An Efficient Digital Image Watermarking Using Diagonal Pixel Value Difference Method (DPVD)

Er. Sonia , Er. Naresh Kumar Garg

Abstract— ***Now a days, due to sharp rise in the Internet services, the critical issue of copyright protection of document content increases.Watermarking is a way of providing protection for ownership on owner's document. To enlarge security of copyright protection and to produce indistinguishable watermarked image from original cover image with human eye, a new watermarking approach using diagonally pixel value differencing in a segment during embedding and extraction with a proposed range table is proposed in this paper. The experimental results show that the proposed method is highly efficient for providing more secure ownership on his/her document and also the proposed method is secured against effects of attacks. Besides, the embedded original watermark can be extracted from watermarked image without the assistance of original cover image.***

Index Terms—*Cover image/Host image, Diagonal pixel value difference, Watermark image, Watermarked image*

I. INTRODUCTION

There are internet and multimedia technologies which are used fast in our daily routine [2]. The facility of distribution of multimedia data such as images etc increases due to these technologies [1]. Hence it has become easier to create copy, transmit and distribute digital data without the owner's consent [2]. Digital watermarking proposes a way to handle this serious problem. It may help to determine the authenticity and ownership of a document [1]. A digital watermark is an identification of ownership of any document such as audio file, image, text file etc. Watermarking is a process of concealing the digital information in a document for providing the ownership on his/her document. The digital information is a digital watermark which may be used to verify authenticity or integrity of the document or to show the identity of its owners [6].The image in which digital watermark is to embed is called host or cover image. The watermarking system is divided into three categories: 1. Embedding 2.Attacks 3.Extraction. In embedding, the digital watermark is to embed into cover image with the help of embedding algorithm. This creates a watermarked image which is transmitted to another authorized person through any channel. If any other unauthorized people try to modify the image, this is called an attack. The unauthorized person may attempt to remove the digital watermark through modification. There are many possible modifications, for example, lossy compression of the data, cropping an image or video or intentionally adding noise. In detection, an extraction algorithm is used to extract the watermark from the watermarked image [6].

There are four important factors which are commonly used to determine the quality of watermarking [2].

Robustness: Watermark should be more difficult to eliminate or to detect or to destroy. Robust measures of immunity of watermark against any attempts or modification and manipulation like compression, filtering, rotation, scaling, and collision attacks, resizing, cropping etc.

Imperceptibility: It measures the quality of host image should not be destroyed by implementing of watermark.

Capacity: It measures the capacity of embedding of the majority of information.

Blind Watermarking: Watermarking is extracted from watermarked image without original image due to difficulty of avail the original image.

II. REVIEW OF PVD METHOD

The basic PVD scheme is used for Steganographic images. In PVD method [4] [8], a gray scale image which acts as a cover image is applied for hiding the original information. The cover image is divided into small segments. These segments are non-overlapping segments consisting of two consecutive pixels such as $X_{(i)}$ and $X_{(i+1)}$.The difference value is generated by subtracting these two consecutive pixels as

$$diff_{(j)} = X_{(j)} - X_{(j+1)}$$

This created difference value is represented by '$diff_{(i)}$.' The set of all difference values may lies in range from -255 to 255.The difference magnitude which is denoted by '$| diff_{(i)} |$' ranges from 0 to 255. The segments having small differences locate in smooth area. So less data can be embedded whereas the segments having large differences locate in sharp edged area. Here more data can be embedded. According to properties of human vision, eyes can tolerate more changes in

Er. Sonia,*M.Tech Student, Deptt.of Computer Science &Engg G.Z.S.P.T.U campus,Punjab,India.*
Er. Naresh Kumar Garg, *Assist Prof. Deptt. of Computer Science & Engg., G.Z.S.P.T.U campus,Pumjab,India.*

sharp edge area than smooth area. Therefore, in PVD method, a range table has been constructed with n contiguous ranges R_m (where m=1, 2, 3...n) where range is from 0 to 255.The lower boundary and upper boundary are represented by l_m and u_m respectively then

$$R_m \in [\, l_m \,,\, u_m \,]$$

The width of R_m is computed as

$$W_m = u_m - l_m + 1$$

Here W_m is width of R_m decides how many bits can be embedded in a segment. During extraction, this original range table is required to extract the embedded data from embedded segment.

