossy compression and image manipulations which do not survive in fragile watermarking are well tolerated in semi fragile schemes [4].

A typical state of the art digital image authentication system utilizes an embedded hash function [5] which is calculated over the image contents by utilizing a secret key [6]. Many different algorithms have been used for calculation of hash function. However, *perceptual hash function* [7] provides a promising and much more robust way of authentication of digital images. The perceptual hash function of an image is a short vector with random values and is indexed by using another vector *i.e.* secret key **K** and the resultant vector/hash is a function of this secret key. The key benefit of perceptual hash is that the numerical contents of image change due to compression, storage and transmission but its perceptual contents to human observer remains the same. Hence a perceptual hash is more resilient to compression and other attacks on the contents. The perceptual hash calculated by this hash algorithm is embedded in image itself in a transparent manner so that it remains invisible to normal storage, compression, communication and display systems. However, a compatible decoding system is capable of extracting the embedded hash and also generating the same hash if the encoding-decoding pair is known. If the hash calculated by the decoding system is the same as the hash embedded in the image, the authentications of contents of the digital image are verified.

Since the watermarking process distorts the image to some extent. It is important to quantify the distortion based on Human Visual System (HVS) with perceptual quality measures. Many techniques in literature

---

[1]General Manager,Human Resource Department,Nescom
Sector H-11/4,Islamabad
samiudin@yahoo.com

[8] include Mean Squared Error (MSE), Peak Signal to Noise Ratio (PSNR), Root Mean Squared Error (RMSE), Mean Absolute Error (MAE) and Signal to Noise Ratio (SNR). The other techniques based on Human Visual System (HVS) with perceptual quality measure. The algorithm proposed by Z. Wang and A. C. Bovik in their research publication [9] for Universal Image Quality Index (UQI) is used to compute the UQI of the watermarked and the host images. This technique for image quality measurement does not depend on the viewing conditions of the scene and the individual observer. This technique provides useful quality measure for digital images after manipulations of image processing applications *e.g.* insecure transmission, storage media, compression and change of image format.

Watermarking using Fourier Transform and Wavelet Transform [12] provide a reliable means of embedding data into the host image [10]. Different flavors of Discrete Wavelet Transform (DWT) based watermarking schemes are known [10]. We propose the use of Quantization Index Modulation (QIM) [11] on wavelet coefficients for embedding of perceptual hash in the digital images.

The robustness of watermark implies the ability to correctly extract watermark in the presence of image distortion due to compression, noise, basic image manipulations (intensity and contrast adjustment) and cropping etc. The adjustments of embedding parameters to increase the robustness of the watermark usually result in increase imperceptible distortion and hence decrease in quality index. The embedding process hence encounters a compromise between the reliability of the embedding and the perceptual quality of the image. An unreliable/ non-robust embedding of hash function may generate positive alarms in the forgery and false tamper detection process. Hence an optimized balance between the robustness and the image quality is desirable. This research aims at designing a suitable objective function, appropriate parameters for this optimization process. The advantage of this scheme is that it does not rely upon the fragility of the watermark as proposed by many research methodologies rather it aims at making the watermarking process as robust as possible while the reliability of the authentication mechanism comes from the use of perceptual hash function [7]. Any modification in the image will distort the perceptual hash function and the image will not be authenticated at the point of use.

A pre-stored key in the digital camera is used to generate the perceptual hash from the acquired image. The bits of this hash algorithm are embedded in the same image using watermarking in image. This watermarked image being optimized for both robustness and perceptual quality does not appear degraded to the user and can be used just like a normal digital image. However, if a deciding algorithm is used on this image with same secret key (compatible if private/ public key is used) then the perceptual hash can be recalculated and computed with the embedded perceptual hash function. For an un-tampered image the values of the two hash functions will be same.

This paper is organized in six sections; Section 1 gives an overview of digital image authentication scheme and its allied technologies. In section 2 embedding of watermark is explained. In section 3 we suggested methodology for optimization. In section 4 the methodology for image authentication mechanism is elaborated and finally sections 5 and 6 are dedicated for experimental results and conclusion respectively.

