Cryptography Based MSLDIP Watermarking Algorithm

Abdelmgeid A. Ali *abdelmgeid@yahoo.com*
Faculty of Science, Computer Science Department
Minia University
Minia, 61519, Egypt

Ahmed H. Ismail *ahamdycs2012@gmail.com*
Faculty of Science, Computer Science Department
Minia University
Minia, 61519, Egypt

Abstract

In recent years, internet revolution resulted in an explosive growth in multimedia applications. The rapid advancement of internet has made it easier to send the data accurate and faster to the destination. Aside to this, it is easier to modify and misuse the valuable information through hacking at the same time. Digital watermarking is one of the proposed solutions for copyright protection of multimedia data. In this paper cryptography based MSLDIP watermarking method (Modified Substitute Last Digit in Pixel) is proposed. The main goal of this method is to increase the security of the MSLDIP technique besides to hiding the watermark in the pixels of digital image in such a manner that the human visual system is not able to differentiate between the cover image and the watermarked image. Also the experimental results showed that this method can be used effectively in the field of watermarking.

Keywords: Cryptography, Encryption, Decryption, Watermarking, Spatial Domain, MSLDIP (Modified Substitute Last Digit in Pixel), Security.

1. INTRODUCTION

Information hiding techniques have recently become important in a number of application areas [1]. The term hiding here can refer to either making the information imperceptible (as in watermarking) or keeping the existence of the information secret (as in steganography) [2]. Information hiding means communication of information by hiding in and retrieving from any digital media. The digital media can be an image, an audio, a video or simply a plain text file. Information hiding is a general term encompassing many sub disciplines. However, generally it encompasses three disciplines: cryptography, watermarking, and steganography [3, 4]. It is graphically shown in (Figure 1.1), Watermarking can be robust or fragile depending upon the application domain.

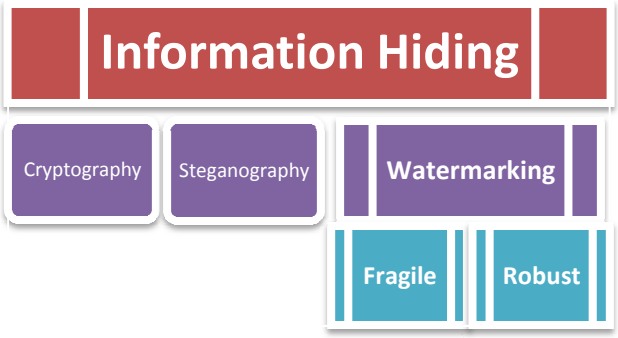

FIGURE 1.1: Information Hiding Disciplines.

Cryptography is an area within the field of cryptology. The name cryptology is a combination of the Greek (cruptos = hidden and logos = study, science). Therefore, the word cryptology literally implies the science of concealing. The cryptography can be divided into two areas: cryptography and cryptanalysis [5]. Cryptanalysis is the area within cryptology which is concerned with techniques for deciphering encrypted data without prior knowledge of which key has been used. This more commonly known as 'Hacking'. The cryptanalyst is the person who tries to find weaknesses in encryption schemes. He will often figure out how to break the cryptography scheme, and then the developer of the scheme will use that information to make it stronger [6].

When people initially tried to communicate over distances, they tried to ensure the secrecy of their communications. The technology of steganography is developed for this goal [7]. The word steganography comes from two Greek words stegauw (steganos) and grafein (graphein) meaning covered writing. It is basically about embedding a secret message in a cover file [8] which looks innocuous. This cover file could be an image file, video file, audio file, text file, or any computer code [4, 9]. Steganography is comprised of two algorithms, one for embedding and one for extraction [10]. A great deal of attention is paid to ensuring that the secret message goes unnoticed if a third party were to intercept the cover file [11].

Watermarking is a technique used to hide data or identifying information within digital multimedia. The discussion will focus primarily on the watermarking of digital images, though digital video, audio, and documents are also routinely watermarked. Digital watermarking is becoming popular, especially for adding undetectable identifying marks, such as author or copyright information. The digital watermarking process embeds a signal into the media without significantly degrading its visual quality. Digital watermarking is a process to embed some information called watermark into different kinds of media called Cover Work [3, 12]. Digital watermarking is used to hide the information inside a signal, which cannot be easily extracted by the third party. Watermarking is used for following reasons, Proof of Ownership (copyrights and IP protection), Copying Prevention, Broadcast Monitoring, Authentication, Data Hiding. Digital watermark is an important research direction for the technique of information hiding, mainly including the characteristics (capacity, invisibility, security, robustness).

