COMPARATIVE ANALYSIS OF ADVANCED REVERSIBLE WATERMARKING TECHNIQUES

By

V. BELMER GLADSON * Y. SAM JOSUVA ** R. BALASUBRAMANIAN ***

* Research Scholar, Department of Computer Science and Engineering, Manonmaniam Sundaranar University, Tamilnadu, India.
** Assistant Professor, Department of Computer Science and Engineering, Manonmaniam Sundaranar University, Tamilnadu, India.
*** Professor, Department of Computer Science and Engineering, Manonmaniam Sundaranar University, Tamilnadu, India.

ABSTRACT

The Reversible watermarking is a field of hiding the information, which hides the crucial information in different forms like an image, song, video for protection of illegal duplication and distribution of multimedia data. This research work is to embed data in encrypted images and decrypt the image to rebuild the original image by removing the hidden data without any distortion. There are many researches in this field and various techniques were proposed. So in order to choose which one is the best technique, a definite need arises to compare with the techniques like Least Significant Bit (LSB), Difference Expansion (DE), Reversible Contrast Mapping (RCM), Wavelet-Fuzzy (WF) and these reversible watermarking methods are analyzed with the help of metrics PSNR, MSE, Processing Time and Correlation. From the experimental results and performance evaluation, LSB is better, but based on correlation and after applying a median filter, Wavelet- Fuzzy (WF) provides better results.

Keywords: Reversible Watermarking, Least Significant Bit (LSB), Difference Expansion (DE), Reversible Contrast Mapping (RCM), Wavelet-Fuzzy (WF).

INTRODUCTION

A digital watermark is a kind of marker covertly embedded in a noise-tolerant such as an audio, video or image data. It is typically used to identify ownership of the copyright of such images. Watermarking is the process of hiding digital information. Digital watermarks may be used to verify the authenticity or integrity to show the identity of its owners. It is prominently used for tracing copyright infringements and for banknote authentication [1]. Traditional Watermarks may be applied to visible media (like images or video), whereas in digital watermarking, the data may be audio, pictures, video, texts or 3D models. For marking media files with copyright information, a digital watermark has to be rather robust against modifications. Instead, if integrity has to be ensured, a fragile watermark would be applied. Digital watermarking tries to control the robustness as top priority.

Digital watermarking techniques have been indicated so far as a possible solution when, in a specific application scenario (Authentication, Copyright Protection, Finger printing, etc.), there is the need to embed an informative message in a digital document in an imperceptible way. Such a goal is basically achieved by performing a slight modification to the original data trying to, at the same time; satisfy other bindings such as capacity and robustness. The watermarked content is different from the original one. This means that any successive assertion, usage, and evaluation must happen on a, though weakly, corrupted version, if original data have not been stored and are not readily available. It is now clear that the dependence of the application scenario, this cannot always be accepted. The watermarking process is zero-impact, but allows at the same time, to convey an informative message. Watermarking can be classified as either Visible Watermarking or Invisible Watermarking.

1. Reversible Watermarking Techniques

Reversible watermarking techniques are also named as invertible or lossless and were born to be applied mainly in scenarios where the authenticity of a digital image has to be granted and the original content is peremptorily needed on the decoding side. It is important to point out that, initially, a high perceptual quality of the watermarked image was not a requirement due to the fact that the original one was recoverable and simple problems of overflow and underflow caused by the watermarking process were not taken into account too. Successively also, this aspect has been considered as basic to permit to the end user to operate on the watermarked image and to possibly decide to resort to the uncorrupted version in a second time if needed. Reversible techniques can be subdivided into two main categories, as evidenced in fragile and semi fragile [2]. Most of the developed techniques belong to the family of fragile that means that the inserted watermark disappears when a modification has occurred to the watermarked image, thus revealing that data integrity has been compromised. The goals of the reversible watermarking are to protect the copyrights and recover the original image. The robustness, imperceptibility, higher embedding capacity, effectiveness, payload capacity, visual quality and the security are the basic criterion of the reversible watermarking [3]. The reversible watermarking is especially suitable for the applications that require high quality images such as medical and military images. Reversible watermarking is also useful in Remote Sensing, Multimedia Archive Management, and Law Enforcement etc.