Embedding of Perceptual Hash

The perceptual hash function H(K,I) is embedded into wavelet coefficients of Discrete Wavelet Transform (DWT) of digital image **I(x,y)**. The DWT provides a simple hierarchical framework for interpretation of the image/signal information [14]. The detail of an image in general characterizes different physical structure at different resolutions. The coarse resolution/ approximation correspond to the larger structure in the

scene. It is, therefore natural to analyze the image initially at coarse level and then resolution gradually be increased from coarse-to-fine for particular application [14]. The DWT of an image provides the sub-bands of an image as LL, LH, HL and HH. The sub-band selection parameter is β , β = 0 for LL, β = 1 for LH, β = 2 for HL and β = 3 for HH. The distribution is shown in Fig. 1.

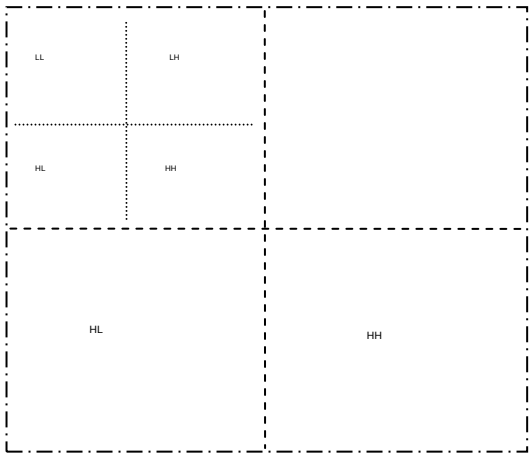

Figure 1. DWT Transform of an image into sub-images.

The selection of sub-band is carried out by Genetic Algorithms between β = 1 or 2 for higher payload to embed maximum data as characterized by the distribution of the contents of the digital images, whereas sub-band β = 3 is used to embed optimizing parameters. The perceptual hash is embedded in wavelet coefficients of the selected sub-band using dither Quantization–Index Modulation (QIM) codes [11]. The scalar uniform quantizer $Q(s)$ of the original signal with the step size γ is given by

$$Q(s) = \gamma \left\lfloor \frac{s}{\gamma} \right\rfloor \qquad (1)$$

The function $Q(s)$ is used to generate two new dithered quantizers as given below

$$Q_{0(x)} = \gamma \left\lfloor \frac{\left(s - \frac{\gamma}{4} \right)}{\gamma} \right\rfloor - \frac{\gamma}{4} \qquad (2)$$

$$Q_{1(x)} = \gamma \left\lfloor \frac{\left(s + \frac{\gamma}{4} \right)}{\gamma} \right\rfloor + \frac{\gamma}{4} \qquad (3)$$

where *s* is the original signal. These dithered quantizers are used to quantize and embed bit *m* of the hash function into the wavelet coefficients $w^{\beta}(x,y)$ as follows

$$w^{\beta}(x,y) = Q_i(w^{\beta}(x,y)) \text{ for } \begin{cases} i=0 \text{ for bit } m=0 \\ i=1 \text{ for bit } m=1 \end{cases} \qquad (4)$$

The graphical representation is depicted in Fig. 2 below.

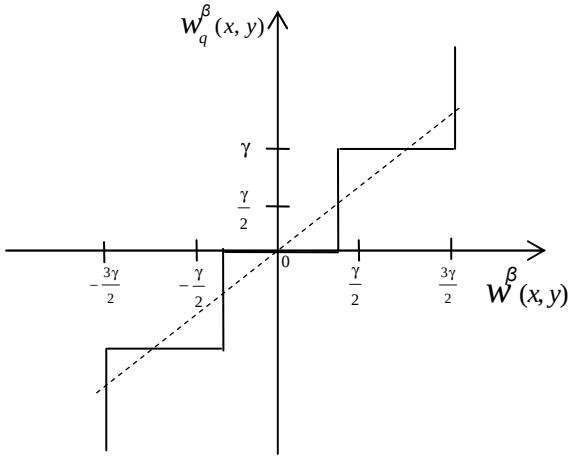

Figure 2. Selection of quantized sample for given sample using original QIM.