2. RELATED WORK

In this section, the MSLDIP Watermarking algorithm will be presented which works on the spatial domain of the cover image. At the first the (SLDIP) will be presented before the (MSLDIP) method. SLDIP method takes the cover image and the watermark as input, convert the blue layer of the cover image into one row, and divide the row into blocks each of which contains 9 values, then consider the watermark is color image then each pixel will be represented in 3 bytes, according to the color image representation (which each pixel is specified by three values one each for red, blue, and green components of the pixel's color and each value represented by one byte, so each pixel will be represented in three bytes) [13].

Each byte in the watermark image will be ranges from 0 to 255, and make each byte value's length equal to 3 digits, for example we have byte of value 15, this value equal to 015 which has length of 3 digits, finally substitute each 9 digits of each pixel with the last digit of each pixel in the current block, so each pixel of the watermark image will be embedded in only one block, and output the watermarked image and 2 keys which be required in the extraction process (Figure 2.1) and (Figure 2.2) [14].

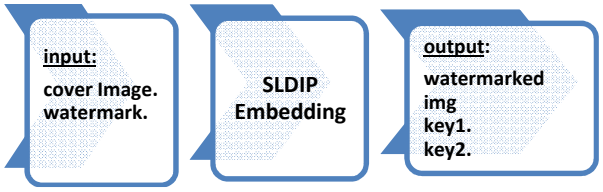

FIGURE 2.1: SLDIP Watermarking Embedding Process [14].

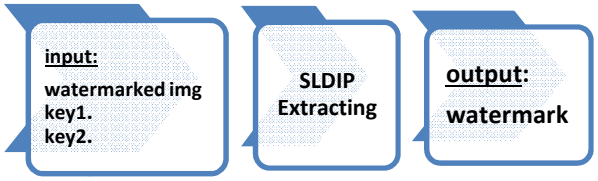

FIGURE 2.2: SLDIP Watermarking Extraction Process [14].

Assuming that watermark image of height 1 pixels and width 1 pixels, and cover image of height 3 pixels and width 3 pixels. The SLDIP will represent the cover image in one row which contains one block of 9 values (125, 255, 086, 192, 145, 210, 035, 099, and 004), and the watermark image will be represented as (230, 105, and 080), the SLDIP will substitute 5 (last digit in cover image) in 125 with 2 (first digit in watermark image) in 230, the result is 122 and also substitutions done until reaching the last digit in the last value of the watermark. The watermarked image will be (122, 253, 080, 195, 140, 215, 030, 098, and 000) [13].

By using this method capacity of embedding has been increased, the maximum area of watermark image that can be embedded in any cover image can be calculated by using this formula [14]:

$$\frac{ImageWidth \times ImageHeight}{9} = watermark_{area}\ (1) \quad [14]$$

If the watermark image is grayscale image this formula can be used:

$$\frac{ImageWidth \times ImageHeight}{3} = watermark_{area}\ (2) \quad [14]$$

Supposing a (8 x 8) cover image, by using equation 1, we can embed colored watermark image of area 7 pixel2 which approximately equals to (2 x 3) colored watermark image, and by using equation 2, a grayscale watermark image of area 21 pixel2 which approximately equals to (4 x 5) grayscale watermark image can be embedded. Notice that SLDIP uses only one layer of the color image neither two nor three layers. This means that we can use this method in color and grayscale images [14].

MSLDIP is a modification on SLDIP by update the substitution step to decrease the difference between the original pixel and the substituted pixel, for example embedding value digit 9 in pixel 100, by using SLDIP the pixel will be 109, but by MSLDIP two possible values can be taken for each substitution and choose the value that has the smallest difference, so the two values will be 109 and 99, then the value with the smallest difference must be chosen, so the pixel value will be 99, the difference will be 1 instead of 9 and this increases the PSNR value of the image [14].

3. PROPSED METHOD

In this section the proposed method will be presented, at the first the proposed method will be divided into two algorithms which are Watermark embedding algorithm and watermark extraction algorithm.