2. Literature Survey

A very high capacity algorithm based on the difference expansion of vectors of an arbitrary size has been developed for embedding a reversible watermark with low image distortion. A reversible watermarking algorithm with very high data-hiding capacity has been developed for color images. The algorithm allows the watermarking process to be reversed, which restores the exact original image. The algorithm hides several bits in the difference expansion of vectors of adjacent pixels. The required general reversible integer transform and the necessary conditions to avoid underflow and overflow are derived for any vector of arbitrary length. Also, the potential payload size that can be embedded into a host image is discussed, and a feedback system for controlling this size is developed. These results indicate that the spatial, quad-based algorithm allows for hiding the largest payload at the highest signal-to-noise ratio [1].

Reversible watermarking enables the embedding of useful information in a host signal without any loss of host information. Difference-expansion technique is a high-capacity, reversible method for data embedding. However, the method suffers from undesirable distortion at low embedding capacities and lack of capacity control due to the need for embedding a location map. A histogram shifting technique as an alternative to embedding the location map is proposed. The proposed technique improves the distortion performance at low embedding capacities and mitigates the capacity control problem. This paper proposed a reversible data-embedding technique called prediction-error expansion. This new technique better exploits the correlation inherent in the neighborhood of a pixel than the difference-expansion scheme. Prediction-error expansion and histogram shifting combine to form an effective method for data embedding. The experimental results for many standard test images show that prediction-error expansion doubles the maximum embedding capacity when compared to difference expansion. There is also a significant improvement in the quality of the watermarked image, especially at moderate embedding capacities [2].

Reversible Contrast Mapping (RCM) is a simple integer transform that applies to pairs of pixels. For some pairs of pixels, RCM is invertible, even if the Least Significant Bits (LSBs) of the transformed pixels are lost. The data space occupied by the LSBs is suitable for data hiding. The embedded information bit-rates of the proposed spatial domain reversible watermarking scheme are close to the highest bit-rates reported so far. The scheme does not need additional data compression, and, in terms of mathematical complexity, it appears to be the lowest complexity one proposed up to now. A very fast lookup table implementation is proposed. Robustness against cropping can be ensured as well [3].

Three basic techniques were introduced for reversible watermarking of digital images, as well as touching on the limitations and possibilities of each. The three are analyzed and compared based on MSE, PSNR and processing time and the result shows that the LSB method is the best and simple technique as compared to the other two techniques because the higher the PSNR, the better the quality of the reconstructed image obtained [4].

This paper presents a novel hardware architecture for watermarking unit which can be used with the JPEG2000 compression standard. This paper presents dual watermark detection which is also a novelty of the proposed algorithm. Hardware assisted watermarking offers advantages over the software implementations in terms of less area, power consumption, and real time. Watermarking using Fuzzy logic is performed. The objective is to develop real time, low cost and robust watermarking hardware, which can be incorporated with existing systems such as digital camera [5].

The result of the quantitative analysis helps us to prove that Least Significant Bit algorithm will boost the capacity of the scheme and provide reversibility, fragility for the transmitting secret data [6].

In this paper, a novel digital watermarking scheme was proposed in DCT domain based fuzzy inference system and the human visual system to adapt the embedding strength of different blocks. Firstly, the original image is divided into some 8\times 8 blocks, and then fuzzy inference system according to different textural features and luminance of each block decide adaptively different embedding strengths. The watermark detection adopts correlation technology. Experimental results show that the proposed scheme has good imperceptibility and high robustness to common image processing operators [7].

3. Techniques

3.1 Least Significant Bit (LSB)

The LSB scheme is based on pixel values; the process is simple to follow and uses binary values of the image to hide the secret image [6]. The LSB technique works by replacing some of the information in a given pixel with information from the data in the image. While it is possible to embed data into an image on any bit-plane, LSB embedding is performed on the Least Significant Bit(s) [8].

