



## Improved Reversible Watermarking Using Hash Function

K. Srilakshmi, K. Srinivas

Department of CSE, Gudlavalleru Engineering College,  
India

**Abstract:** Protection of digital multimedia contents, as well as security and privacy have become a major challenge due to the recent advances in the fields of networking, and digital multimedia, as well as the readily availability of copying and manipulative devices and software programs to the public. One possible explanation is that the traditional wavelet transform coefficients are more sensitive to filtering and noise than originally expected. Hence, the embedded mark could not survive these modifications. One way to overcome this problem is to use a hash robust watermark embedding algorithm. Experimental results show that proposed model outperformed well against traditional approaches.

**Keywords:** watermarking, Security, Encode and Decode, Fragile watermarking, PSNR ratio.

### I. INTRODUCTION

Digital Watermarking (also known as Multimedia data Embedding, Steganography) protects the copyright of digital images. Reversible watermarking or Lossless Data embedding has to meet the requirements are Robustness, imperceptibility, embedding and retrieving, high embedding capacity. Usually Watermarking process introduces irreversible degradation of the original medium. For classical watermarking, the images with high content of textures provide more capacity for data hiding than the one without textures. This is due to the fact that the human visual system is less sensitive to degradation in textured areas and thus one can embed more in textured than in uniform areas (see [1], etc.).

For reversible watermarking, this is not true: one can embed more data in uniform than in textured areas. This can be easily explained by the fact that the reversible watermarking schemes are based on pixel correlation, and the correlation in textured areas is lower than in uniform areas. We remind that reversible watermarking not only demands imperceptible embedding of data, but also the recovery of the original host without any errors. The algorithms providing the highest embedding bit-rates are the so called difference expansion reversible watermarking [2, 3], etc. Difference expansion creates room for data embedding into the least significant bit (LSB) of a certain pixel based difference, usually in the prediction error. More precisely, pixels are modified such that, the prediction error at detection be two times larger. The multiplication by two sets to zero the LSB and leaves room for a bit of data.

Even a very slight change in pixel values may not be acceptable for military, medical data and also multimedia archiving of valuable original works. By embedding its message authentication code, Reversible data embedding provide True self authentication scheme. If noise like signal can be added to images, audio, video Steganography [2] protect it from alteration and authenticate its content. [3] Presented the RS scheme to embed watermark bits into the status group of pixels. Fredrich also extended the technique to GIF and PNG images. [4] enhanced fridrich's approach and develop a low distortion Reversible watermark that is capable of embedding 0.7 bits per pixel.

Generalization of LSB [5] based on the scheme by applying data compression. From the literature review we have seen that most of the RW scheme belongs to fragile watermarking technique. Fragile watermarking is a type of watermarking technique which embeds secret information called watermark into an image that is not readable anymore if the content gets altered by any kind of intentional or unintentional attacks. And the term 'semi' indicates if it can sustain some attacks, moreover, if any watermark can sustain with all kinds of attacks is called robust watermarking technique. Fragile watermarking is the subject of many applications like content authentication.

Reversible Watermarking is a special case of digital watermarking with an intriguing feature that when the watermarked content has been authenticated, one can remove the watermark to retrieve the exact same original information. Such reversibility is highly desirable in case of high secured data communication, especially for medical and military applications where even a small amount of distortion is not permissible.

### II. LITERATURE SURVEY

#### IMAGE PARTITIONING AND DISTORTION CONTROL

It is seen that a natural images possess different characteristics like smooth, edge, texture region, etc. and different regions are in a different way sensitive to embedding distortion. This needs adaptive watermark power control so that the overall structure of the watermarked image is less affected. In an automatic identification of image regions, it is difficult to find threshold gray values due to imprecise and uncertainties in gray values. Here, we partition an image into three components using the computed gradient magnitudes [5]; gives a simple image partition method that we used to obtain different image regions.