3.1 Watermark Embedding Algorithm

Algorithm: Secured MSLDIP Embedding Algorithm.
Input: Watermark W; Cover Image C; Secret Key K.
Output: Encrypted Watermark W', Secured Watermarked Image SWI.
Steps: (Figure 3.1)

1. Take W and encrypt it by performing RC4 Encryption algorithm with K, the output of this step is called W'.
2. Apply MSLDIP Watermarking Embedding procedure to embed W' in C, the output of this step is called secured watermarked image SWI.

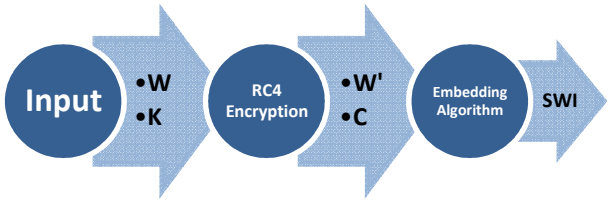

FIGURE 3.1: Modified MSLDIP Embedding Process.

3.2 Watermark Extraction Algorithm

Algorithm: Secured MSLDIP Extraction Algorithm.
Input: Secured Watermarked Image SWI; Secret Key K.
Output: Encrypted Watermark W', Watermark W.
Steps: (Figure 3.2)

1. Apply procedure MSLDIP extraction to extract the encrypted watermark from SWI, the output of this step is called W'.
2. Take W' and decrypt it by performing RC4 Decryption algorithm using K, the output of this step is called W.

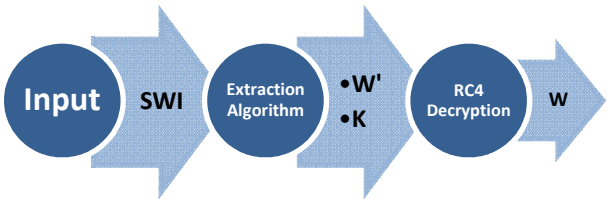

FIGURE 3.2: Modified MSLDIP Extraction Process.

4. EXPERIMENTAL RESULTS

In order to evaluate the performance of the watermarked images, there are some quality measures such as PSNR and MSE.

The **MSE (Mean Square Root)** is defined as an average squared difference between a reference image and a distorted image. It can be calculated by the formula given below

$$MSE = \frac{1}{XY}\left[\sum_{i=1}^{X}\sum_{j=1}^{Y}(c(i,\ j) - e(i,\ j))^2\right] \quad (3)$$

Where X and Y are height and width respectively of the cover image, the c(i, j) is the pixel value of the cover image and e(i, j) is the pixel value of the watermarked image.

The **PSNR (Peak Signal to Noise Ratio)** is an expression for the ratio between the maximum possible value (power) of a signal and the power of distorting noise that affects the quality of its representation. It can be calculated by the formula as

$$PSNR = 10\ log_{10}\left(\frac{L \times L}{MSE}\right) \quad (4)$$

Where L is the peak signal value of the cover image which is equal to 255 for 8 bit images [15].

In order to make the watermarking algorithm more secured, RC4 Encryption Algorithm is merged with the MSLDIP Embedding Algorithm (Figure 4.1), and in the other hand RC4 Decryption Algorithm is merged with the MSLDIP Extraction Algorithm as anyone can know the MSLDIP watermarking algorithm and do the reverse of embedding algorithm and so the watermark can be

known, but by using an encryption algorithm the user who doing the reverse of the MSLDIP embedding algorithm must know the key to extract the correct watermark, if the key has been entered is incorrect the watermark will be fake (Figure 4.2).

Modified MSLDIP have been implemented in MATLAB 2014 platform and the experiment has been conducted on various images.

FIGURE 4.1: Embedding a, b using Modified MSLDIP Watermarking to output the watermarked image c.

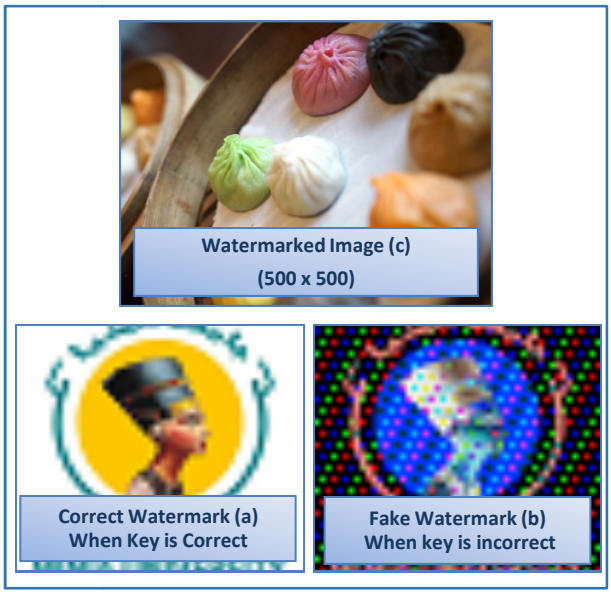

FIGURE 4.2: Watermark Extraction using Modified MSLDIP when input can be correct key and incorrect key.