The steps followed in LSB image watermarking are:

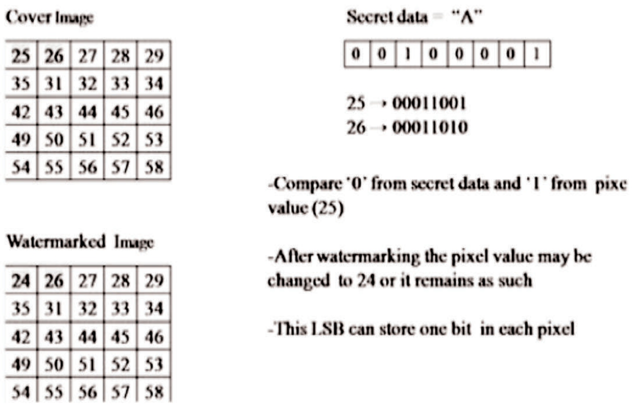
- Select cover image.
- Select information type for secret data as image or text.
- Convert image pixels into binary values.
- Hide the information in the LSB bit of the image using the parameter that results in high value.
- Repeat the steps until image or text is hidden in image.

After getting the watermarked image, we need to create a matrix initialized with zeros, whose dimension is equal to the watermarked image. By XOR-ing each and every pixel of both the original and watermarked image, the result will be stored in the corresponding position in the newly created matrix. This matrix will also be sent to the extraction phase along with the watermarked image. During extraction, the value of the newly created matrix will be checked. If it is 1, then watermarked images LSB of each pixel must be changed, else vice versa.

Figure 1 shows the 1-bit LSB which can store 1-bit in each pixel. If the cover image size is 256 x256 pixel image, it can thus store a total amount of 65,536 bits or 8,192 bytes of embedded data.

3.2 Difference Expansion (DE)

Difference expansion explores the redundancy in digital



Cover Image

25	26	27	28	29
35	31	32	33	34
42	43	44	45	46
49	50	51	52	53
54	55	56	57	58

Secret data = "A"

0	0	1	0	0	0	0	1

25 → 00011001
26 → 00011010

-Compare '0' from secret data and '1' from pixe value (25)

Watermarked Image

24	26	27	28	29
35	31	32	33	34
42	43	44	45	46
49	50	51	52	53
54	55	56	57	58

-After watermarking the pixel value may be changed to 24 or it remains as such

-This LSB can store one bit in each pixel

Figure 1. LSB Example

images to achieve very high embedding capacity and keep the distortion low. The difference expansion scheme is based on an integer transform defined on groups of two pixels. One bit of information is inserted into each transformed pixel pair, and then the inverse transform is performed. A location map is necessary to identify the pairs of pixels, where information was inserted. This scheme usually generates some small values to represent the features of the original image. Then, the authors expand (enlarge) the generated values to embed the bits of watermark information. The watermark information is usually embedded in the LSB parts of the expanded value. Then the watermark image is reconstructed by using the modified values [8].

The steps are:

1. Take two adjacent pixel values x and y.
2. Find average and difference values of pixels.

$$a = \frac{x+y}{2} \qquad (1)$$

$$d = x\text{-}y \qquad (2)$$

3. Then we expand d into its binary form and add watermark bit w right most significant bit to get d.
4. Reconstruct the image using a and d, we get the watermarked image.

The similar process is required to be followed for the lossless recovery of the original image and the watermark.

3.3 Reversible Contrast Mapping (RCM)

Reversible Contrast Mapping (RCM) provides high data embedding bit-rate at a low mathematical complexity. The RCM scheme is based on a simple integer transform defined on pairs of pixels. RCM is perfectly invertible, even if the Least Significant Bits (LSBs) of the transformed pixels are lost. The data space occupied by the LSBs is suitable for data hiding. The basic RCM watermarking scheme was introduced in which a modified version that allows robustness against cropping is proposed [4]. The control of distortions introduced by the watermarking is investigated as well. The mathematical complexity of the RCM watermarking is further analyzed, and a very low cost implementation is proposed [8].