TABLE 1
ORIGINAL PVD RANGE TABLE

Range	l_m	u_m	W_m	b= log(W_m)
T1=[0-7]	0	7	8	3
T2=[8-15]	8	15	8	3
T3=[16-31]	16	31	16	4
T4=[32-63]	32	63	32	5
T5=[64-127]	64	127	64	6
T6=[128-255]	128	255	128	7

The embedding algorithm[4] is given as

- Find the difference value of two consecutive pixels from each segment.

$$diff_j = | X_{(j)} - X_{(j+1)} |$$

- Find the optimal range in which difference lies in range table as

$$R_m = \min(u_m - diff_j)$$

Where $u_m \geq diff_j$ for all $l \leq m \leq n$.

- Calculate the number of bits 'b' according to which 'b' bits of data are carried for embedding in a segment as

$$b=\log(W_m)$$

- Carry 'b' bits from binary of original data and convert it into decimal number 'D'.
- Compute the new difference '$Ndiff_j$' ' as

$$Ndiff_j = l_m + D$$

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

$$X'_{(j)} \text{ and } X'_{(j+1)} = (X_{(j)} + M/2 \,,\, X_{(j+1)} - M/2) \quad \text{if } X_{(j)} > X_{(j+1)} \text{ and } Ndiff > diff$$

$$X'_{(j)} \text{ and } X'_{(j+1)} = (X_{(j)} - M/2 \,,\, X_{(j+1)} + M/2) \quad \text{if } X_{(j)} < X_{(j+1)} \text{ and } Ndiff > diff$$

$$X'_{(j)} \text{ and } X'_{(j+1)} = (X_{(j)} - M/2 \,,\, X_{(j+1)} + M/2) \quad \text{if } X_{(j)} > X_{(j+1)} \text{ and } Ndiff < diff$$

$$X'_{(j)} \text{ and } X'_{(j+1)} = (X_{(j)} + M/2 \,,\, X_{(j+1)} - M/2) \quad \text{if } X_{(j)} < X_{(j+1)} \text{ and } Ndiff < diff$$

Where M=|Ndiff – diff |. $X'_{(j)}$ and $X'_{(j+1)}$ are new pixel values after embedding the original information bits and repeat these all steps for embedding the entire original information bits.
Original range table is necessity while extracting the embedded bits from Stego-Image. The Stego-Image is divided into segments as doing in embedding process. Then calculate the magnitude difference between $X'_{(j)}$ and $X'_{(j+1)}$.Now find the optimum range R_m in which magnitude difference lies. Then D' is obtained by subtracting l_m from magnitude difference. Convert D' into its binary equivalent. These binary equivalent bits are the hidden secret data obtained from the pixel segment ($X'_{(j)}, X'_{(j+1)}$).

III. PROPOSED WORK

The proposed work is divided into four parts.

A. Encryption Process

B. Embedding Process

C. Extraction Process

D. Decryption Process

A. Encryption Process:

- Take the original watermark image having size of 32 * 32.
- Segmentation of original watermark image into small segments of size of 2 * 2.
- Subtract each pixel of each segment from square of that pixel position of that segment.
- Shift the pixels of each segment diagonally for constructing the new segments.
- Convert the binary equivalent of pixels of each new segment into its gray equivalent.
- Choose the random keys having 8 bits binary equivalent of each character of keys.
- Encrypt the all gray equivalents with all binary equivalents of random keys using XOR operation.

- Convert the all gray bits into nibbles and subtract the decimal value of nibbles from the higher value of selected range in which decimal value

ISSN: 2278 – 1323

lies in following proposed table for encryption process.

TABLE 2
PROPOSED ENCRYPTION RANGE TABLE

Range	Lower Range	Higher Range
0 – 2	0	2
3 – 5	3	5
6 – 7	6	7
8 – 10	8	10
11 – 13	11	13
14 – 15	14	15

B. Embedding Process:

- Take the Cover image having size of 256 * 256 for embedding the watermark image.
- Segmentation of Cover image into small segments of size of 2 * 2 in form of odd and even segments.
- Take odd row pixels of odd segment in first row of new odd segment and place the pixels in second row of new odd segment after interchanging the even row pixels of even segment.
- Take even row pixels of odd segment in first row of new even segment and place the pixels in second row of new even segment after interchanging the odd row pixels of even segment.
- Calculate the both diagonal pixel difference of each odd and even segments as

$$diff_j = | X_{(j)} - X_{(j+2)} |$$

- Find range of diagonal pixel difference from the range table 3 in which the diagonal pixel difference lies as

$$R_m = \min(u_m - diff_j)$$

Where $u_m \geq diff_j$ for all $l \leq m \leq n$.

