DIGITAL WATERMARKING

Rahul Janardhanan
rahul25jana@gmail.com
Nov 17, 2017

ABSTRACT

The growth of technology has made our life very easy in many ways. Millions of people depend on the technology in their day to day lives. But, it has also lead to many major problems like securing our own data from duplication. Digital Watermarking is the solution used. Digital Watermarking helps us to embed information on digital data. The primary goal of this paper is to encrypt some information in our digital image, so that our image cannot be used by others. It is just giving copy rights to our image. By doing this process, we can protect our image from un-authorized access. The Watermarked image can be decrypted by appropriate algorithm or detection algorithm. We will be using two different images, where one will be original image and other will be watermarked logo in it. The idea behind this, is to insert our logo in the main image. We would like to focus on hidden watermark in the image. The proposed algorithm uses Bit- shuffling method.

Keywords

Embed, Encrypt, Decrypt, Digital Watermarking, Logo, Bit- Shuffling, Watermarked logo, Least Significant Bit(LSB), Copy Rights, Detection.

INTRODUCTION

In recent years, there has been a rapid growth of technology. Today's generation is witness of developments of digital media [5]. This has led to many piracy of the data, duplication and un-authorized access. Many hackers are developing tools to crack the data with the help of technology. To reduce these problems, Digital Watermarking was introduced. Digital Watermarking is the process of embedding information in the digital image [11]. In other words Watermarking is a branch of information hiding [1]. Digital Watermarking focuses mainly on

the protection of the property and illegal access [6]. Watermarking can be applied on static images, multimedia formats like videos and on documents. The Watermarked image can be visible or invisible. To explain in brief, visible watermark can be seen in naked eyes. Invisible Watermark can be seen only by using appropriate detection algorithm. The above mentioned technique will solve duplication problems, hacking illegally, un-authorized access and copyright protection.

BASIC OF WATERMARKING

The basic strategy behind Watermarking consists of two parts [3]:

- Watermark embedding
- Watermark extraction

Watermark Embedding

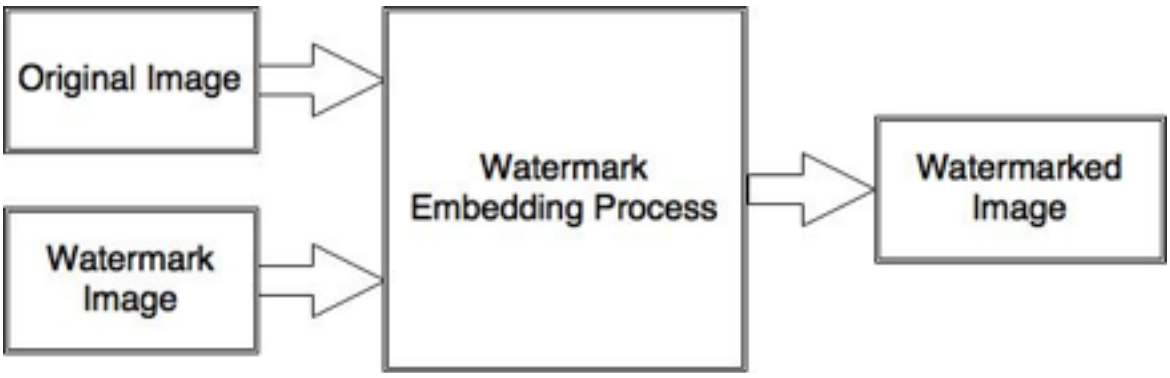


Figure 1. Watermarking Embedding process

Watermark Extraction

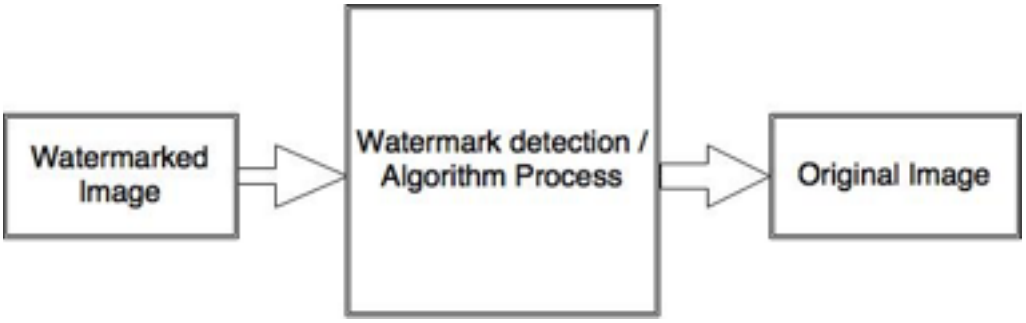


Figure 2. Watermarking Extraction process

MOTIVATION

It is really annoying when someone illegally access our image or data without permission. We would have taken much time to compose some wonderful image or developed good data and all of a sudden it gets used by some unknown person. Every designer, developer or whoever may be the person, would have faced this problem. We personally faced this problem, our team design picture was illegally used by an unknown person. To overcome this issue, we decided to do Digital Watermarking which protects our data from illegal access.

RELATED WORK

Many recent digital studies have showed that Digital Watermarking can be used to protect our data/ image from illegal and un-authorized access. [1] Similar bit- shuffling algorithm was used, researchers used new algorithm for encrypting watermark in image using pixel- shuffling. As Watermarking techniques have developed, hackers are developing new methods to attack or destroy watermark [5]. Researchers using digital watermarking approach on protecting their data have found several issues like image getting compressed, introduction of noise, image composition and geometric transformations. Some main issues seen were multiple watermarking, collusion attacks and forgery [5].

Table 1: Related Work

Year	Work
1999	Hsu *et al*. proposed hidden approach by selectively modifying the middle- frequency parts of the image.
2009	Robert *et al*. presented survey on different watermarking techniques.
2012	Perwej *et al*. gave an adaptive watermarking method. This method uses LSB to encrypt message in image.
2014	Islam *et al*. proposed three methods like, DWT DCT and SVD. Robustness was main factor.
2014	Saini *et al*. presented digital watermarking techniques and its applications. Here PSNR was used.
2014	Sarkar *et al*. Watermarking was done in spatial domain and frequency domain.

2016	Tyagi *et al*. gave detailed explanation of watermarking and techniques, its pros and cons with different methods.
2017	Joshi *et al*. proposed performance analysis on three methods. Bit- shuffling scheme was used for encrypting.

METHODOLOGY

We will be using a binary level image which consists of 8-bits. This algorithm uses bit- shuffling method. Bit- shuffling algorithm is used to shuffle the elements of encrypted watermark in order to embed the watermark in random positions in the main image [1]. Matlab programming will be used to encode and decode the data into the image. There is no specific data set to be used. But however some there are geospatial data sets, kaggle datasets.

Figure 3. Original Image

Figure 3, is the original/ input image to be watermarked. The red square in it is the random pixel area used by bit- shuffling method.

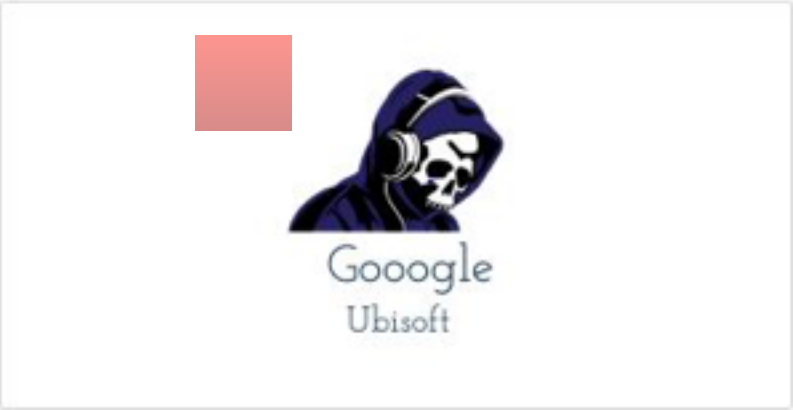


Figure 4. Watermark Image

First a random pixel from the input image(Fig. 3) is taken, say 250 and a pixel from the watermark image(Fig. 4), 150. Now by converting those pixel value into binary representation. Table 2. gives the representation of those pixel values.