Chang D.Yoo et al. (2007), explains high capacity and low distortion reversible image watermarking using integer to integer wavelet transform (IWT) and this condition to avoid overflow/underflow in the spatial domain are derived for an arbitrary wavelet and block size. They describe the most popular method of watermarking which includes spread spectrum such as additive and multiplicative spread spectrum. [5] Proposed lossless watermarking based on a circular interpretation of Objective transformations. Tian (2003), gave one of the first few development of reversible watermarking. Yang et al. (2004) proposed a reversible watermarking technique based on the Discrete Cosine Transform. [6] Adopted the histogram shifting technique to embed the location map that the DE scheme required. They then proposed a PEE method to embed watermarks. They present multibit, multiplicative, spread spectrum watermarking using the discrete multiwavelet. [7] proposed a reversible watermarking method in medical and defense imagery with the combination of IWT and Genetic algorithm. They describe another popular class of reversible watermarking algorithm is based on the hybrid IWT. IWT based adaptive data hiding scheme is to protect medical images. They applied the compounding technique to reversibly embed a large amount of data into an audio proposed a reversible watermarking scheme based on Integer DCT.[9] develops a blind image watermarking based on multiband wavelet transform and the empirical mode decomposition. The scheme is robust against JPEG compression, Gaussian noise, salt and pepper noise. Histogram modification is another important technique in RWM.[9] compares wavelet and multiwavelet domain watermarking under a variety of attacks. Furthermore, they describe both wavelet style and multi wavelet style watermarking under multiwavelet domain watermarking. Multiwavelets offer better visual quality than scalar wavelets.

Watermarking as it is used today may refer to all four categories mentioned above. To address the intended applications properly, in this thesis watermarking refers to the overt watermarking and steganography categories. Furthermore, this thesis focuses on the still images as a part of the multimedia contents; all the reviews, discussions, and the proposed reversible watermarking scheme and biometric watermark framework principally target digital still images. Although, the suggested algorithms can be modified and adjusted to extend to the video contents.

These schemes show a certain degree of robustness when the watermarked image undergoes specific alterations or processes. In the case of semi-fragile methods, the tolerable process is usually confined to a slight compression process or other mild intentional or unintentional changes. On the other hand, robust schemes often present good tolerance against specific intentional attacks or unintentional sever modifications, depending on the purpose they are designed for. Hence, a watermarking scheme is called semi-fragile or robust if the extracted watermark from the modified/processed marked image stays ascertainable and valid.

#### **1) Least Significant Bit Coding (LSB)**

LSB coding is one of the earliest methods. It can be applied to any form of watermarking. In this method the LSB of the carrier signal is substituted with the watermark.

The bits are embedded in a sequence which acts as the key. In order to retrieve it back this sequence should be known. The watermark encoder first selects a subset of pixel values on which the watermark has to be embedded. It then embeds the information on the LSBs of the pixels from this subset. LSB coding is a very simple technique but the robustness of the watermark will be too low. With LSB coding almost always the watermark cannot be retrieved without a noise component [9].

#### **2) Predictive Coding Schemes**

Predictive coding scheme was planned by Matsui and Tanaka in [2] for gray scale images. In this method the correlation between neighboring pixels are broken. A set of pixels where the watermark has to be embedded is chosen and alternate pixels are replaced by the difference between the adjacent pixels. This can be further enhanced by adding a constant to all the differences. A cipher key is created which enables the retrieval of the embedded watermark at the receiver. This is much more robust as compared to LSB coding.

#### **3) Correlation-Based Techniques**

In this method a pseudo random noise (PN) with a pattern  $W(x, y)$  is added to an image. At the decoder the correlation between the random noise and the image is found out and if the value exceeds a certain threshold value the watermark is detected else it is not.

#### **4) Patchwork Techniques**

In patchwork watermarking, the image is divided into two subsets. One feature or an operation is chosen and it is applied to these two subsets in the opposite direction. For instance, if one subset is increased by a factor  $k$ , the other subset will be decreased by the same amount. If  $a[i]$  is the value of the sample at  $I$  in subset 'A' which is increased and  $b[i]$  is the value of the sample in the subset 'B' whose value is decreased, then the difference between the two subsets would intuitively result in  $\sum(a[i]-b[i])=2N$  for watermarked images  $1 \leq i \leq N$  otherwise

### **III. PROPOSED WORK**

In the past decade, application of digital multimedia contents has grown rapidly because of their advantages over analog contents. Ease of transferring and broadcasting over networks, higher quality and durability, online/offline easy editing, copying, and simplicity of archiving or are just storing a few advantages of digital multimedia over analog contents. Ironically, all the above advantageous properties have raised the main concerns in copyright management and privacy protection of such contents.

