A Gray Scale High Quality Digital Image Watermarking using Equal Pixel Value Difference Method (EPVD)

Sonia
M.Tech Student
G.Z.S.P.T.U.Campus
Punjab, India

Naresh Kumar Garg
Assistant Prof.
G.Z.S.P.T.U.Campus
Punjab, India

Gurvinder Singh
Assistant Prof.
G.T.B.K.I.E.T
Punjab, India

ABSTRACT

Due to growth of Internet and multimedia technologies in today's life, it made easy to copy and distribution of any document without any owner's consent. Watermarking is a process of concealing the digital information in a document for providing the ownership on his/her document. To increase security of ownership of a document and to improve quality of indistinguishable watermarked image from host image, a new watermarking approach equal pixel value difference method is proposed in this paper during embedding and extraction process. This method provides equal differences between pixels of watermarked image and host image placed at same pixel position which improves the quality of watermarked image. The experimental results show watermarked images with good robustness and Imperceptibility.

General Terms

Security, Watermarking, Embedding, Extraction.

Keywords

Host Image, Watermarked Image, Even/odd positioned pixel difference.

1. INTRODUCTION

Internet and multimedia applications are used in enormous amount recently. Due to this digital data can be easily copied, tampered and distributed. In this way, there is duplication, distribution and editing of digital data in huge amount without owner's permission [6]. Hence, the copyright protection for digital contents such as images, audio and video is one of the major issues. The new technology used for protecting copyrights of digital contents is Digital Watermarking [1]. Digital watermarking is defined as the method of embedding a certain part of information (technically known as watermark) into multimedia content including text documents, images, audio or video streams [3]. Certifiable information like owner's identity, name, company logo, etc is contained in digital Watermark. Watermark can be extracted later to know about host media [2]. The watermarking system can be categorized into three forms as Embedding, Attacks and Extraction. In embedding, the digital watermark is inserted into cover image with the help of embedding algorithm. This generates a watermarked image which is transferred to an authorized person. If any unauthorized person attempts to change the image then this is called an attack. There are many possible alterations, for example, lossy compression of the data, cropping an image or video or intentionally adding noise. In extraction, decoding algorithms are used to detect the watermark from watermarked image [7].

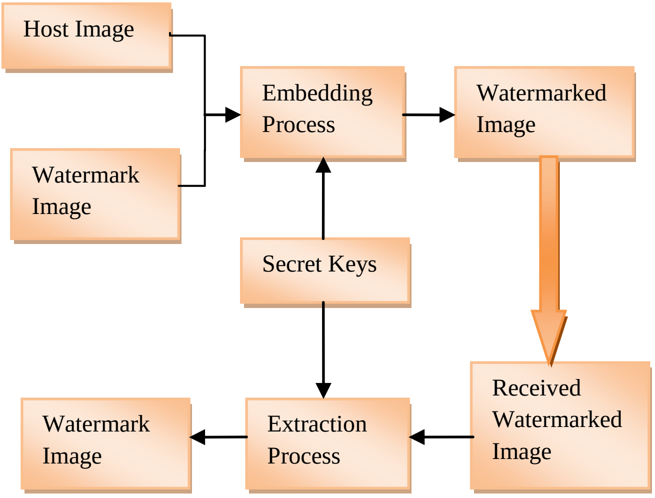

Figure 1: Watermarking Embedding and Extraction Process

A watermark should possess following characteristics to be efficient [7]:-

- ***a)*** **Unobtrusive**:-The watermark should not be visible.
- ***b)*** **Robust**:-The watermark needs to be difficult to remove if there is incomplete knowledge.
- ***c)*** **Universal**:-The same digital watermarking algorithm can be implemented. It will be helpful in watermarking of multimedia products.
- ***d)*** **Unambiguous**:-The retrieved watermark should identify the owner without any ambiguity.

