ISSN 2350-1022

International Journal of Recent Research in Mathematics Computer Science and Information Technology
Vol. 3, Issue 1, pp: (51-57), Month: April 2016 – September 2016, Available at: www.paperpublications.org

Robust Image Watermarking Based on Dual Intermediate Significant Bit (DISB) Invariant to Rotation, Scaling and Translation

[1]Er. Sukhpreet Kaur, [2]Praiksha Matharu

[1]Assistant Professor, Department of Computer Science Engineering ,Shaheed Udham Singh Engeering College Tangori
[2]Department of Computer Science Engineering SUSCET, Tangori

***Abstract*: The most important requirements should be available on any watermarking systems which are the robustness against possible attacks and the quality of the watermarked images. In most applications, the watermarking algorithm embeds the watermark have to be robust against possible attacks and keep the quality of the host media as possible. The relationship between the two requirements is completely conflict. In this study, the method focuses on the robustness against RST attacks for the watermarked image based on Dual Intermediate Significant Bit (DISB) model. This method requires embedding two bits into every pixel of the original image, while and the other six bits are changed so as to directly assimilate the original pixel. In the case, when the two hidden bits are equal or not equal to the original bits, there is a need to use mathematical equations to solve this problem which derived and applied in this study. The results show that the proposed model also produces robustness watermarked images after applying geometric attacks on the RGB images as compared to our previous grayscale images. The best values investigated when the Peak Signal to Noise Ratio (PSNR) is equal or more than 30db, and finding the best Normalized Cross Correlation (NCC) to evaluate the image resistance against attacks. The best values investigated for Rotation when the two embedded bits are k1=1 and k2=4, for Scaling when the two embedded bits are k1=2 and k2=4 , for Translation when the two embedded bits are k1=3 and k2=4.**

***Keywords:* Watermarking; DISB; ISB; LSB; Robustness.**

1. INTRODUCTION

Nowadays, the evolution of computer network technologies has revolutionized the manner used in the transference of information through the internet have to be robust against possible attacks and do not take into account the quality of the content. Digital watermarking is one of the hiding techniques used in information technologies that embed copyright information into the host media which is used in identifying the ownership of various types of multimedia. It achieves the copyright protection purpose of embedding a signal that contains useful certifiable information for the original media owner, such as company logo, producer's name into the host media [1, 2].The robustness of the watermarked image is considered as one of the most important requirements in any watermarking system. In other word, the watermarking algorithm embeds the watermark without affecting the quality of the host media.

In general, improving the quality of the watermarked image should take into consideration the other requirements, such as the resistance against attacks and the distortion for watermarked image should be impenetrable by third party.

2. RELATED WORKS

Research works on image watermarking has been carried out at a constant the past. They can be classified into frequency domain based, spatial domain based, or both.

ISSN 2350-1022

International Journal of Recent Research in Mathematics Computer Science and Information Technology
Vol. 3, Issue 1, pp: (51-57), Month: April 2016 – September 2016, Available at: www.paperpublications.org

A study that discussed a robust method for digital watermarking in spatial domain. The method deals with an image in the spatial domain which is watermarked at different intensity subsections. Also the study compares the PSNR that can be obtained using the proposed spatial domain watermarking. The normal watermark can be extracted out from the conventional spatial domain watermarked image just by subtracting the original image from the watermarked image. Only the intended user can extract the watermark by using the same key at the receiver end. So this would prevent any eavesdropper from extracting the information embedded in the watermark, which makes the method suitable in security aspect as well. The robustness of this watermarking technique can also be verified by the use of pseudo random noise with the watermarked image. In this case an intruder who does not know the proper key that is multiplied by the image cannot extract the watermark.

The effectiveness of a digital watermarking algorithm is indicated by the robustness of embedded watermarks against various attacks [6]. Improving the robustness of a watermark so as to withstand attacks has been one of the main study objectives in digital image watermarking. In order to achieve robustness, an overall architecture for a feature-based robust digital image watermarking scheme is designed. A simulated attacking procedure is performed using predefined attacks to evaluate the robustness of every candidate feature region selected. Comparing with some well-known feature-based methods, the proposed method exhibits better performance in robust digital watermarking.