This Scalar QIM embedding scheme is modified to reduce the quantization noise in wavelet coefficients of the host image *s*, therefore quantization step γ is to be optimized. An additional parameter α is introduced to upgrade these quantizers to distortion-compensated QIM.

$$w_q^{\beta}(x,y) = Q_i(\alpha w^{\beta}(x,y)) + (1-\alpha) w^{\beta}(x,y) \quad (5)$$

where $\alpha \in (0,1]$ and $\begin{Bmatrix} i=0 & for & bit\ m=0 \\ i=1 & for & bit\ m=1 \end{Bmatrix}$ (6)

The graphical representation of distortion-compensation is shown in Fig. 3.

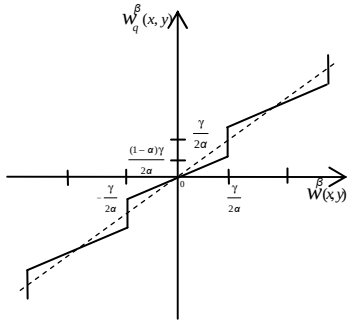

Figure 3. Selection of quantized sample for given sample using distortion compensated QIM.

For $\alpha = 1$ the results are the same as Scalar QIM and for $\alpha = 0$ the results are

$w_q^{\beta}(x,y) = w^{\beta}(x,y)$ indicating that nothing is embedded hence no distortion is introduced. The distortion introduced by the quantizer can be compensated by the adjustment of value of $\alpha \in (0,1]$. This distortion compensated technique is selected for achieving the objectives of distortion less embedding and error free retrieval of the embedded/hidden message.

Optimization of Embedding Parameters

The key factors in the process of embedding of watermark in digital images are Quality of image, robustness of watermark and security/reliability of the authentication process. These all parameters have conflicting properties and are interdependent and hence it is necessary to attain compromise between these factors. The parameters which are optimized in this algorithm are the distortion compensation factor of embedding process α, the choice of wavelet sub-band β and the quantization step γ. All of these factors have been introduced above. The optimization process tunes these parameters according to the objective function ***J*** described later.

- **Tuning process of** α – As the value of α increases the distortion-compensation in the embedding process decreases and hence the quality of image degrades. As mentioned above the extreme case is $\alpha = 1$ where the distortion-compensation Quantizer-Index Modulation becomes Scalar Quantizer-Index Modulation. On the other hand when α is lowered the distortion compensation improves but the embedding capacity decreases and hence the watermark goes from robust to fragile. The extreme case is $\alpha = 0$ where the quantization step becomes a straight line and no embedding can take place. This is degenerate case and hence $\alpha = 0$ is not included in the valid range of α.
- **Choice of** β - The choice of 'β' is translated into the objective function in such a way that a sub-band with higher absolute values of wavelet coefficients is chosen because higher values of wavelet coefficient ensure greater embedding capacity and hence robustness and also the better perceptual quality because of lower percentage of distortion.
- **Selection of** γ **-** A higher value of γ results in larger quantization bands and hence more robust watermark. Unfortunately larger γ result in greater distortion and visual quality becomes poor. On the other hand if we degrade the robustness it eventually improves the quality of the image (UQI).