Marking: The marking proceeds as follows:

1) Partition the entire image into pairs of pixels (for instance, on rows, on columns, or on any space filling curve).

2) For each pair (x,y)

a) If (x,y) $\in D_c$ and if it is not composed of odd pixel values, transform the pair using equation (3), set the LSB of x' to "1," and consider the LSB of y'as available for data embedding.

$$x' = 2x\text{-}y,\ y' = 2y\text{-}x \qquad (3)$$

b) If (x,y) $\in D_c$ and if it is composed of odd pixel values, set the LSB of x to "0," and consider the LSB of y as available for data embedding.

c) If (x,y) $\in D_c$, set the LSB of x to "0," and save the true value.

3) Mark the image by simply overwriting the bits of the watermark.

A different marking procedure is used in which a map of transforming pairs and the sequence of LSBs for all non transformed pairs are first collected. Then, the entire image LSB plane is overwritten by the payload and by the collected bit sequences. The slightly modified procedure was proposed, which provides robustness against cropping. The location map of the entire image is replaced by the LSB of the first pixel of each pair showing if the pair was transformed or not. Let us further consider that the saved LSB of a non transformed pair is embedded into the available LSB of the closest transformed pair. Thus, all the information needed to recover any original pixel pair is embedded into the pair itself or very close to it. In the case of cropping, except for the borders where some errors may appear, the original pixels of the cropped image are exactly recovered together with the embedded payload. For pixel pairing on a row or column direction, there are no problems of synchronization. Some control codes should be inserted in the payload to validate watermark integrity.

3.3.1 Detection and Original Recovery

Watermark extraction and exact recovery of the original image is performed as follows [8]:

1) Partition the entire image into pairs of pixels.

2) For each pair

a) If the LSB x' is"1," extract the LSB y' and store it into the detected watermark sequence, set the LSBs of x', y' to "0," and recover the original pair by inverse transform.

b) If the LSB x' is "0" and the pair with the LSBs set to "1" belongs to domain transform without the ambiguous odd pixel pairs, extract the LSB y', store it into the detected watermark sequence, and restore the original pair as with the LSBs set to "1".

c) If the LSB x' is "0" and the pair with the LSBs set to "1" does not belong to domain transform without the ambiguous odd pixel pairs, the original pair is recovered by replacing the LSB of x' with the corresponding true value extracted from the watermark sequence. MSE and PSNR are calculated to compare the results with the existing approaches.

3.4 Fuzzy Interface System (FIS)

This block is used to calculate the local variance of the image block. The calculated variance is fed to the FIS. Each input is composed of three membership functions minimum, medium, maximum based on the variance distributed among smooth, slightly rough and rough subsets, respectively [7]. The output of the FIS is the gain factor for the particular block. This gain is based on the three membership functions. It is important to realize that this approach enables adjustment of gain so as to best fit the image properties.

In order to calculate and correct the amount of gain for a particular block, the fuzzy rules [5] are given.

The following simple fuzzy rules are given below.

1. If the image block is smooth (low variance), then the gain is minimum.
2. If the image block is slightly rough (medium variance), then the gain is medium.
3. If the image block is rough (high variance), then the gain is maximum.

D is calculated for the composite output set using a weighted average Defuzzification method given by using equation.

$$D = \frac{\sum z_j c_j}{\sum z_j} \qquad (4)$$

Where c_j is center of the consequent set of rules j, and z_j is the extent to which rule is fired. Figure 2 shows the graph of block number V_s gain and variance. The weighted average method requires simple calculations and it requires less hardware. It can be observed from the graph that gain varies according to the variance of the block.

4. Performance Metrices

4.1 Mean Squared Error (MSE)

The simplest, oldest and most widely used technique to quantify image quality is the Mean Squared Error (MSE). Mathematically it is defined as [8]:

$$\text{MSE} = \frac{1}{\text{MN}} \sum_{i=0}^{M-1} \sum_{j=0}^{N-1} (u - v)^2 \qquad (5)$$

Where, two images u and v having size M×N, one of them is the noisy (watermarked) approximation of the original one.