TABLE 3
RANGE TABLE [5]

Range	l_m	u_m	W_m	$b=\log(W_m)$
0 – 15	0	15	16	4
16 – 31	16	31	16	4
32 – 63	32	63	32	5
64 – 127	64	127	64	6
128 – 255	128	255	128	7

- Compute the width of range where diagonal pixel difference exists as

$$b=\log(W_m)$$

- Choose encrypted bits of original watermark image according to computed width of range and convert it into decimal number D.
- Calculate new difference as

$$Ndiff_j = l_m + D$$

- Calculating the magnitude difference between $Ndiff_j$ and $diff_j$ for finding the value of variable M

$$M = | Ndiff_j - diff_j |$$

- Calculating the M/2 for computing h.The addition of h to diagonal pixels which are related to diagonal pixel difference generates new pixels X_j' & X_{j+2}' if h has integer type value.
- In addition process of h having float value to diagonal pixels for constructing new pixels, a constant value is added and subtracted from h and results two constant values C_1 and C_2 resp.

If $X_j > X_{j+2}$
then $X_j' = X_j + C_1$
$X_{j+2}' = X_{j+2} + C_2$

otherwise
$X_j' = X_j + C_2$
$X_{j+2}' = X_{j+2} + C_1$

- Repeat these steps for embedding the entire data.
- After embedding complete data , reposition the even row pixels and odd row pixels at their original position in corresponding even/odd segments.
- Construct the Watermarked image with reconstructing the all new even/odd embedded segments in a matrix of size of 256 * 256.

C. Extraction Process

- Received the Watermarked image through any channel.

- Segmentation of Watermarked image into small segments of size of 2 * 2 in form of odd and even segments.
- Take odd row pixels of embedded odd segment and embedded even segment in first and second row of a segment resp. to make original odd segment.
- Take even row pixels of embedded even segment and embedded odd segment resp. and interchanging their pixels column wise to make first row and second row of original even segment resp.
- Calculate the both diagonal pixel difference of each odd and even segments.
- Find range of diagonal pixel difference from the range table 3 in which the diagonal pixel difference lies.
- In this, M values are taken as keys for extracting the encrypted data. If M is odd, subtract diagonal pixel difference from 1 then subtract the addition of diagonal pixel difference and M from low range for extracting encrypted data bits
- If M is even, subtract the addition of diagonal pixel difference and M from low range for extracting encrypted data bits.

D. Decryption Process:

- Subtracting the decimal number of extracted bit stream groups having 2 bits in each group from higher range of encrypted range table then convert into nibbles and Construct 8 bit bytes with concatenation of two nibbles.
- Compute the gray equivalents using XOR operation between 8 bit bytes and random keys.
- Change the gray equivalents into binary equivalents.
- Convert all binary equivalents into decimal numbers and place decimal numbers in form of segments.
- Interchange the diagonal pixels after rearranging all decimal numbers as pixels into segments of 2 * 2.
- Add the square of position of each pixel of each segment to pixels for getting the original pixel value of Watermark image.
- Reconstruct the Watermark image after placing the all segments in a matrix of size of 32 * 32.

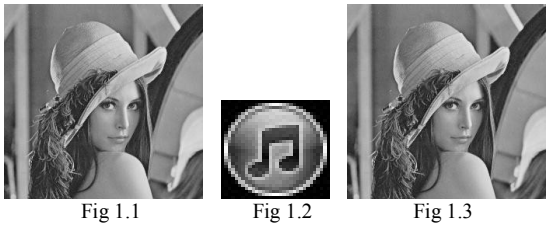

Fig 1.1 Host Image (Leena) | Fig 1.2 Watermark Image | Fig 1.3 Watermarked Image

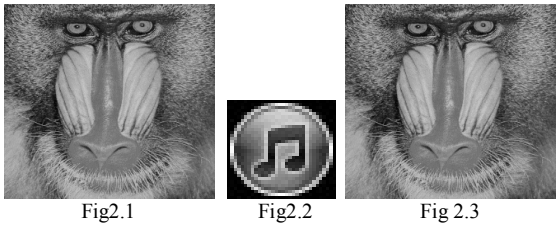

Fig2.1 Host Image(Baboon) | Fig2.2 Watermark Image | Fig 2.3 Watermarked Image

Fig 3.1 Host Image(Peppers) | Fig 3.2 Watermark Image | Fig 3.3 Watermarked Image