Encryption methods such as conventional connection-based security systems cannot carry out the required proper protection level as it is impossible to monitor how a legitimate user handles the content after decryption, which makes it possible for hackers and adversaries to illegally redistribute or manipulate the content.

The encoder creates the symbols from the input message and transmits them across a noisy channel, then at the receiver side the encoder reconstructs the original message from the received noisy transmitted symbols. To ensure the security of the model and the transmission secret keys can be employed at the encoder and decoder. The same generic model can be adopted to illustrate a digital watermarking system. In a digital watermarking model the to-be-embedded watermark can be considered as the input message, the cover media plays the same role as the noisy channel and the detector has the same function as the decoder.

Fig. 1 is a block diagram of a watermarking system using content-dependent watermarks. The emphasis of this chapter is to design a robust hash function which can be used to generate a description of the original signal. This description is then embedded into the cover signal. In authentication, the watermark is compared to the original signal.

Conventional cryptographic hash functions such as MD5 and SHA-1 are very sensitive to changes in the input signal. Generally, a single-bit change will produce a completely different hash. Since the cover image will undoubtedly be different after watermark embedding, an image hash function should be robust to perceptually insignificant modifications.

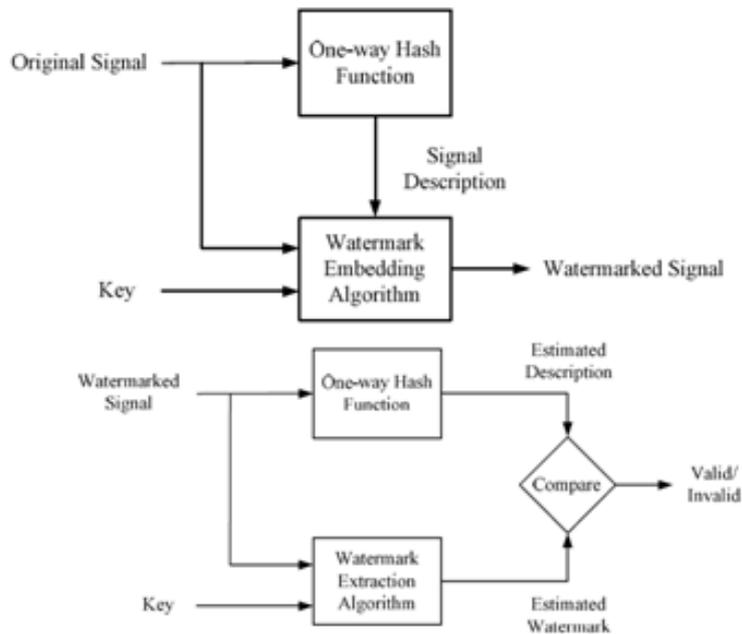


Fig 1: Conventional Model

### Proposed Model

Pre-processing methods use a small neighborhood of a pixel in an input image to get a new brightness value in the output image. The aim of pre-processing is an improvement of the image data that suppresses unwanted distortions or enhances some image features important for further processing. In this system we are converting different image formats into JPEG-LS image as JPEG-LS is a lossless compression standard for images and was developed with the aim of providing a low-complexity lossless compression standard that could offer better compression efficiency than lossless JPEG. Lossless image compression attempts to retain absolutely all the information present in the original image.

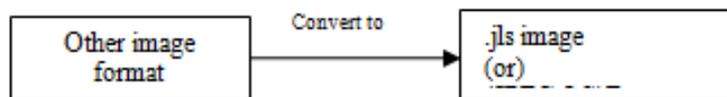


Fig 2: Proposed Model

### Proposed Algorithm

**Step 1:** Apply the Gaussian Low pass filter:

The low pass filtering model can be represented by using Gaussian Function  $G(p,q)$  and an image  $I(p,q)$ .

$$Gf(p, q, \sigma_{I(p,q)}^2) = G(p, q) * I(p, q).$$

$$G(p, q) = (1 / 2\pi\sigma_{I(p,q)}^2) * e^{-(p^2+q^2)/2\sigma_{I(p,q)}^2}$$

Where  $\sigma$  is the standard deviation of the distribution.