2. REVIEW OF PVD METHOD

Pixel Value Difference (PVD) method [4] is made for Steganographic images. In this method, a cover image that is in gray scale is used for hiding the confidential information. The cover image is partitioned into small non-overlapping segments consisting of two consecutive pixels like P_i and P_{i+1} for embedding the information. The difference value of these pixels is given as df $=P_{(i)}-P_{(i+1)}$. These difference values lie in the range of -255 to 255. The magnitudes of these difference values are represented by |df| which lie in the range of 0 to 255. The large difference segments located in an edge area and large amount of data can be embedded here. On the other side, the small difference segments located in a smooth area and less secret data can be hidden. The human eyes can endure more changes in sharp edge area than smooth area according to property of human vision. Therefore, a range table has been constructed with m contiguous ranges R_n

(where n=1, 2, 3...m) where range is from 0 to 255.The lower boundary and upper boundary are denoted by L_n and U_n respectively then $R_n \in [L_n , U_n]$.
The width of R_n is computed as:

$$TH_n = U_n – L_n+1$$

Here width TH_n tells about total number of bits which can embed in a segment. Range Table 1 is used during embedding as well as in extraction process.

Table 1: Range Table [4][19]

Range	**L_n**	**U_n**	**TH_n**	**B=log(TH_n)**
0 – 7	0	7	8	3
8 – 15	8	15	8	3
16 – 31	16	31	16	4
32 – 63	32	63	32	5
64 – 127	64	127	64	6
128-255	128	255	128	7

The embedding algorithm [4] [6] is given as

- Calculate the difference value of two consecutive pixels from each segment. $df_j=|P_{(j)}-P_{(j+1)}|$
- Find the optimal range in which difference lies in range table as $R_j =\min (U_n - df_j)$ where $U_n \geq df_j$ for all $1 \leq n \leq m$.
- Calculate the number of bits 'B' according to which 'B' bits of data are carried for embedding in a segment as B=log(TH_n)
- Choose 'B' bits from binary stream of original data and convert it into decimal number 'd'.
- Compute the new difference 'Ndf' as

$$Ndf = L_n + d$$

- Change the values of $P_{(i)}$ and $P_{(i+1)}$ as below:

$$P'_{(i)} \text{ and } P'_{(i+1)} = (P_{(i)} +M/2 , P_{(i+1)} -M/2)$$

$$\text{if } P_{(i)} > P_{(i+1)} \text{ and } Ndf > df$$

$$P'_{(i)} \text{ and } P'_{(i+1)} = (P_{(i)} -M/2 , P_{(i+1)} +M/2)$$

$$\text{if } P_{(i)} < P_{(i+1)} \text{ and } Ndf > df$$

$$P'_{(i)} \text{ and } P'_{(i+1)} = (P_{(i)} -M/2 , P_{(i+1)} +M/2)$$

$$\text{if } P_{(i)} > P_{(i+1)} \text{ and } Ndf < df$$

$$P'_{(i)} \text{ and } P'_{(i+1)} = (P_{(i)} +M/2 , P_{(i+1)} -M/2)$$

$$\text{if } P_{(i)} < P_{(i+1)} \text{ and } Ndf < df$$

Where M=|Ndf– df |. $P'_{(i)}$ and $P'_{(i+1)}$ are new pixel values after embedding the data. Repeat these all steps for embedding the whole information. Original PVD range table is required for extracting the embedded bits from Stego-Image. The Stego-Image is partitioned into segments as doing in embedding process. Then calculate the magnitude difference between $P'_{(i)}$ and $P'_{(i+1)}$.Now find the optimum range in which magnitude difference lies. Then d' is obtained by subtracting L_n from magnitude difference. df' is converted into its binary equivalent. These binary equivalent bits are the secret data obtained from the pixel segment ($P'_{(i)}$, $P'_{(i+1)}$).

3. ALGORITHM

3.1 Encoding:

- Choose original watermark image having dimensions of 32 * 32 in size.
- Now partitioned the entire image into small parts in form of segments of 2 * 2 in dimensions.
- Retrieve each pixel from small parts for converting into its corresponding binary equivalent.
- Select the random keys having 8 bits binary equivalent for encrypting the entire image.
- Encrypt all pixels of image with selected random keys using XOR operation resulting in encrypted bits.
- For embedding all encrypted bits of watermark image, choose a gray scale image as a host image having size of 256 * 256 in dimensions.
- Calculate the difference between even/odd pixels of a segment constructing by segmentation process applied on host image such as (Z_i & Z_{i+2} / Z_j & Z_{j+2}) i=1 and j=2