Modified MSLDIP Watermarking has been applied on set of images different in sizes and the Peak Signal to Noise Ratio (PSNR), and Mean Square Root (MSE) have been calculated, all results recorded in (Table 1).

Cover Image	PSNR	MSE	Watermark Image
(150 x 150)	43.21	3.11	(50 x 50)
(200 x 200)	45.87	1.68	(50 x 50)
(500 x 500)	53.29	0.31	(50 x 50)
(700 x 700)	56.22	0.16	(50 x 50)
(1000 x 1000)	59.82	0.07	(50 x 50)

TABLE 1: Results of applying Modified MSLDIP watermarking on various sizes images.

In (Figure 4.3), Chart showing the results of MSE and PSNR between the cover image and watermarked image in the Modified MSLDIP Algorithm.

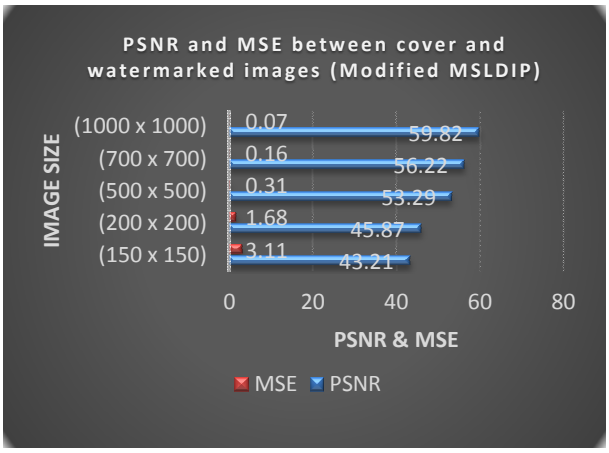

FIGURE 4.3: Chart showing the results of Modified MSLDIP.

Modified MSLDIP has been compared with [16] (Table 2), supposed four cover image with squared sizes 128, 256, 512, and 1024, and a watermark with full capacity with cover images according to [16], thus the full watermark capacity can be calculated using cover image sizes according to [16] by using formula

$$Round\ up\left(\sqrt{\frac{ImageWidth\ \times ImageHeight}{24}}\right) = watermark\ side\ length \qquad (5)$$

Then Modified MSLDIP has been compared with [14] (the previous version method) (Table 3), the results have been approximately equal to each other but in the modified MSLDIP the user who extracting the watermark from the watermarked image must have the key to get the correct watermark if not the watermark which has been extracted from the watermarked image will be fake, thus the Modified MSLDIP can be better than MSLDIP as the first one is more secured than the other.

Finally the Modified MSLDIP has been compared with [17], supposed the grayscale baboon.bmp as a cover image and, the grayscales lena.bmp, and barbara.bmp as watermark and the full capacities of the embedded watermark according to each algorithm have been calculated using formulas

$$Round\ up\left(\sqrt{\frac{CoverImageWidth \times CoverImageHeight}{3}}\right) = watermark\ side\ length\ (Modified\ MSLDIP) \quad (6)$$

$$Round\ up\left(\sqrt{\frac{CoverImageWidth \times CoverImageHeight}{8}}\right) = watermark\ side\ length\ of\ [14] \quad (7)$$

Cover Image	Watermark FC [10]	[16] 3rd Bit		Modified MSLDIP	
		PSNR	MSE	PSNR	MSE
Baboon 128	(27 x 27)	31.68 dB	44.50	46.90 dB	1.33
Bird 256	(53 x 53)	31.68 dB	44.50	46.99 dB	1.30
Boat 512	(125 x 125)	31.68 dB	44.50	46.10 dB	1.60
Pepper 1024	(210 x 210)	31.68 dB	44.50	47.17 dB	1.25

TABLE 2: Results Comparison between [16] 3rd Bit and Modified MSLDIP.