In view of the above discussion the robustness of the watermark is defined as

$$R(\alpha,\beta,\gamma) = \frac{\gamma}{\alpha N}\sum_{n=0}^{N-1}\left|w^{\beta}(x,y)\right| \qquad (7)$$

Where *N* is total number of wavelet coefficient in the sub-band and $\alpha \in (0,1]$ for β = 1 or 2

- **Objective Function Evaluation -** The objective function *J*, $J = \max_{\alpha,\beta,\gamma}(w_1 R + w_2 Q_{I,I_w})$

I and I_w are host and watermarked images respectively. Subject to the constrains

$$w_1 + w_2 = 1\ ; \qquad \alpha \in (0,1] \qquad \beta = 1 \text{ or } 2, \qquad \gamma = (0, L) \qquad (8)$$

L is maximum absolute value of the wavelet coefficient. The distortion measure parameters w_1 and w_2 are empirically related with the condition, however $w_1 \neq 0$ and $w_2 \neq 0$. For this experiment we select both the factors of equal importance *i.e.* $w_1 = 0.5$ and $w_2 = 0.5$.

- **Genetic Algorithm-** The optimizing parameters *(* α , β , γ *)* for embedding of hash function are searched using Genetic Algorithms (GA). Genetic Algorithms are very efficient and stable for searching optimum solutions [15]. The GA uses the group of chromosomes for representation of the solution. The chromosomes and the problem solution are inter-transformed. The fitness function is evaluated for objective function for the fitness of each chromosome. The particular fittest chromosomes are chosen to be parents. The crossover and mutation are used to generate offspring from the parents. The fitness of offspring is evaluated and replacement of the selected chromosome is performed and the cycle is repeated until desired criterion is achieved.

4 Image Authentication Mechanism

The complete architecture of an image authentication mechanism is depicted in Fig. 4. This mainly consists of two processes entitled as watermark encoding and decoding process. The detail of both these processes is given as follows:

Encoding Process

The inputs of encoding process of the image authentication mechanism are digital image **I(x,y)** and the secret key **K**. The digital image **I(x,y)** is the data extracted by the image sensor such that $\mathbf{I(x, y) \in I}$ where **I** is set of all possible images of same size. The perceptual hash of the image **I(x,y)** is computed through perceptual hash algorithm as function of secret key **H(K,I)**. The secret key is unique for each media device and hence the perceptual hash computed for the same image with different devices will be different. Similarly, the perceptual hash is different if image has gone through certain malicious manipulations. The bit stream of perceptual hash function is embedded into image in DWT domain by quantizing the wavelet coefficients of the selected sub-band. The value of β *i.e.* the sub-band is calculated as one of the output parameter of the optimization process. This selection of sub-band is done for embedding of perceptual hash function. The optimization function aims at enhancing the robustness of the embedding process through proper selection of β =1 or 2 as described in section 3. The quantization step size for amplitude quantization of wavelet coefficients is another parameter γ computed by optimizing process utilizing Genetic Algorithms [14]. The Inverse Discrete Wavelet Transform of the watermarked image is computed after embedding of the perceptual hash and the image is watermarked but visually undistorted.