$$\text{If } Z_i > Z_{i+2} \;\; \& \;\; Z_j > Z_{j+2}$$

$$df_i=| Z_i- Z_{i+2} | \text{ and } df_j=| Z_j- Z_{j+2} |$$

$$\text{If } Z_i < Z_{i+2} \;\; \& \;\; Z_j < Z_{j+2}$$

$$df_i=| Z_{i+2} - Z_i | \text{ and } df_j=| Z_{j+2} - Z_j |$$

$$\text{If } Z_i > Z_{i+2} \;\; \& \;\; Z_j < Z_{j+2}$$

$$df_i=| Z_i - Z_{i+2} | \text{ and } df_j=| Z_{j+2} - Z_j |$$

$$\text{If } Z_i< Z_{i+2} \;\; \& \;\; Z_j> Z_{j+2}$$

$$df_i=| Z_{i+2} - Z_i | \text{ and } df_j=| Z_j- Z_{j+2}|$$

$$NZ_i = Z_i+ df_i \quad \text{and} \quad NZ_{i+2} = Z_{i+2} +df_i$$
$$NZ_j = Z_j + df_j \quad \text{and} \quad NZ_{j+2} = Z_{j+2} + df_j$$

- Compute the both new even/odd pixel difference of each new segments as

$$DF_k=| NZ_{(i/j)} – NZ_{(i+2/j+2)} |$$

- Observe range of new even/odd pixel difference from the PVD original range table in which difference lies.
- Calculate the number of encrypted data bits ‘B’ to be embedded into new even/odd pixel pairs from the width TH_n optimum range, this can be defined as $B=\log_2 TH_n$.
- Choose encrypted data bits of original watermark image according to computed width of range and convert it into its corresponding decimal number.
- Calculate new difference NDF with adding of decimal number to lower range.
- Calculating the magnitude difference between NDF and DF for finding the value of M.
- Calculating the M/2.

a.) If M/2 is integer

$NZ_i' = NZ_i - M/2$ and

$NZ_{i+2}' = NZ_{i+2} - M/2$

b.) If M/2 is float then the integer part ‘i’ of M/2 is subtracted from pixel NZ and float part of M/2 is discarded as

$NZ_j' = NZ_j - i$ and

$NZ_{j+2}' = NZ_{j+2} - i$

- The above ‘a’ and ‘b' part generates pixel differences between all pixels of host image which are equal to pixel differences generated by pixels of watermarked image at same pixel position.

- After embedding the complete encrypted data bits, construct the watermarked image by reconstructing all new embedded segments in a matrix of size of 256 * 256.

3.2 Extraction:

- Receive the watermarked image through any channel.
- Divide the watermarked image into small parts in form of segments of 2 * 2 in dimensions.
- Calculate the difference between even/odd pixels (NZ_i' & NZ_{i+2}' / NZ_j' & NZ_{j+2}') of each segment.
- Find range of even/odd pixel difference from the range table in which the difference lies.
- Add even/odd pixel difference with ‘M’ for getting new difference and subtract from low range for extracting encrypted data bits. Here M values are used for extracting the encrypted data as keys.
- Now compute the original binary equivalents using XOR operation between extracted encrypting data and random keys used in embedding process.
- Convert all binary equivalents into decimal numbers.
- Rearranging all decimal numbers as pixels into segments of size of 2 * 2.
- Reconstruct the watermark image after combining the all segments in a matrix of size of 32 * 32.

Host Images **Watermark Images** **Watermarked Images**

Butterfly:

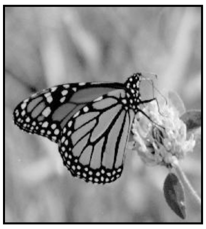

Figure 2 [16]

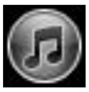

Figure 3 [8]

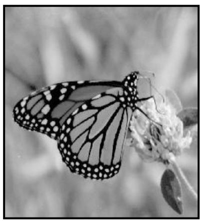

Figure 4

Old-Man:

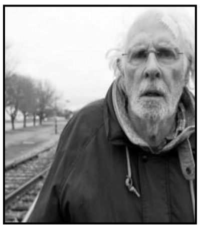

Figure 5 [10]

Figure 6 [8]

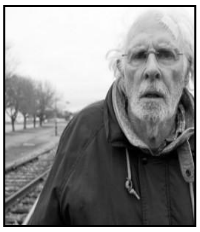

Figure 7

Home:

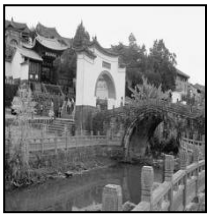

Figure 8 [13]

Figure 9 [8]

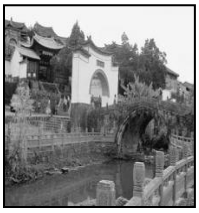

Figure 10

Cameraman:

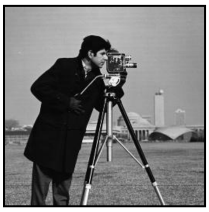

Figure 11 [11]

Figure 12 [8]

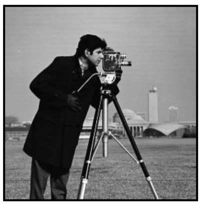

Figure 13

Bridge:

Figure 14 [17]

Figure 15 [8]

Figure 16

Bird:

Figure 17 [14]

Figure 18 [8]

Figure 19

Table 2: Experiment Results of Proposed Method

S. No.	Host Image	PSNR	MSE
1.	Butter-Fly	57.4082	0.3437
2.	Old-Man	57.0265	0.3591
3.	Home	55.1302	0.4467
4.	Cameraman	54.4419	0.4836
5.	Bridge	54.1743	0.4987
6.	Bird	50.5615	0.7559

4. EXPERIMENT GRAPHS

4.1 PSNR Graph:

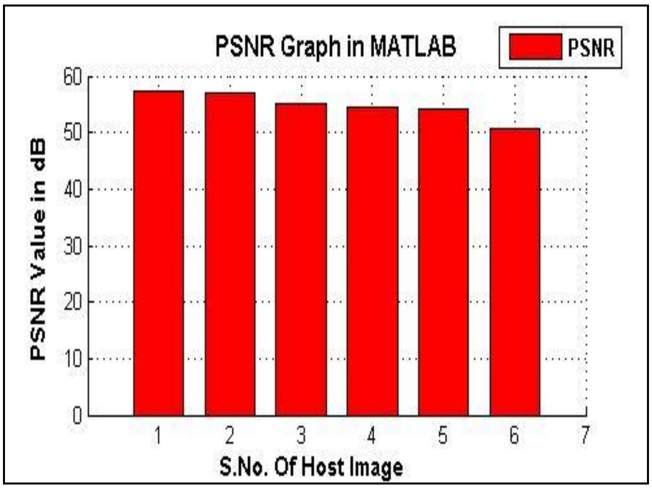

Figure 20: PSNR Graph (1. Butterfly 2.Old man 3.Home 4. Cameraman 5. Bridge 6.Bird)

4.2 MSE Graph:

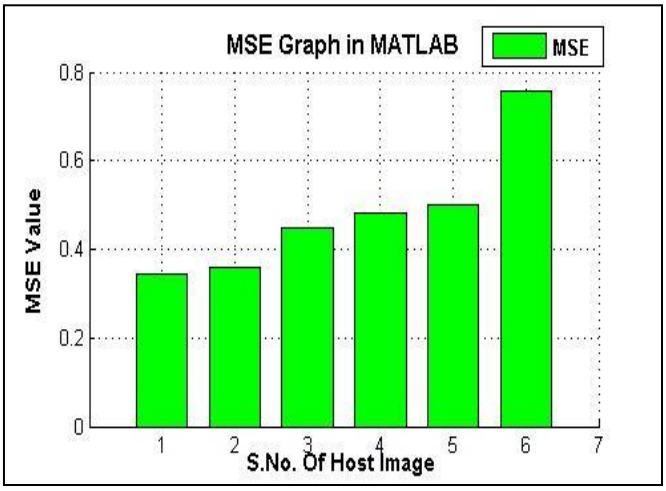

Figure 21: MSE Graph (1.Butterfly 2.Old man 3.Home 4.Cameraman 5. Bridge 6.Bird)