Table 2: Binary Representation

Image Pixel	Binary Representation
250	11111010
150	10010110

Now by making the two least significant bits of the input image value 250 to zero (i.e., 11111010 to 11111000) . This step is also done for our watermark image, by taking the two most significant bits without replacing with zero (i.e.,10010110). The next step in our algorithm is to place the two most significant bits of the watermarked image with the two least significants bits of our input image.

i. e 11111000 + 00000010 = 11111010 ==> 250

Our algorithm will generate one common value from which our watermarked logo will be embedded. To test this, the algorithm is made to run series of steps. First, original image and watermarked image are added together by the reducing the visibility of our watermark logo. One important factor to make sure is, to have the input image and watermark image same size. The visibility is set between 0 and 1.

Figure 5. Sample watermark with same size of input image

From adding the input image and watermark logo,

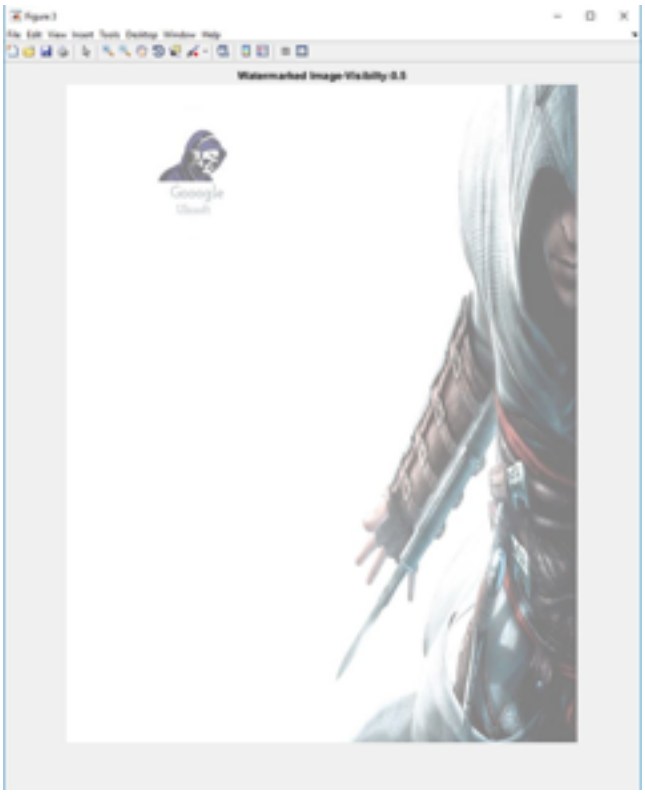
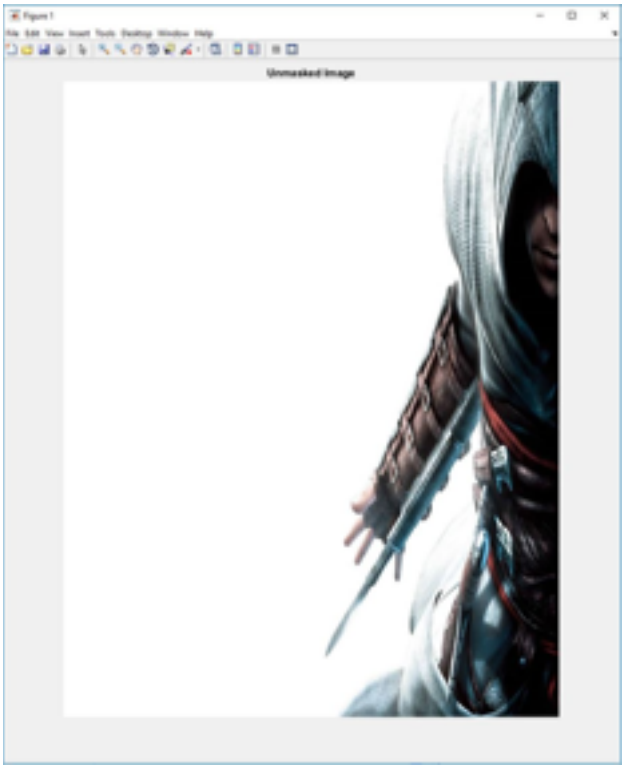
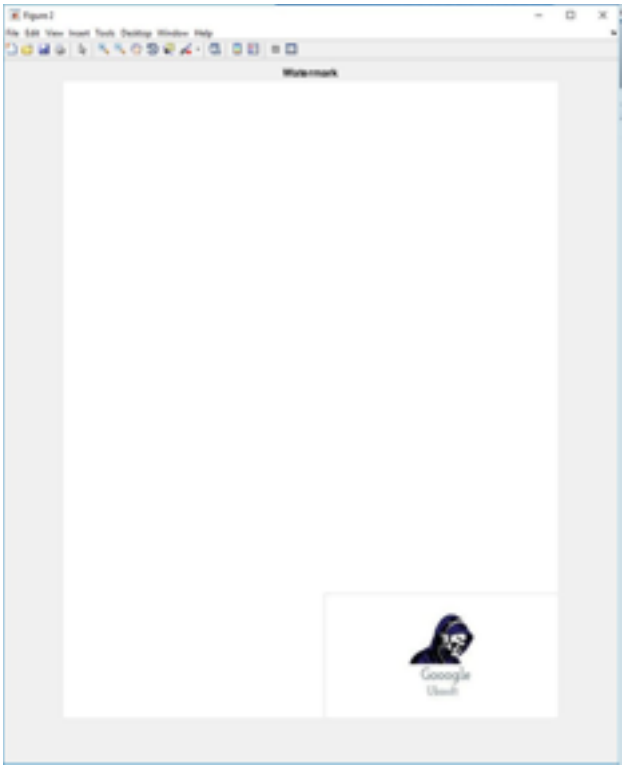