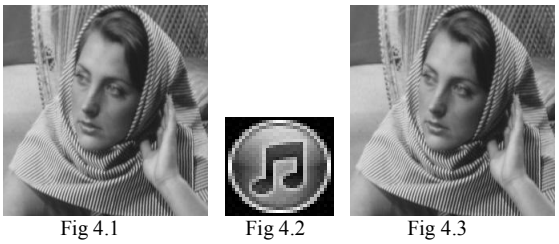

Fig 4.1 Host Image(Barbara) | Fig 4.2 Watermark Image | Fig 4.3 Watermarked Image

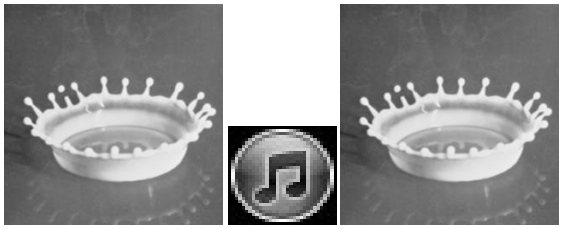

Fig 5.1 Host Image (Milk-drop) | Fig 5.2 Watermark Image | Fig 5.3 Watermarked Image

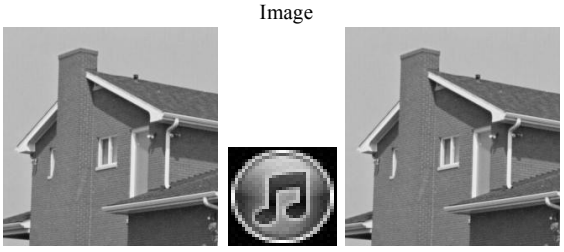

Fig 6.1 Host Image (House) | Fig 6.2 Watermark Image | Fig 6.3 Watermarked Image

Fig 7.1 Host Image(F16) | Fig 7.2 Watermark Image | Fig 7.3 Watermarked Image

ISSN: 2278 – 1323

Fig 8.1
Host Image(Boat)

Fig 8.2
Watermark Image

Fig 8.3
Watermarked Image

TABLE 4
PARAMETER RESULTS USING PROPOSED DPVD METHOD

S.NO	COVER IMAGE	PSNR	NCC	MSE
1.	Leena	54.7066	1.0000	0.4690
2.	Baboon	56.4189	1.0000	0.3851
3.	Peppers	49.5150	1.0000	0.8527
4.	Barbara	51.7178	1.0000	0.6617
5.	Milk-drop	56.5298	1.0000	0.3802
6.	House	55.1582	1.0000	0.4453
7.	F16	59.2618	1.0000	0.2776
8.	Boat	53.8964	1.0000	0.5149

TABLE 5
COMPARISON DPVD METHOD WITH FWSPVD

S.NO.	COVER IMAGE	PSNR FWSPVD	PSNR DPVD	NCC FWSPD	NCC DPVD
1.	Leena	44.81	54.7066	0.96	1.0000
2.	Baboon	46.79	56.4189	0.97	1.0000
3.	Peppers	45.45	49.5150	0.99	1.0000
4.	Barbara	44.70	51.7178	0.96	1.0000
5.	Milk-Drop	47.64	56.5298	0.97	1.0000
6.	House	47.28	55.1582	0.98	1.0000
7.	F16	49.81	59.2618	0.97	1.0000
8.	Boat	47.37	53.8964	0.97	1.0000