**Step 2:** Normalize the size of the  $I(p,q)$ .

UL	UC	UR
L	C	R
LL	LC	LR

$$N = (I(p, q) - \max(p, q)) / (\max(p, q) - \min(p, q))$$

L2 Norm can be processed using the following vector representation.

$$vec_i = vec_c / \sqrt{\|vec_k\|^2 + \epsilon^2}, i = 1, 2, \dots$$

$vec_c$  is a vector consisting of HoG descriptors of cell. For  $i=1$ , vector  $vec_k$  contains  $vec_c$  and the descriptors of cells UL, UC and L.

For  $i=2$ , vector  $vec_k$  contains  $vec_c$  and the descriptors of cells UR, UC and R.

For  $i=3$ , vector  $vec_k$  contains  $vec_c$  and the descriptors of cells LR, LC and R.

For  $i=4$ , vector  $vec_k$  contains  $vec_c$  and the descriptors of cells LL, LC and L.

**Step 3:** Compute the local histogram of the Image I.

$$\text{Hist}(I) = \text{LocalHist}(vec_i);$$

**Step 4:** Watermark feature extraction using compressed coding. Watermark compressed feature is computed by using

$$CF(i, j) = (1 / N_1 N_2) \sum_{m=1}^{N_1} \sum_{n=1}^{N_2} d_{(i,j)}(m, n)^3$$

$$F_i = \max(CF(i, j))$$

**Step 5:** In order to construct the hash each compressed feature  $F_i$  is transformed into the bit string  $hash_i$  using the following equation.

$$hash_i = 0, \text{ if } F_i \leq \text{var}(F_i)$$

$$= 1, \text{ if } F_i > \text{var}(F_i)$$

Step 6: Feature hash vector  $h = \{hash_1, hash_2, hash_3, hash \dots hash_n\}$ .

Watermark recovery is usually more robust if the original, unwatermarked data are available. Further, availability of the original data set in the recovery process allows the detection and inversion of distortions which change the data geometry. This helps, for example, if a watermarked image has been rotated by an attacker. However, access to the original data is not possible in all cases, for example, in applications such as data monitoring or tracking.