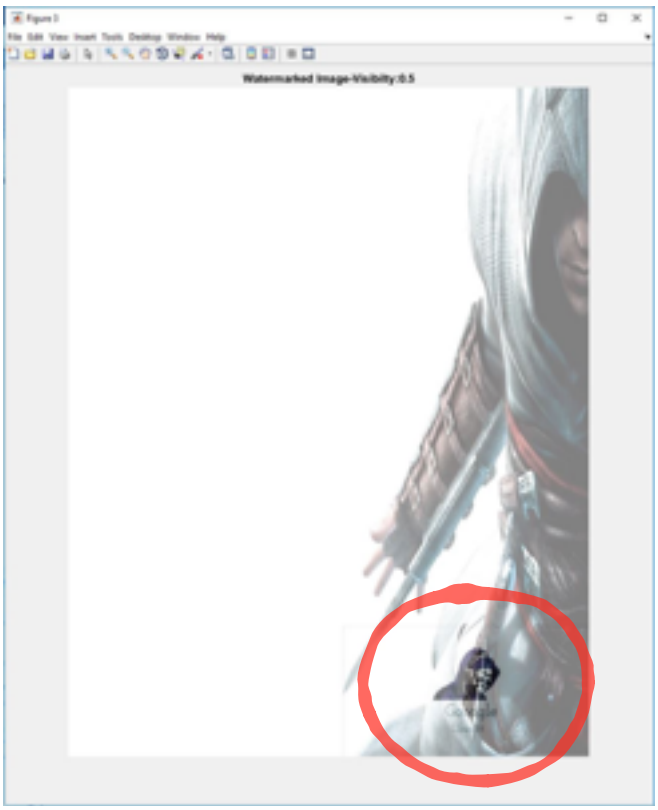
Figure 6. Composed image with watermarked logo