An ISB model based on blocks of pixels is developed to improve its resistance against different types of attacks and at

represents the binary number for the two bit planes. The length of each range depends on the value of k2, (L_ range

^{2}). Each range is divided into equal periods; (period is the same time maintain the quality of the image [7]. In another

ISB model the data of the watermark is repeated for a certain number of times (3, 5, 7, and 9 times) in order to improve the resistance of the watermarking technique. At the same time, the watermark technique is mainly used in the watermark detecting procedure, which makes the algorithm more resistant, especially to the geometric transformation attacks. An enhanced system based on multiple watermarks in which two different watermarks are embedded concurrently into the ISB of the host image pixels [8].

The DISB method which improves the quality of the watermarked image by [10], by embedding two bits into every pixel of the original image, while and the other six bits are changed so as to directly assimilate the original pixel. The method produces high watermarked image quality as compared to the quality of the watermarked image produced by the use of Least Significant Bit (LSB) method. In addition, the method increasing the capacity as compared with the ISB method because of using two bits, so the capacity equal to 25% while the ISB was 12.5%.

Another improvement of the image quality proposed by [9]. The method focuses on the greatest quality of the watermarked image based on DISB model. The embedding

$=2*K_2$ 1

on the left and period$_2$ is on the right) to do guarantee that the first part contain k_2 where k_2=0, while k_2 in the second part contain k_2 where k_2 =1. This process is to help speediest reachable to the exact pixel, also to make embedding process easier in embedding and to get the suitable values after embedding. At the same time, k1 similar to k_2 but the length of the period is ($2^{\wedge K-1}$). The length of each period can be obtained by dividing the length of the range with two (L-period = L_range/2), as shown in Figure 3.3. The number of ranges (N) can be obtained by dividing 256 by the length of the range (N=256/L). The two embedded bits are b1 and b2, in which b1 is embedded into k1, while b_2 is embedded into k_2 respectively.

The first step is done by selecting the pixel in the exact range and period for the original image and the positions of the two keys k_1 and k_2, and select the two embedded bits b_1 and b_2, then convert the pixel into binary. By comparing the value of the position k_1 with b_1 and k_2 with b_2, if they are equal, then the equation below will be used: p`=p-mod (p,($2^{\wedge(k-1)}$-1)

So, the new position of the watermarked pixel will be found by calculating the differences between the original pixel and the watermarked pixel, the minimum difference will be chosen, k1-1 process is done by using two keys k_1 and k_2 where $k_2 > k_1$. The then by shifting the length of (2^) to the right or to the left.

extracting process has been done after applying some types of attacks. The proposed method has got the best value for PSNR which represent the criterion for quality and the clarity of image.

A comparison of watermarking image quality was performed between two existing methods: Dual Intermediate Significant Bit (DISB) and Genetic Algorithm (GA) by [10]. The first method focuses on the high quality of the watermarked image based on DISB model. The second method, GA method is used to embed two bits of watermarking data within every pixel of the original image and to find the optimal value based on the existing DISB. GA is used in determining the minimum fitness value in which the fittest is the absolute value between the pixel and chromosome and the value of chromosome between 0-255. The results indicate that the two methods produce a high quality for watermarked image, but there is a big difference in the processing time, so the DISB method is faster than the GA method.

The paper is organized as follows: section 3 introduces the proposed method and the proposed algorithm in detail. Section 4 discusses the achieved results. Section 5 concludes the paper. Finally, section 6 introduces the references that used in this paper.