Cover Image	Watermark Image	[14] MSLDIP		Modified MSLDIP	
		PSNR	MSE	PSNR	MSE
(600 x 600)	(200 x 200)	43.10 dB	3.18	43.06 dB	3.22
(768 x 768)	(200 x 200)	45.66 dB	1.77	45.63 dB	1.78
(1024 x 1024)	(200 x 200)	48.23 dB	0.98	48.22 dB	0.98
(1280 x 1280)	(200 x 200)	49.69 dB	0.67	49.46 dB	0.74
(1500 x 1500)	(200 x 200)	51.29 dB	0.48	51.19 dB	0.49

TABLE 3: Results Comparison between [14] MSLDIP and Modified MSLDIP.

Cover Image	Watermark Image	[17]	Modified MSLDIP
		PSNR	PSNR
baboon.bmp (512 x 512)	lena.bmp (64 x 64)	58.64 dB	52.00 dB
baboon.bmp (512 x 512)	Barbara.bmp (64 x 64)	58.99 dB	51.81 dB
Watermark (FC) applying equations (6,7) With Cover Image size (512 x 512)		(181 x 181)	(295 x 295)

TABLE 4: Results Comparison between [17] and Modified MSLDIP.

5. COMPARATIVE EVALUATION

From the comparison in table (2), the reason of why Modified MSLDIP has been compared with [16] 3rd Bit? Has been clarified as, in Modified MSLDIP substitutions can change the value of pixel which the difference ranges from 0 to 5 and change in the 3rd Bit in pixel can change the value of pixel which the difference ranges from 0 to 7 which include the Modified MSLDIP difference range. However results in Modified MSLDIP are better.

From the comparison in table (3), the results of the modified MSLDIP are compared with the results of the MSLDIP [14] (the previous version), and It can be concluded that the results were very close, as the difference didn't not exceed the one after the decimal point, but in the modified MSLDIP the data which has been watermarked is more secured with a key, it can be proved that the modified MSLDIP technique is better.

From the comparison in table (4), the results of modified MSLDIP are compared with results of [17], and from the comparison it can be concluded that the two algorithm have very good PSNR results that mean no one can discover the watermark when looking at the image, also it can be conducted that the watermark full capacity of modified MSLDIP is greater than [17], suppose cover image (512 x 512) and watermark (256 x 256) algorithm of [17] cannot embed the watermark in cover image but the modified MSLDIP can embed this watermark successfully.

After Implementing and analyzing the results, conclude that, the visual quality of the image doesn't change significantly, on the other hand this algorithm is more robust than LSB technique [17], because in LSB technique some attackers can possibly zero out several least significant bit of pixels of the image and hence clear the watermark. This technique has increased the capacity of watermark in embedding process.

6. CRITICAL DISCUSSION

Watermarking algorithm proposed in [16], the full capacity of watermark which can be embedded in cover image of size 128x128 pixels is 682.67 px^2 that approximately equal to watermark of size 26x26 pixels however in our proposed method the full capacity of watermark is 1280.44 px^2 that approximately equal watermark of size 42x42 pixels, that mean our proposed method can embed watermark with capacity larger than [16], also in [16] there isn't any way to prevent unauthorized users from accessing the watermark, however in our proposed method the watermark is encrypted using RC4 with a key which only users who have this key can access the watermark, that mean in our proposed method the watermark is more secured.

Watermarking algorithm proposed in [14], regardless of it can embed watermark with capacity equal to our proposed method, in [14] there isn't any way to prevent unauthorized users from accessing the watermark, however in our proposed method the watermark is encrypted using RC4 with a key which only users who have this key can access the watermark that mean in our proposed method the watermark is more secured.

Watermarking algorithm proposed in [17], the full capacity of watermark which can be embedded in cover image of size 512x512 pixels is 32768 px^2 that approximately equal to watermark of size 181x181 pixels however in our proposed method the full capacity of watermark is 87381.33 px^2 that approximately equal watermark of size 295x295 pixels, that mean our proposed method can embed watermark with capacity larger than [17], also in [17] there isn't any way to prevent unauthorized users from accessing the watermark, however in our proposed method the watermark is encrypted using RC4 with a key which only users who have this key can access the watermark, that mean in our proposed method the watermark is more secured.

7. CONCLUSION

Digital watermarking with cryptography is the current area of research where lot of scope exists. Currently digital watermarking with cryptographic technique is being used by several countries for secretly transfer of hand written documents, text images, financial documents, internet voting etc.