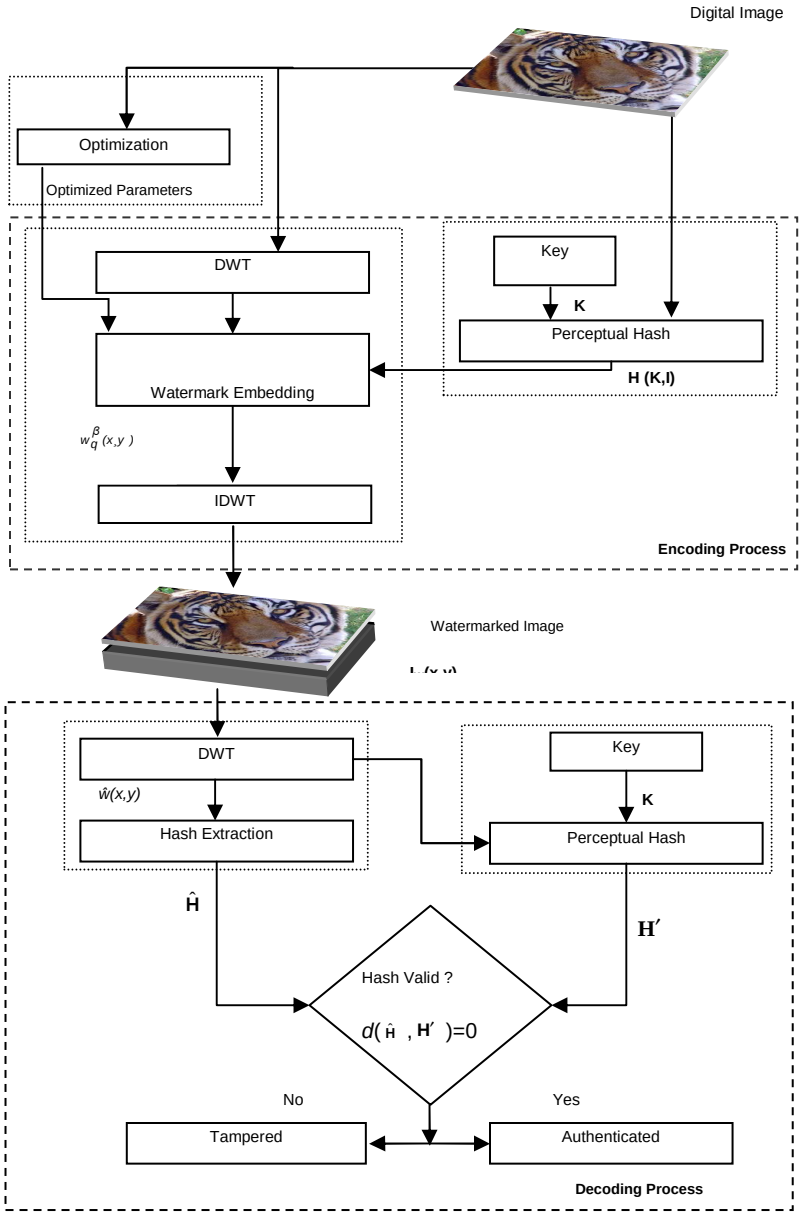

Figure 4. Algorithm for image authentication aided with perceptual hash of the host image.

Decoding Process

The decoding process starts first of all by taking Discrete Wavelet Transform of the watermarked image $\mathbf{I_w(x,y)}$. The perceptual hash $\hat{\mathbf{H}}$ [7] of the watermarked image $\mathbf{I_w(x,y)}$ is computed with the same secret key **K** utilized at the encoding end for computing perceptual hash **H(K,I)**. Similarly, perceptual hash $\mathbf{H}'$ of watermarked image $\mathbf{I_w(x,y)}$ is also computed [7]. The perceptual hashes $\hat{\mathbf{H}}$ and $\mathbf{H}'$ computed are compared and the absolute error is tested for a certain threshold ε as given

$$|\mathbf{H}' - \hat{\mathbf{H}}| < \boldsymbol{\varepsilon} \qquad (9)$$

Where ε is the expected error due to different image/signal processing application through which the image is passed. The image authenticity is verified if absolute error is less than ε and otherwise image is declared as tampered.

Experimental Results

The algorithm is tested over a large data base of images and reliable results are observed indicating the effectiveness of proposed watermarking scheme. In this scheme original image is not required whereas secret key and the optimized parameters from Genetic Algorithm are required, which are embedded in sub-band β = 3 i.e. HH. We selected four images for which the computed optimized parameters, α, β, γ are tabulated in table I. High contrast images give large variation in amplitude of wavelet coefficients as compare to low contrast images and hence results in large quantization step size γ. Similarly, sub-band selection depends on the total number of wavelet coefficients in the sub-band. We observe β =1 for image (d) in Fig. 5 as image has high vertical frequencies thus more coefficients in LH sub-band. We selected a set of ten images and pass these images through a variety of attacks from StirMarks software [16] after embedding watermark and then evaluate the algorithm for tamper detection and achieve significantly reliable results. We measure/ observe the robustness and imperceptibility of the watermark by content authentication and UQI of I and Iw respectively. The results of watermark survivability of the selected images at different compression levels by JPEG are shown in Fig. 6. The height of bars show the compressing ratio at which the watermark fails. We computed the quality of watermark image by computing UQI. The resulted UQIs for selected test images after embedding of watermark are shown Fig.7. The results obtained are then compared with other proposed watermarking techniques with and without hash function embedding and the results are found significantly reliable for tamper detection.