The same thing will be done if the two embedded bits are not equal to the original pixel in the original image by calculating the short distance between the original bits and the watermarked bits. The proposed method algorithm as in Figure 1 below:

3. PROPOSED METHOD

The proposed method The proposed method, can be explained by dividing the bit plane into a number of ranges depending on the key k_2 and selecting any two bit-planes from 1 to 8 which are called (k_1, k_2) where (k_2> k_1) and Yk_1, Yk_2

```
Input k1, k2 where k2>k1
Input two embedded bits b1 and b2
Read pixel p from the original image
Convert p into binary (Y)
If Y (k1) =b1 and Y (k2)=b2
Then
if p>p-mod(p,(2^(k1-1) -1)+2^(k1-1))/2
p`=p-mod(p,(2^(k1-1) -1)
else
p`=p-mod(p,(2^(k1-1) -1)+2^(k1-1)-1 ;
end
If Y (k2) =b2 and Y (k1) <>b1
Then
 p`=MIN ( p-mod(p,(2^(k1-1) -1, p-mod (p,(2^(k1-1)) +2^ (k1-1))
If Y (k2) <>b2
Then
 If b1=0
Then
 p`=MIN( min_period (p)-2^(k1-1)-1, min_period (p)+2^ (k2-1))
If b1=1
Then
 p`=MIN( min_period(p)-1,min_period (p)+2^(k2-1)+2(k1-1))
if p`<p
Then
 p`=p`-2^(k1-1)-1
else
p`=p`+2^(k1-1)-1
end
```

Figure 1. The proposed Algorithm

ISSN 2350-1022

International Journal of Recent Research in Mathematics Computer Science and Information Technology
Vol. 3, Issue 1, pp: (51-57), Month: April 2016 – September 2016, Available at: www.paperpublications.org

4. RESULTS FOR THE PROPOSED METHOD

A. Method development:

In this study, the watermark embedded for all bit-planes and the NCC calculated to show the improvement of image robustness against geometric attacks by using this method. Meanwhile, the host images selected in rgb with 500

× 500 pixels, which have been downloaded from the Internet, http://www.google.com). The Figures (2&3) below show the host images and watermark image that used in this method, at the same time the next section shows the results for the proposed method.

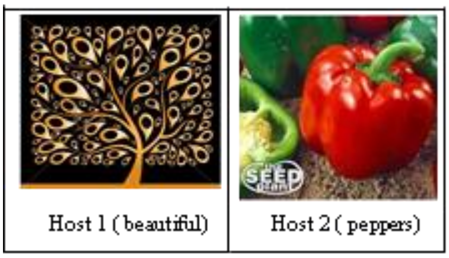

Figure2.Host images before embedding

Figure 3. Watermark image

B. Results of the proposed method:

The results clearly indicate the robustness of the watermarked images by using the proposed method show the gradual decrease from the first bits-plane (MSB) (k_1=1, k_2=2) to the last bits-plane (LSB) (k_1=1 k_2=8). The watermarked object is inserted into the two selected bits, and the other

6 bits are changed to directly assimilate the original pixel. In the case when 2 hidden bits are equal to the original bits, there will be an equation used. However, if the original value is not equal to the embedded one, the nearest pixel in the original will be chosen and by shifting the length ($2^{\wedge k1-1}$) to find the watermarked image.

Table 1 shows the PSNR after embedding watermark using the proposed method for all the bit-planes, starting from (k_1=1, k_2=2) (the most significant bits -MSB) through the 8th bit- plane (the least significant bits - LSB).

Table 1

Results after applying Rotation (145 degree)							
Bit planes		**Host Image 1**			**Host Image 2**		
K1	**K2**	**MSE**	**PSNR**	**NCC**	**MSE**	**PSNR**	**NCC**
1	2	141.61	26.61	4.0e-036	141.61	26.61	4.0e-036
1	3	79.21	29.14	NaN	79.21	29.14	NaN
1	4	28.09	33.64	-2.0e-036	28.09	33.64	-2.0e-036
1	5	1.1e+003	17.37	7.1e-039	1.1e+003	17.37	7.1e-039
1	6	3.6e+003	12.55	8.9e-040	3.6e+003	12.55	8.9e-040
1	7	1.2e+004	7.20	1.1e-040	1.2e+004	7.20	1.1e-040
1	8	4.5e+004	1.53	1.3e-041	4.5e+004	1.53	1.3e-041
2	3	79.21	29.14	NaN	79.21	29.14	NaN
2	4	28.09	33.64	-2.0e-036	28.09	33.64	-2.0e-036
2	5	1.1e+003	17.37	7.1e-039	1.1e+003	17.37	7.1e-039