This paper starts from some basic knowledge of information hiding categories includes digital image watermarking, and from results conclude that the visual quality of the image doesn't change significantly, this algorithm is more robust than LSB technique because in LSB technique some attackers can possibly zero out several least significant bit of pixels of the image and hence clear the watermark, this algorithm is more secure because of using cryptographic technique which has been merged with the watermarking technique, and this technique has increased the capacity of watermark which will be embedded. In the future, the aim of this paper is to extend the cryptography to higher dimensions and apply it in frequency domain in order to consider more security and robustness.

8. REFERENCES

[1] F. A. P. Petitcolas, R. J. Anderson and M. G. Kuhn, "Information Hiding – A Survey", proceedings of the IEEE, Special Issue on Protection of Multimedia Content, vol. 87(7), pp. 1062 - 1078, July 1999.

[2] I. J. Cox, m. L. Miller, J. A. Bloom, J. Fridrich and T. Kalker, "Digital Watermarking and Steganography", ISBN 978-0-12-372585-1, 2nd edition, Elsevier inc, 2008.

[3] Preeti Gupta, “Cryptography based digital image watermarking algorithm to increase security of watermark data”, International Journal of Scientific & Engineering Research, Volume 3, Issue 9 (September 2012) ISSN 2229-5518.

[4] J. A. Mathew, "Steganographic Techniques for Subliminal Communication in Open Systems Environment", Sam Higginbottom Institute of Agriculture, Technology and Sciences, PHD. Thesis, 2010.

[5] Jan C A, Van Der Lubbe, "Basic Methods of Cryptography", English translation Cambridge University Press 1998.

[6] E. Cole, "Hiding In Plain Sight: Steganography and The Art of Covert Communication", ISBN 0-471-44449-9, Wiley publishing, inc, 2003.

[7] S. A. Baker and Dr. A. S. Nori, "Steganography in Mobile Phone over Bluetooth", International Journal of Information Technology and Business Management (JITBM), Volume 16, Number 1, Pages 111- 117, 29 August 2013.

[8] T. Morkel, "Image Steganography Applications for Secure Communication", Master of Science (Computer Science) Thesis, Faculty of Engineering, Built Environment and Information Technology University of Pretoria, Pretoria, May 2012.

[9] F.C.Gonzalez, "Counter Terrorist Steganography Search Engine", Master of Science Thesis, Department of Aerospace, Power and Sensors, Royal Military College of Science, Shrivenham, Cranfield University, 2002.

[10] S. A. Sohag, Dr. M. K. Islam and M. B. Islam, "American Journal of Engineering Research (AJER)", Volume 2, Issue 9, Pages 118 - 126, 2013.

[11] S.Deepa and R.Umarani, "A Study on Digital Image Steganography", International Journal of Advanced Research in Computer Science and Software Engineering, International Journal of Advanced Research in Computer Science and Software Engineering, Volume 3, Issue 1, January 2013.

[12] B Surekha, Dr GN Swamy, “A Spatial Domain Public Image Watermarking”, International Journal of Security and Its Applications Vol. 5 No. 1, January, 2011M. Abdullatif, A. M. Zeki, J. Chebil, and T. S. Gunawan, "Properties of Digital Image Watermarking".

[13] Ahmed A. Radwan, Ahmed Swilem, Al-Hussien Seddik, "A High Capacity SLDIP method", ICICIS, July 2011.

[14] Abdelmgeid A. Ali, Ahmed A. Radwan, and Ahmed H. Ismail, "Digital Image Watermarking using MSLDIP (Modified Substitute Last Digit in Pixel)", IJCA, Volume 108 – No 7, Pages 30-34, December 2014.

[15] Amit Kumar Singh, Nomit Sharma, Mayank Dave, Anand Mohan, "A Novel Technique for Digital Image Watermarking in Spatial Domain", 2012 2nd IEEE International Conference on Parallel, Distributed and Grid Computing.

[16] Deepshikha Chopra, Preeti Gupta, Gaur Sanjay, Anil Gupta, "LSB based digital image watermarking for gray scale image", IOSRJCE, October 2012.

[17] Krishna Kumar, and Shashank Dwivedi, "Digital Watermarking using Asymmetric Key Cryptography and Spatial Domain Technique", IJARCSMS, Volume 2, Issue 8, August 2014.