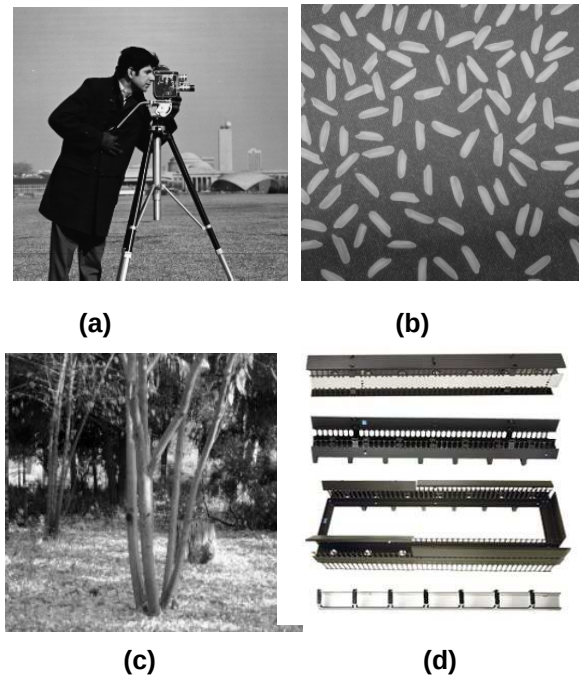

Figure 5. Different type of images for the verification of optimization factors: (a) High contrast image, (b) Low contrast image, (c) Image with vertical details and (d) image with vertical frequencies.

Table I. Optimized Parameters

Image	α	β	γ
Image (a)	0.60	2	15
Image (b)	0.53	2	11
Image (c)	0.31	2	05
Image (d)	0.59	1	14

We used Genetic Algorithm toolbox in MATLAB 7.1 environment with population size of 20 for 100,000 maximum generations with 100 stall generations (number of generations in which fitness value is unchanged) and two point crossover with mutation rate 0.01 for the design of desired parameters.

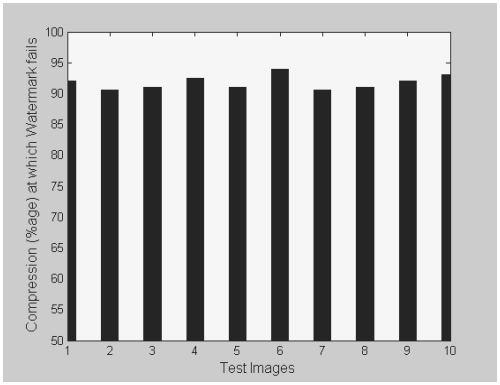

Figure 6. Watermark survivability for ten different images at different compression levels by JPEG compression.

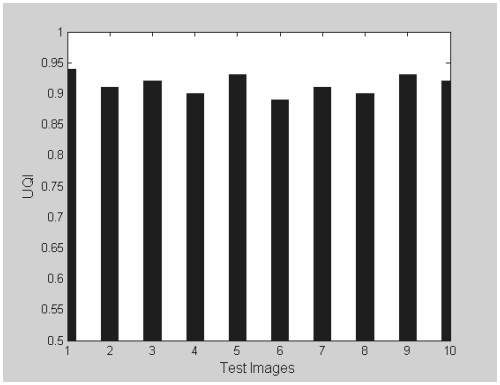

Figure 7. The Universal Quality Index of ten different watermarked images.