ISSN 2350-1022

International Journal of Recent Research in Mathematics Computer Science and Information Technology
Vol. 3, Issue 1, pp: (51-57), Month: April 2016 – September 2016, Available at: www.paperpublications.org

2	6	3.6e+003	12.55	8.9e-040	3.6e+003	12.55	8.9e-040
2	7	1.2e+004	7.20	1.1e-040	1.2e+004	7.20	1.1e-040
2	8	4.5e+004	1.53	1.3e-041	4.5e+004	1.53	1.3e-041
3	4	28.09	33.64	-2.0e-036	28.09	33.64	-2.0e-036
3	5	1.1e+003	17.37	7.1e-039	1.1e+003	17.37	7.1e-039
3	6	3.6e+003	12.55	8.9e-040	3.6e+003	12.55	8.9e-040
3	7	1.2e+004	7.20	1.1e-040	1.2e+004	7.20	1.1e-040
3	8	4.5e+004	1.53	1.3e-041	4.5e+004	1.53	1.3e-041
4	5	1.1e+003	17.37	7.1e-039	1.1e+003	17.37	7.1e-039
4	6	3.6e+003	12.55	8.9e-040	3.6e+003	12.55	8.9e-040
4	7	1.2e+004	7.20	1.1e-040	1.2e+004	7.20	1.1e-040
4	8	4.5e+004	1.53	1.3e-041	4.5e+004	1.53	1.3e-041
5	6	3.6e+003	12.55	3.8e-040	3.6e+003	12.55	3.8e-040
5	7	1.2e+004	7.20	4.8e-041	1.2e+004	7.20	4.8e-041
5	8	4.5e+004	1.53	6.0e-042	4.5e+004	1.53	6.0e-042
6	7	4.5e+004	1.53	3.0e-042	1.2e+004	7.20	3.0e-042
6	8	4.5e+004	1.53	3.0e-042	1.2e+004	7.20	3.0e-042
7	8	4.5e+004	1.53	1.1e-042	1.2e+004	7.20	1.1e-042

From above table 1, it is easily noted the PSNR and NCC value after applying Rotation (145 degree) on host images from bit plane (k1=1,k1=2) to (k1=7 , k2=8) and it is observed that best value generate on k1=1 and k2=4

Table 2

Results after applying Scaling							
Bit planes		**Host Image 1**			**Host Image 2**		
K1	**K2**	**MSE**	**PSNR**	**NCC**	**MSE**	**PSNR**	**NCC**
1	2	91.48	28.51	9.4e-036	2.95	43.42	-6.4e-035
1	3	43.42	31.75	NaN	21.97	34.71	NaN
1	4	9.50	38.34	-4.4e-036	68.57	29.76	5.6e-035
1	5	1.0e+003	17.99	1.7e-038	438.18	21.71	-8.3e-038
1	6	3.3e+003	12.90	2.1e-039	2.1e+003	14.77	-1.0e-038
1	7	1.1e+004	7.38	2.6e-040	9.5e+003	8.33	-1.2e-039
1	8	4.4e+004	1.63	3.3e-041	4.0e+004	2.1046	-1.6e-040
2	3	43.42	31.75	NaN	21.97	34.71	NaN
2	4	9.50	38.34	-4.5e-036	68.5709	29.769	6.8e-035
2	5	1.0e+003	17.99	1.5e-038	438.18	21.71	-9.6e-038
2	6	3.3e+003	12.90	1.9e-039	2.1e+003	14.77	-1.2e-038
2	7	1.1e+004	7.38	2.4e-040	9.5e+003	8.33	-1.5e-039
2	8	4.4e+004	1.63	3.1e-041	4.0e+004	2.1046	-1.8e-040
3	4	9.50	38.34	-3.5e-036	68.5709	29.76	1.0e-034
3	5	1.0e+003	17.99	1.3e-038	438.18	21.71	-1.3e-037
3	6	3.3e+003	12.90	1.7e-039	2.1e+003	14.77	-1.6e-038
3	7	1.1e+004	7.38	2.4e-040	9.5e+003	8.33	-2.0e-039
3	8	4.4e+004	1.63	2.6e-041	4.0e+004	2.1046	-2.5e-040
4	5	1.0e+003	17.99	1.0e-038	438.18	21.71	-2.8e-037
4	6	3.3e+003	12.90	1.2e-039	2.1e+003	14.77	-3.5e-038
4	7	1.1e+004	7.38	1.5e-040	9.5e+003	8.33	-4.4e-039
4	8	4.4e+004	1.63	1.9e-041	4.0e+004	2.1046	-5.5e-040
5	6	3.3e+003	12.90	7.3e-040	2.1e+003	14.77	-4.8e-037
5	7	1.1e+004	7.38	9.2e-041	9.5e+003	8.33	-6.0e-038
5	8	4.4e+004	1.63	1.1e-041	4.0e+004	2.1046	-7.5e-039
6	7	4.4e+004	1.63	5.0e-042	4.0e+004	2.1046	1.3e-039
6	8	4.4e+004	1.63	5.0e-042	4.0e+004	2.1046	1.3e-039
7	8	4.4e+004	1.63	1.6e-042	4.0e+004	2.1046	2.2e-041