Mean Squared Error (MSE) or Mean Squared Deviation (MSD) of an + measures the average of the squares of the errors or deviations, that is, the difference between the estimator and what is estimated. MSE is a risk function, corresponding to the expected value of the squared error loss or quadratic loss. The difference occurs because of randomness or because the estimator doesn't account for information that could produce a more accurate estimate.

The MSE is the second moment (about the origin) of the error, and thus incorporates both the variance of the estimator and its bias. For an unbiased estimator, the MSE is the variance of the estimator. Like the variance, MSE has the same units of measurement as the square of the

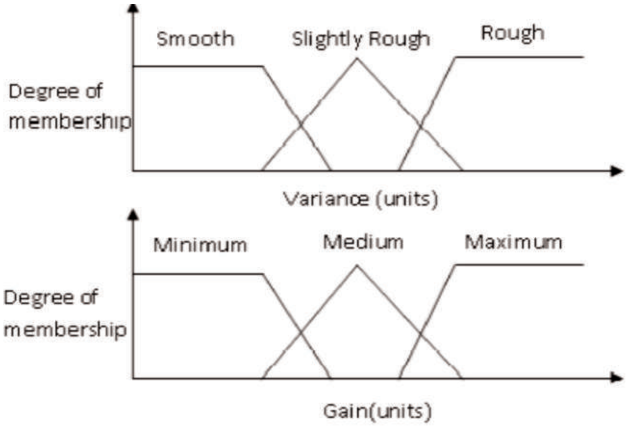


Figure 2. Fuzzy Membership Function

quantity being estimated.

4.2 Peak Signal-to Noise Ratio (PSNR)

It is used to quantify the visual distortion made by watermarking process as well as different attack operations. The PSNR is a popular index term to evaluate the difference between the pre-processing image and the post-processing image [8]. Mathematically for an 8 bit gray scale image it is defined as:

$$PSNR = 10 log_{10} \frac{255^2}{MSE} \qquad (6)$$

PSNR is usually expressed in terms of the logarithmic decibel scale. PSNR is most commonly used to measure the quality of reconstruction of lossy compression codes (e.g., for image compression). The signal in this case is the original data, and the noise is the error introduced by compression. When comparing compression codes, PSNR is an approximation to human perception of reconstruction quality. Although a higher PSNR generally indicates that the reconstruction is of higher quality, in some cases it may not. One has to be extremely careful with the range of validity of this metric; it is only conclusively valid when it is used to compare results from the same codec and same content.

4.3 Correlation

The correlation factor measures the similarity between the original watermark and the extracted watermark from the image (robustness). The correlation factor may take the values between 0 (random relationship) to 1 (perfect linear relationship).

$$\rho = \frac{x}{row \cdot column} \qquad (7)$$

Where, $X = \Sigma^{N}_{i=1} (W_i * B_i)$

W = Watermarked Image, B = Secret Image.

5. Performance Evaluation

To know the working of the project, the performance evaluation is calculated. For this the values are plotted in Tables 1 and 2.

Techniques	MSE	PSNR	Processing Time	Correlation
LSB	0.4983	51.1561	Very Low	-0.0780
DE	0.501	51.1326	Low	0.8510
RCM	8.0947	9.0488	High	0.0968
WF	1.4118	6.6136	Very High	0.9789

Table 1. Performance Evaluation of Recovered Image

Techniques	MSE	PSNR
LSB	5.8475	10.4611
DE	24.1610	27.1910
RCM	8.1166	9.0371
WF	1.418	36.6136

Table 2. Performance Evaluation of Recovered Image after applying Median Filter

Conclusion

In this work, four basic techniques for Reversible Watermarking of digital images, namely Least Significant Bit, Difference Expansion, Reversible Contrast Mapping, Wavelet Fuzzy are compared, as well as touching on the limitations and possibilities of each. The four types are analyzed and compared based on Performance Metrics such as MSE, PSNR, Processing Time and Correlation and the result shows that the LSB method is the best and simple technique as compared to the other three techniques because the higher the PSNR, the better the quality of the reconstructed image is obtained and less processing time. Based on correlation and after applying a median filter, Wavelet-Fuzzy provides better results than other techniques.