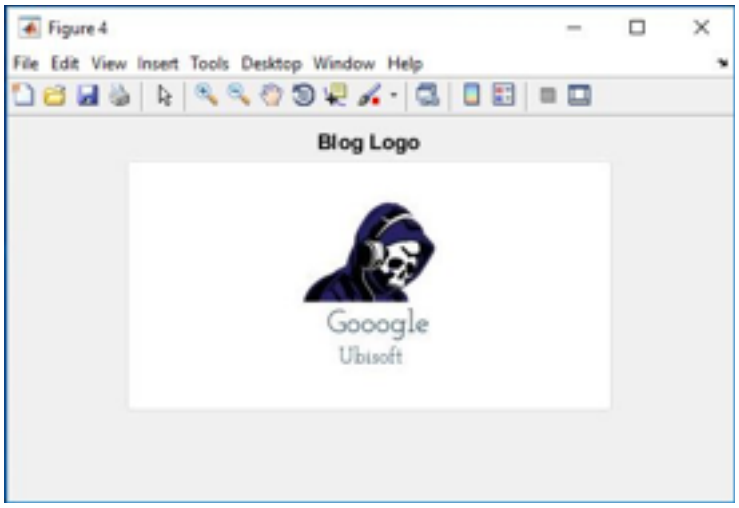
PRELIMINARY RESULTS

From the methodology process, the results where pretty much known. The images were watermarked with corresponding logos.

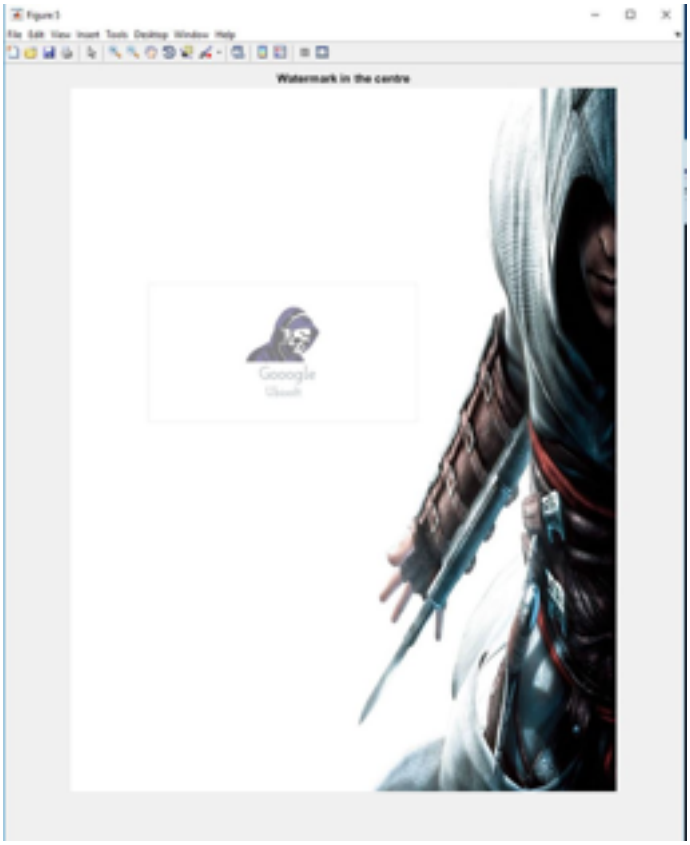








Our data set was from the google where we took a picture and wanted to give copyrights or apply digital watermarking. A series of steps will be followed to obtain the optimal solution. From the above figures, the images have been processed in Matlab and applied watermark. First, the input image and watermark image are added with visibility. Then it is processed for invisible watermarking. The results can been seen in below figures. We tested and trained more than 10 images, applied watermarking.