From above table 2, it is easily noted the PSNR and NCC value after applying Scaling on host images from bitplane (k1=1,k1=2) to (k1=7 , k2=8) and it is observed that best value generate on k1=2 and k2=4

Table 3

Results after applying Translation							
Bit planes		**Host Image 1**			**Host Image 2**		
K1	**K2**	**MSE**	**PSNR**	**NCC**	**MSE**	**PSNR**	**NCC**
1	2	92.05	28.49	9.6e-036	3.09	43.22	-6.6e-035
1	3	44.34	31.66	NaN	21.88	34.72	NaN
1	4	10.84	37.77	-4.5e-036	68.19	29.79	5.8e-035
1	5	1.0e+003	18.00	1.7e-038	440.08	21.69	-8.5e-038
1	6	3.3e+003	12.911	2.2e-039	2.1e+03	14.76	-1.0e-038
1	7	1.1e+004	7.39	2.75e-40	9.5e+03	8.32	-1.3e-039
1	8	4.4e+004	1.63	3.4e-041	4.0e+04	2.10	-1.6e-040
2	3	44.34	31.66	NaN	21.88	34.72	NaN
2	4	10.84	37.77	-4.2e-036	68.19	29.79	7.0e-035
2	5	1.0e+003	18.00	1.6e-038	440.08	21.69	-9.9e-038
2	6	3.3e+003	12.911	2.0e-039	2.1e+03	14.76	-1.2e-038
2	7	1.1e+004	7.39	2.5e-040	9.5e+03	8.32	-1.5e-039
2	8	4.4e+004	1.63	3.2e-041	4.0e+04	2.10	-1.9e-040
3	4	10.84	37.77	-3.6e-035	68.19	29.79	1.0e-034
3	5	1.0e+003	18.00	1.4e-038	440.08	21.69	-1.3e-037
3	6	3.3e+003	12.911	1.8e-039	2.1e+03	14.76	-1.7e-038
3	7	1.1e+004	7.39	2.2e-040	9.5e+03	8.32	-2.1e-039
3	8	4.4e+004	1.63	2.8e-041	4.0e+04	2.10	-2.6e-040
4	5	1.0e+003	18.00	1.1e-038	440.08	21.69	-2.9e-037
4	6	3.3e+003	12.911	1.3e-039	2.1e+03	14.76	-3.7e-038
4	7	1.1e+004	7.39	1.7e-040	9.5e+03	8.32	-4.6e-039
4	8	4.4e+004	1.63	2.1e-041	4.0e+04	2.10	-5.8e-040
5	6	3.3e+003	12.91	7.5e-042	2.1e+03	14.76	-5.3e-037
5	7	1.1e+004	7.39	9.4e-041	9.5e+03	8.32	-6.6e-038
5	8	4.4e+004	1.63	1.1e-041	4.0e+04	2.10	-8.3e-039
6	7	4.4e+004	1.63	5.1e-042	9.5e+03	8.32	1.0e-038
6	8	4.4e+004	1.63	5.1e-042	4.0e+04	2.10	1.2e-039
7	8	4.4e+004	1.63	1.6e-042	4.0e+04	2.10	2.1e-041