Future Scope

In future, these methods can be improved by increasing the payload, visual quality, and security. To overcome various limitations of existing techniques, the Human Visual System (HVS) can be considered while embedding the secret information, in order to increase the PSNR as high as possible.

References

[1]. **Alattar, Adnan M. (2004).** "Reversible watermark using the difference expansion of a generalized integer transform". *IEEE Transactions on Image Processing,* Vol. 13, No. 8, pp. 1147-1156.

[2]. **Thodi, Diljith M., and Jeffrey J. Rodríguez, (2007).** "Expansion embedding techniques for reversible watermarking". *IEEE Transactions on Image Processing,* Vol. 16, No. 3, pp. 721-730.

[3]. **D. Coltuc, and J. M. Chassery, (2007).** "Very fast watermarking by reversible contrast mapping". *IEEE Signal Process. Lett.,* Vol. 14, No. 4, pp. 255-258.

[4]. **Patanwar, Abhishek, and Shikha Singh, (2015).** "A Comparative Study of Reversible Watermarking Techniques". *International Journal of Advanced Research in Computer and Communication Engineering,* Vol. 4, No. 4.

[5]. **Lande, Pankaj U., Sanjay N. Talbar, and G. N. Shinde, (2010).** "Robust image adaptive watermarking using fuzzy logic an FPGA approach". *International Journal of Signal Processing, Image Processing and Pattern Recognition,* Vol. 3, No. 4, pp. 43-54.

[6]. **Arthi, R., V. Jaganya, and S. Poonkuntran, (2012).** "Modified LSB watermarking for image authentication". *International Journal of Communication Technology,* Vol. 3, No. 3, pp. 2231-0371.0.

[7]. **Oueslati, Sameh, Adnane Cherif, and Bassel Solaiman, (2010).** "Maximizing strength of digital watermarks using fuzzy logic". *Signal and Image Processing: An International Journal (SIPIJ),* Vol. 1, No. 2, pp. 112-124.

[8]. **Abhishek Patanwar, and Shikha Singh, (2015).** "A Comparative Study of Reversible Watermarking Techniques". *International Journal of Advanced Research in Computer and Communication Engineering,* Vol. 4, No. 4.

ABOUT THE AUTHORS

V. Belmer Gladson is presently pursuing his Ph.D in the specialization of Image Processing in MS University, Tirunelveli, TamilNadu, India. He has received his Diploma in Information Technology from CSI Polytechnic College, Salem, Bachelor of Engineering Degree in Computer Science & Engineering from Vins Christian College, and Master of Engineering Degree in Computer Science & Engineering from M S University, Tirunelveli. His areas of interests are Computer Networks and Digital Image Processing.

Y. Sam Josuva is presently working as an Assistant Professor in M S University, Tirunelveli, TamilNadu, India. He has received his Diploma in Electrical & Electronics & Engineering from JACSI Polytechnic, TamilNadu, Bachelor of Engineering Degree in Computer science & Engineering from Madras Institute of Technology, Chennai and Master of Engineering Degree in Computer Science & Engineering from M S University, Tirunelveli. His areas of interests are Computer Networks and Digital Image Processing.

Dr. R. Balasubramanian is currently working as a Professor in the Department of Computer Science & Engineering at Manonmaniam Sundaranar University, Tirunelveli, TamilNadu, India. He received his B.E [Hons] in Computer Science & Engineering from Bharathidhasan University and M.E in Computer Science & Engineering from Regional Engineering College, Bharathidhasan University, Tirunelveli. He received his Doctorate in Computer Science & Engineering from Manonmaniam Sundaranar University, Tirunelveli. He has published many papers in various National and International level Journals and Conferences. His research interests are in the field of Digital Image Processing, Data Mining, and Wireless Networks.