Conclusion

In this paper, we propose the optimized image authentication perceptual hash function indexed with secret key of digital camera as watermark. The experimental results show that proposed methodology improves the quality of the watermarked image while giving extremely good robustness and security. The proposed authentication mechanism is resilient to compression transformations and common geometric operations because of embedding of perceptual hash rather than numerical hash. The key benefit of perceptual hash is exploited as the numerical contents of image change due to compression, storage and transmission but its perceptual contents to human observer remain the same. Hence a perceptual hash is more resilient to compression and other attacks on the contents. Furthermore algorithms for perceptual hash computation are highly secure and reliable as compare to randomly chosen regions which provides unpredictable results for different intermediate hashes.

References

[1] G. L. Friedman, 1993 “The trustworthy digital camera: Restoring credibility to the photographic images,” *IEEE Trans. Consumer Electronics,* vol. 39, no.4, pp 905-910, Nov.

[2] L. Xie and G. R. Arce, July 1999 “A class of authentication digital watermarks for secure multimedia communication,” *IEEE Trans. Image Processing*, vol. 10, no. 11, pp. 1754-1764, Nov 2001.

[3] F. Hartung and M. Kutter, “Multimedia watermarking techniques,” *Proc. IEEE*, vol. 87, no. 7, pp. 1079-1107.

[4] E. Martinian, G. W. Wornell and B. Chen, July 2005 “Authentication with Distortion criteria,” *IEEE Trans. on Information. Theory,* vol. 51, no. 7, pp.2523-2542.

[5] J. Cannons and P. Moulin,Oct. 2004 “Design and Statistical Aalysis of a Hash-Aidd Image Watermarkin System,” *IEEE Trans. on Image Processing*, vol. 13, no. 10, pp. 1393-1408.

[6] M. S. Hawang, C. Chang and K. Hwang, May 1999 “A Watermarking Technique Based on One-Way Hash Functions,” *IEEE Trans. on Consumer Electronics*, vol. 45, no. 2, pp. 286-294.

[7] V. Monga and B. L. Evans, Nov. 2006. “Perceptual Image Hashing Via Feature Points: Performance Evaluation and Tradeoffs,” *IEEE Trans. on Image Processing*, vol. 15, no. 11, pp3453-3466, T. N. Pappas and R. J. Safranek, “Perceptual criteria for image quality evaluation,” in Handbook of Image and Video Processing, A.C. Bovik, Ed. New York: Academic, May 2000.

[8] Z. Wang and A. C. Bovik, March 2002 “A Universal Image Quality Index,” *IEEE Signal Processing Letters*, vol. 9, no. 3, pp. 81-84.

[9] M. D. Swanson, M. Kobayashi, and A. H. Tewfik,“ Multimedia data-embedding and watermarking technologies,” *Proc. IEEE*, vol. 86, pp. 1064-1087.

[10] B. Chen and G. W. Wornell,June 1998Quantization index modulation: A class of provably good methods for digital watermarking and information embedding,” *IEEE Trans. Information Theory,* vol. 47, no. 4, pp.1423-1443, May 2001.

[11] W. Zhu, Z. Xiong, and Y. Q. Zhang, 1998 “Multiresolution Watermarking for images and video: a unified approach,” *in Proc. Int. Conf. on Image Processing (ICIP)*, Chicago, IL.

[12] S. G. Mallat, July 1989 “A Theory for Multiresulation Signal Decomposition: The Wavelet Representation,” *IEEE Trans Pattern Analysis and Machine Intelligence,* vol. 11, no.7, pp. 674-693.

[13] P. Kumsawat, K. Attakitmongcol and A. Srikew, “A New Approach for Optimization in image Watermarking by Using Genetic Algorithms,” *IEEE Trams. on Signal Processing*, vol. 53, no. 12, pp. 4707-4719,.

[14] J. H. Holland, 1975 *Adaptation in Natural and Artificial Systems*. Ann Arbor, MI: University of Michigan Press.

[15] Fair Evalution Proceddures for Watermarking System, 2000[online]. Aavailablehttp://www.petitocolas.net/fabien/watermarking/strimark.html