#### IV. EXPERIMENTAL RESULTS

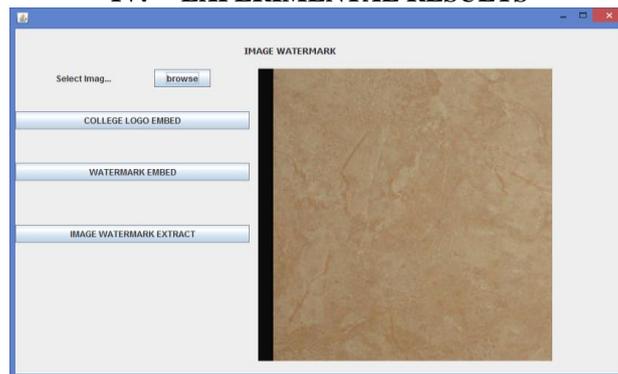


Fig 3: Loading source image

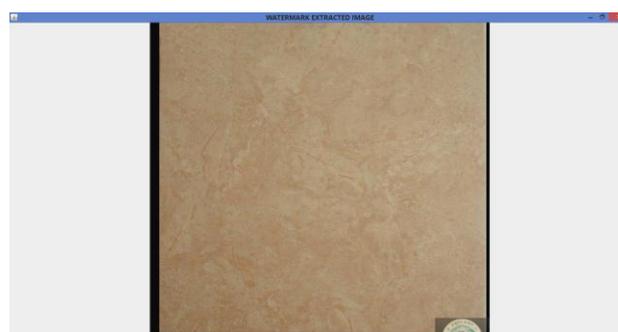


Fig 4: Embedded Watermark



Fig 5: Computing Hash Value

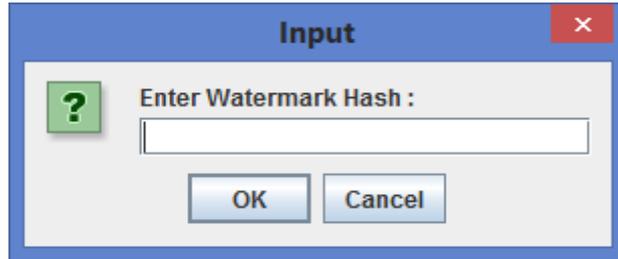


Fig 6: Enter hash value for Extraction



Fig 7: Entered hash Value



Fig 8: Extracted Logo

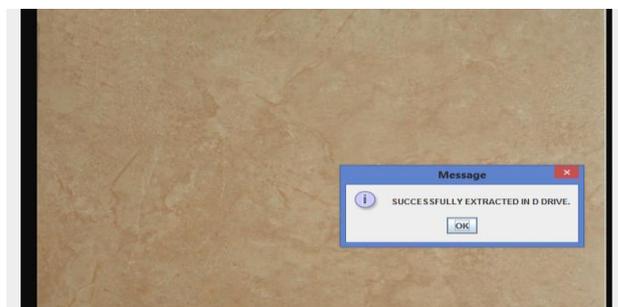


Fig 9: Extracted source image

Table 1: Computational performance

Model	Encoding Time	DecodingTime	RunTime
DCT model	6646	6743	16363
reversible model	5933	5936	12754
Proposed model	2635	3166	7461

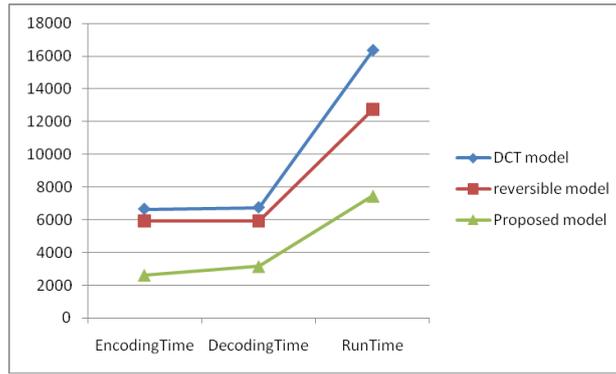


Fig 10: Performance graph

Table 2: Local prediction table

Model	Bitrate	LocalPrediction
DCT model	0.67	0.81
reversible model	0.79	0.82
Proposed model	0.94	0.93

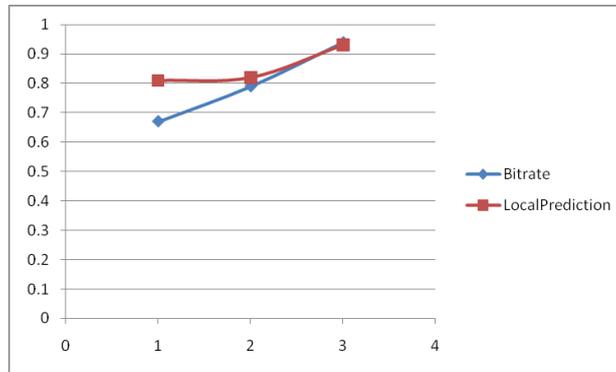


Fig 11: Comparison with other other models

Table 3: PSNR ratio with Local prediction

Model	PSNR ratio	LocalPrediction
DCT model	0.65	0.81
reversible model	0.71	0.82
Proposed model	0.9	0.93

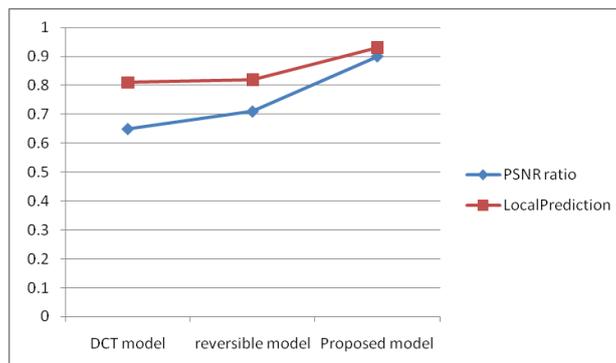


Fig 12: Graph comparison with other models

## V. CONCLUSION

The hash based watermark embedding technique presented in this paper is robust against high quality images and other image processing operations. One possible explanation is that the traditional wavelet transform coefficients are more sensitive to filtering and noise than originally expected. Hence, the embedded mark could not survive these modifications. One way to overcome this problem is to use a hash robust watermark embedding algorithm. Experimental results show that proposed model outperformed well against traditional approaches.