5. CONCLUSION

In this paper, a method is proposed which works on gray scale image to conceal the watermark image for providing more protection of ownership of owner's digital image or document. This proposed method generates pixel differences between all pixels of host image which are equal to pixel differences generated by pixels of watermarked image at same pixel position. This provides good robustness and imperceptibility to digital image after embedding watermark image. The encryption of each pixel of original watermark image with random keys is hidden in a gray scale host image of 256 * 256 without any data compression and extract with proposed method. Experimental results show watermarked images with good robustness and Imperceptibility.

6. REFERENCES

[1] Singh, D., Choudhary, N., Agrawal, M. “Spatial and Frequency Domain for Grey level Digital Images”, Special Issue of International Journal of Computer Applications (0975–8887) on Communication Security, No.4, pp.16-20, Mar. 2012.

[2] Aggarwal, A., Singla, M. “Image Watermarking Techniques in Spatial Domain: A Review”, International Journal of Computer Technology and Applications, vol.2 (5), pp. 1357–1363, ISSN: 2229-6093, Sept-Oct, 2011.

[3] Singh, S. P. , Agrawal, S. “A Literature Review on Water Marking Techniques”, International Journal of Scientific Engineering and Technology, Volume No.1, Issue No.4, pp: 21-23, ISSN: 2277-1581, Oct. 2012.

[4] Wu, D.C. and Tsai, W.H. “A Steganographic method for images by pixel- value differencing”, Pattern Recognition Letters, Vol. 24, pp. 1613-1626, 2003.

[5] Madane, A. R. , Talele, K. T., Shah, M. M. “Watermark Logo in Digital Image using DWT”, Proceedings of SPIT-IEEE Colloquium and International Conference, Mumbai, India, Vol. 1, pp.121-127.

[6] Mandal, J. K., Das, D. "Steganography Using Adaptive Pixel Value Differencing (APVD) of Gray Images Through Exclusion of Overflow/Underflow ", CCSEA, SEA, CLOUD, DKMP, CS & IT 05, pp. 93–102, 2012.

[7] http://en.wikipedia.org/wiki/Digital_watermarking.

[8] http://cache.filehippo.com/img/ex/1906__iTunes_icon.png.

[9] Er. Sonia, Er. Garg, N. K. “An Efficient Digital Image Watermarking Using Diagonal Pixel Value Difference Method”, International Journal of Advanced Research in Computer Engineering & Technology , Volume 3, Issue 5, May 2014.

[10] www.cinephiled.com/wp-content/uploads/2013/12/nebraska_0-560x315-256x256.jpg

[11] www.josephsalmon.eu/images/cameraman.png.

[12] Yusof Y. and Khalifa O.O.. “Digital Watermarking For Digital Images Using Wavelet Transform”, Proceedings of the 2007 IEEE International Conference on Telecommunications andMalaysia International Conference on Communications, 14-17 May 2007, Penang, Malaysia.

[13] www.ynly118.com/travel/UploadFiles_7937/201306/2013062516420239.jpg.

[14] www.ee.columbia.edu/~sfchang/course/dip-S04/demos/homework3.html

[15] Madane A.R., Talele K T. and Shah M. M.,” Watermark Logo in Digital Image using DWT”, Proceedings of SPIT-IEEE Colloquium and International Conference, Mumbai, India.

[16] www.en.pudn.com/downloads137/sourcecode/graph/texture_mapping/detail586610_en.html.

[17] http://user.engineering.uiowa.edu/~dip/examples/images/sf.jpg.

[18] S.Dharm, Choudhary N., Agrawal M., “Spatial and Frequency Domain for Grey level Digital Images “Special Issue of International Journal of Computer Applications (0975 – 8887) on Communication Security, No.4. Mar.2012.

[19] Maruthuperumal S., Dr. V.Vijayakumar & Vijayakumar B., “Sorted Pixel Value Difference on Fuzzy Watermarking Scheme” ,Global Journal of Computer Science and Technology, Volume 12, issue 4, version 0.1 Feb 2012.