From above table 3, it is easily noted the PSNR and NCC value after applying Scaling on host images from bitplane (k1=1,k1=2) to (k1=7 , k2=8) and it is observed that best value generate on k1=3 and k2=4

5. CONCLUSION

The robustness of watermarked image considered as one of the most important requirements for any watermarking system. The main problem that faces people when using the Internet is how to keep their special information from any hacker. There are the most important requirements should be available on any watermarking systems which are the robustness against possible attacks and the quality of the watermarked images. This study attempts to obtain better values for NCC, which represents the criterion for robustness. This study enhanced the robustness against some type image attacks by embedding two bits of watermark image into each pixel of the host imaged on the existing DISB method.

International Journal of Recent Research in Mathematics Computer Science and Information Technology
Vol. 3, Issue 1, pp: (51-57), Month: April 2016 – September 2016, Available at: www.paperpublications.org

The results show that the proposed model produces robustness watermarked image on RGB images. The best image robustness against geometric attacks investigated different on different bit planes. For the future work, we can apply guassian attacks after applying geometric attacks Besides, to make more enhancement to be applied based on the blocks of few pixels instead of one pixel.

REFERENCES

[1] A. Peungpa and T. Amornraksa, "An Improving Method for Image Watermarking Using Image Averaging and Tuned Pixels Prediction," IEEE, ISCIT, 2010, pp. 755-760.

[2] W. Taiyue, and L. Hongwei. "An Adaptive Color Image Digital Watermarking Algorithm Based on Discrete Wavelet Transform", JCIT: Journal of Convergence Information Technology, Vol. 8, No. 1, pp. 489– 45, 2013.

[3] Ghassan N. Mohammed, Azman Yasin and Akram M.Zeki, "Robust Image watermarking based on Dual Intermediate Significant Bit (DISB)" , ISBN :987-1-4799-3999-2.

[4] Zhu Yuefeng,Lin Li, "Digital Image Watermarking Algorithm based on dual Transform domain and self recovery," International Journel on Smart Sensing and intelligent Systems Vol.8,No.1 ,march 2015 ISSN 1178-5608.

[5] Akram M. Zeki and Azizah A. Manaf, "A Novel Digital watermarking Technique based on ISB", World Academy of Science , Engineering and Technology Vol : 3 2009-02-23.

[6] Hemahlathaa, & Chellppan. A Feature-Based Robust Digital Image Watermarking Scheme. IEEE International Conference on Computing, Communication and Applications (ICCCA), 1-5, 2012.

[7] A. M. Zeki and A. A. Manaf, "Analysis of ISB watermarking model: block based methods vs. embedding repetition methods," 9th International Conference on Advances in Mobile Computing and Multimedia pp. 198-201, 2011.

[8] M. S. Emami, G. B. Sulong, and S. B. Seliman, "A Novel Multiple Semi-Blind Enhanced ISB Watermarking Algorithm Using Watermark Bit-Pattern Histogram For Copyright Protection", International Journal of Innovative Computing, Information and Control ICIC International, ISSN 1349-4198 , March, vol. Volume 8, No 3(A), pp. 1665-1687, 2012.

[9] Ghassan N. Mohammed,Azman Ya,Akram M. Zeki."Improvement of the Quality for Digital Image Watermarking Based on DISB", IEEE: IT Convergence and Security (ICITCS), 2013 International Conference on 16-18 Dec. 2013, pp. 1 – 4, 2013.

[10] Ghassan N. Mohammed, Azman Yasin, Akram M. Zeki," A Comparison of Watermarking Image Quality Based on Dual Intermediate Significant Bit with Genetic Algorithm", Proceedings of the 4th International Conference on Computing and Informatics, ICOCI 2013, pp.272-278, 2013.

[11] Internet (RGB Images, http://www.google.com).