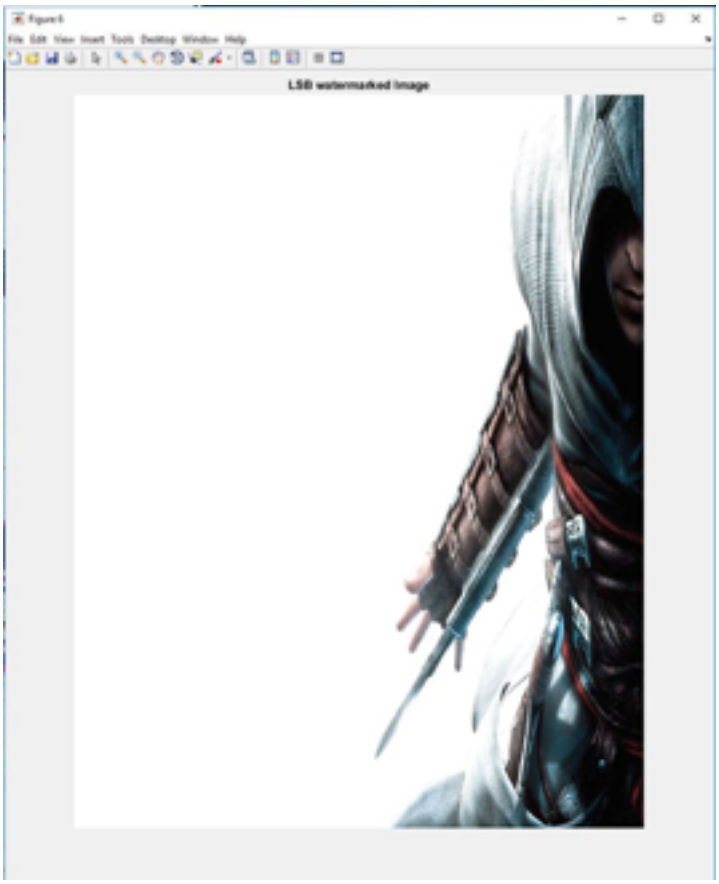


Figure 7. Invisible Watermarked Image

Figure 8 - 9. Watermark Extracted Images

After visibility process, our input image was applied invisible watermark algorithm. We can clearly see from the above figure 7. From the invisible watermarked image, we can only extract or see the watermark with the appropriate watermarking detection algorithms. The above two figures 8 - 9, shows the watermark extracted from the appropriate algorithm. The red circle defines the extracted watermark image.

EVALUATION/ CONCLUSION

In this paper, we have studied how Digital Watermarking can be done by bit- shuffling algorithm. The proposed algorithm works perfectly with little drawbacks. Furthermore, digital watermarking proved to be efficient method for data protection. This method guarantees the protection of data from illegal access and un-authorized users. We applied watermarking technique on more than 10 images and similar results were found. For the result, we have taken an image, encrypted digital watermarking and extracted watermark image. Our results show that our proposed algorithm is very robust. But still there will be little drawbacks when it is attacked against Salt and Pepper, Gaussian Noise. Recent studies showed, there are many techniques emerging to protect data.

REFERENCES

[1] A. Joshi, S. A. Kumar, S. Nikhila, ”Performance Analysis of Digital Water Marking Techniques”, 2017, *International Journal of Research and Scientific Innovation(IJRSI)*, Bangalore.

[2] S. Tyagi, H. V. Singh, R. Agarwal, ”Digital Watermarking Techniques for Security Applications”, 2016, *International Conference on Emerging Trends in Electrical, Electronics and Sustainable Energy Systems*.

[3] R. Patel, P. Bhatt, ”A Review Paper on Digital Watermarking and its Techniques”, 2015, *International Journal of Computer Applications*.

[4] T. Sarkar, S. Sanyal, “Digital Watermarking Techniques in Spatial and Frequency Domain”, 2014.

[5] L. K. Saini, V. Shrivastava, ”A Survey of Digital Watermarking Techniques and its Applications”, 2014, *International Journal of Computer Science Trends and Technology(IJCST),* India.

[6] M. S. Islam, U. P. Chong, “A Digital Image Watermarking Algorithm Based on DWT DCT and SVD”, 2014, *International Journal of Computer and Communication Engineering*.

[7] Y. Perwej, F. Parwej, A. Perwej, “An Adaptive Watermarking Technique for the copyright of digital images and Digital Image Protection”, 2012, *The International Journal of Multimedia & Its Application(IJMA)*, Saudi Arabia.

[8] S. S. katariya, ”Digital Watermarking: Review”, 2012, *International Journal of Engineering and Innovative Technology(IJEIT)*.

[9] L. Robert, T. Shanmugapriya, ” A Study on Digital Watermarking Techniques”, 2009, *International Journal of Recent Trends in Engineering*, Coimbatore.

[10] C. T. Hsu, J. L. Wu, “Hidden Digital Watermarks in Images”, 1999, *The Institute of Electrical and Electronics Engineers(IEEE)*.

[11] https://en.wikipedia.org/wiki/Digital_watermarking