## REFERENCES

- [1] "Robust Watermarking of Compressed and Encrypted JPEG2000 Images" A.V.Subramanyam, Sabu Emmanuel, Member, IEEE, and Mohan S.Kankanhalli, Senior Member, IEEE.
- [2] "CHAKRA: A New Approach for Symmetric Key Encryption", P.Ramesh Kumar, S.S.Dhenakaran, IEEE International Conferences on Acoustics, Speech and signal processing, Vol.4, 1996, pp. 2168-2171.
- [3] A.Subramanyam, S.Emmanuel, and M.Kankanhalli "Compressed encrypted domain JPEG2000 Image watermarking," in *Proc. IEEE Int. Conf. Multimedia and Expo, 2010*, pp. 1315–1320.
- [4] Qunting Yang "A Novel Semi-fragile Authentication Watermarking Scheme of Color JPEG Image in Compressed Domain" college of Information Science, Nankai University Tianjin, China. *2010 International Conference on Multimedia Information Networking and Security*
- [5] R. Schyndel, A. Tirkel, and C. Osborne, "A digital watermark," in *IEEE Proc. Int. Conf. Image Processing*, 1994, vol. 2, pp. 86–90.
- [6] "A robust multiple watermarking scheme in the Discrete Wavelet Transform domain" by Peining TAO and Ahmet M. Eskicioglu The Graduate Center, The City University of New York, 365 Fifth Avenue, New York.
- [7] "A robust multiple watermarking scheme in the Discrete Wavelet Transform domain" by Peining TAO and Ahmet M. Eskicioglu Department of Computer and Information Science, Brooklyn College, The City University of New York, 2900 Bedford Avenue, Brooklyn, NY 11210
- [8] W. Bender, D. Gruhl, N. Morimoto, and A. Lu, "Techniques for data hiding," *IBM Systems Journal*, vol. 35, no. 3-4, pp. 313-336, 1996.
- [9] R.B.Wolfgang and E.j.Delp, "A watermark for digital images" in *IEEE proc.Int.conf.Image Processing*, 1996, vol.3, pp.219-222.
- [9] M. D. Swanson, B. Zhu, and A. H. Tewfik, "Transparent robust image watermarking," in *IEEE Proc. Int. Conf. Image Processing*, 1996, vol. 3, pp. 211–214.
- [10] J. Cox, J. Kilian, T. Leighton, and T. Shamoan, "Secure spread watermarking for multimedia," *IEEE Trans. Image Processing*, vol. 6, no. 12, pp. 1673–1687, Dec. 1997.
- [11] M. Barni, F. Bartolini, and A. Piva, "Improved wavelet-based watermarking through pixel-wise masking", *IEEE Trans. Image Processing*, vol. 10, no. 5, pp. 783–791, 2001.
- [12] X. Xia, C. G. Bonchelet, and G. R. Arce, "A multiresolution watermark for digital images," in *IEEE Proc. Int. Conf. Image Processing, USA, 1997*, pp. 548-551.
- [13] J. R. Kim, and Y. S. Moon, "A robust wavelet-based digital watermarking using level-adaptive thresholding," in *IEEE Proc. Int. Conf. Image Processing, Japan, 1999*, pp. 226-230.
- [14] T. Hsu, and J. L. Wu, "Hidden digital watermarks in images," *IEEE Trans. Image Processing*, vol. 8, no. 1, pp. 58–68, Jan. 1999.
- [15] Dugad, K. Ratakonda, and N. Ahuja, "A new wavelet-based scheme for watermarking images," in *IEEE Proc. Int. Conf. Image Processing, USA, 1998*, pp. 419-423.