IV. GRAPH OF PARAMETERS FOR DPVD METHOD

- PSNR GRAPH

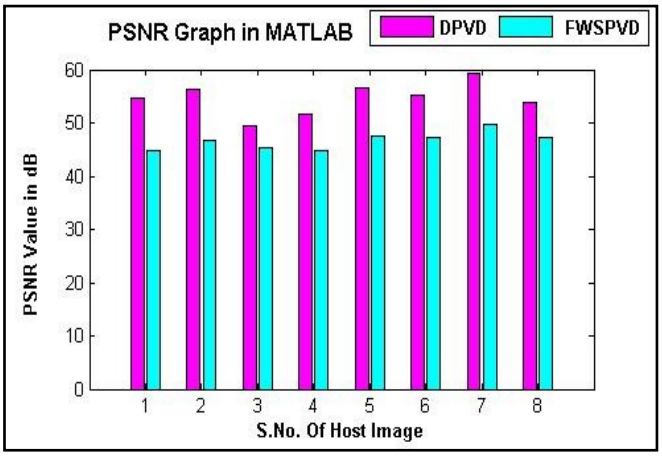

Fig 9 Graph of PSNR in MATLAB

- NCC GRAPH

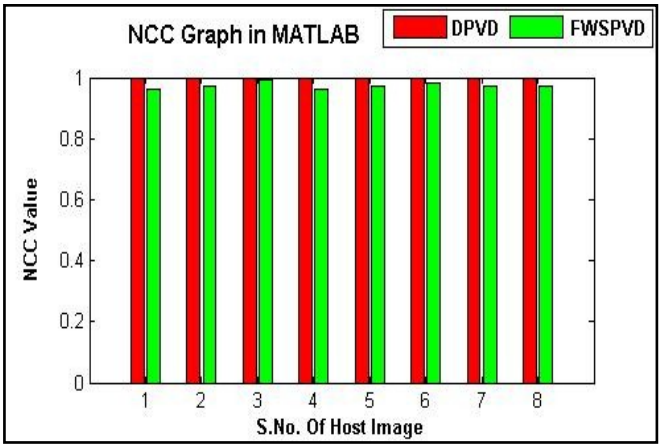

Fig 10 Graph of NCC in MATLAB

- MSE GRAPH

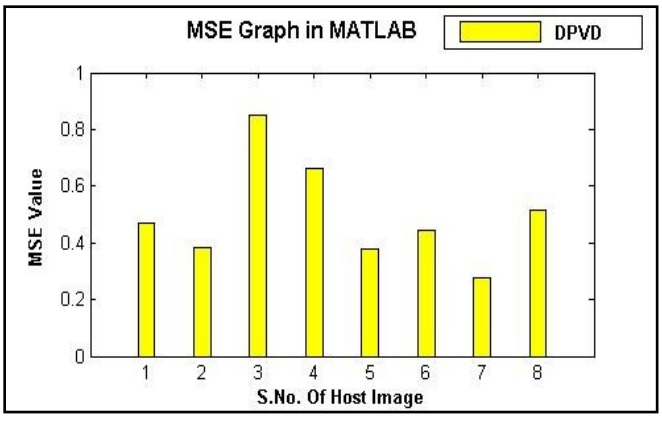

Fig 11 Graph of MSE in MATLAB

V. CONCLUSION

I.

Due to rise in internet services and new technologies, it is easier to creating a copy of digital data or transmition and distribution of this digital data without any owner's consent. In this paper, a proposed method provides more protection for copyright and ownership for digital images with its good robustness and imperceptibility. A gray scale image of 32*32 size is used as a watermark image. Each pixel of original watermark image after its encryption with random keys is concealed in a gray scale host image having size of 256 * 256 and decrypt after its extraction with proposed method. Experimental results show watermarked images with good robustness and Imperceptibility.

VI. REFERENCES

[1] M. Kaur, S. Jindal, S. Behal, " A Study Of Digital Image Watermarking", *International Journal of Research in Engineering & Applied Sciences,* vol. 2, pp. 126–136, ISSN: 2249-3905 , Feb. 2012.

[2] B.L. Gunjal , R.R. Manthalkar, " An Overview of Transform Domain Robust Digital Image Watermarking Algorithms", *Journal of Emerging Trends in Computing and Information Sciences,* vol. 2, pp. 37–42, ISSN 2079-8407.

[3] S.Maruthuperumal,V.Vijayakumar, B.Vijayakumar, "Sorted Pixel Value Difference on Fuzzy Watermarking Scheme" , *Global journal of Computer Science and Technology* , Volume 12, Issue 4, Version 1.0, Fabruary 2012.

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

[5] G, Singh, K. Singla, "A High Quality Image Steganography using Highest Pixel Value Difference",proceeding of international conference on Information and mathematical sciences ,Oct 2013,Punjab,India.

[6] https//www.watermarking.

[7] Y. Yusof and O. O. Khalifa, "Digital Watermarking for Digital Images Using Wavelet Transform", Proceedings of the 2007 IEEE International Conference on Telecommunications and Malaysia International Conference on Communications, 14-17 May 2007, Penang, Malaysia.

[8] J. K. Mandal, D. Das, "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.

ISSN: 2278 – 1323