Modified Least Significant Bit(LSB) Matching Technique for Robust Information Hiding

[1] Somnath Maiti, [2] Manas Ranjan Nayak, [3] Subir Kumar Sarkar
[1] Research Scholar, [2] Research Scholar , [3] Professor
[1]Electronics &Tele Communication Engineering Department,
[1] Department of E.T.C.E., Jadavpur University, Kolkata, India

Abstract— **The effortless accessibility of digital information and the simplicity of the digital systems have left the contents over the digital media extremely insecure. The need for mechanisms to protect such information is undeniable. Digital watermark based information hiding is a prospective means for copyright protection, authentication, integrity verification and intellectual property right protection. The proposed method is a modification of LSB matching technique where addition or subtraction of bits to or from the cover image is decided by a binary function. In general, LSB insertion is not at all a technique for data hiding. On the flip side, it's very easy to extract LSBs with simple programs. Its comparatively high data rate naturally fits for steganography, where robustness is not such an important constraint. The technique miserably fails to resist even simple processing like compression/decompression. LSB insertion is almost useless for digital watermarking, where it must face malevolent attempts of its destruction. The proposed method is a modification of LSB matching technique where addition or subtraction of bits to or from the cover image is decided by a binary function. The embedding and extraction are performed using pair of pixels. Therefore this method allows better embedding scheme with fewer changes to the cover image. Additional security is imposed with encrypted watermark by means of Symmetric Key Cryptography. The results reflect a vastly improved performance of LSB matching as data hiding technique.***(Abstract)*

Index Terms— **Digital Watermark, Information Hiding, Copyright Protection, Authentication, LSB Matching , Steganography, Robustness, Symmetric Key Cryptography.** *(key words)*

I. INTRODUCTION

In recent time multimedia transmission on the digital communications through the internet faces a wide range of security issues [1]. Accordingly, powerful digital techniques are essential to establish the right on digital data during its transmission on the internet. One of the great potential solutions used to protect data is data hiding [2]. Data hiding is the art of invisible communication by hiding a secret message in a digital cover media such as images [3] text [4], audio [5], video [6] and network traffic[7] ,without being dubious[8] . Because digital images have a great deal of redundant data, there has been an increased interest in utilizing them as cover media for data hiding purposes [9]. Information can be hidden in many different ways in multimedia contents. Data hiding is a kind of concealment that allows the imperceptible transmission of secret data between two or more parties. Over the past decade, data hiding schemes encompasses two broad areas namely digital watermarking and steganography. The aim of a digital watermarking technique is to protect the ownership of copyright, and as such, its robustness is a critical research topic. However, the main application of the steganographic technique is the sharing of secret. The most simple and attractive way is the direct encoding of every bit of information in the cover image or selectively embed the message in visually insignificant areas that draw less attention in other word ,those areas where there is a great deal of natural color variation[10]. The message may also be scattered randomly throughout the image. The well known technique is known as Least Significant Bit (LSB) encoding. There are two distinct techniques used in LSB based data embedding [11].

1. **LSB replacement/substitution:** Technique involves in substitution of message bit in place of the LSB of the pixel in cover image. LSB substitution is intrinsically asymmetric, i.e. an even valued pixel will either remain unchanged or be incremented by one. The reverse is true for odd-valued pixels. Only LSB is modified [12].
2. **LSB matching:** Technique of matching the LSB of pixel in cover image to the message bit. Matching produces more bit modification even there are possibilities that all bits may required to be changed. Consequently, pixel value is arbitrarily incremented or decremented, thus removing the asymmetry of even and odd pixels [12].

Both methods are comparable in terms imperceptibility image after hiding the message and simpler to implement. But, the steganalysis of LSB matching method is quite difficult as compare to that of LSB substitution [13**].** LSB insertion modifies the LSBs of each colour 24 or 8 bit images.LSB insertion is very much exposed to a lot of signal transformations which rely on basic principle of eliminating redundancy of cover data to reduce the data rate of images. The lossy compression like JPEG will destroy it completely. The main reason is that the gap in the Human Visual System (HVS) that LSB insertion tries to exploit is highly sensitive to added noise [14].Any kind of intentional and unintentional modification of cover image are likely to destroy the

embedded message. In general, LSB insertion is not at all a technique for data hiding. On the flip side it's very easy, to extract LSBs even with simple programs [15]. Since it miserably fails to resist even for simple processing, LSB insertion is almost useless for digital watermarking, where it must face malevolent attempts of its destruction, moreover normal transformations like compression/decompression or conversion to analog (printing or visualization)/conversion to digital (scanning)[16]. Its comparatively high data rate naturally fits for steganography, where robustness is not such an important constraint. We can try to improve one of its major drawbacks i.e. robustness. This is usually accomplished with two complementary techniques in order to protect the integrity of the message, firstly [17]

a) Original message is encryption before insertion and thereby enhancing the strength of detection.
b) Randomizing the placement of the bits using suitable function, so that it's almost impossible to rebuild the message.

Secondly, unusually big files exchanged between two peers, are likely to arise suspicion. Since we need to have small image file sizes, we should resort in using 8-bit images if we want to communicate using LSB insertion, because their size considered as normal [18].

The paper is organized in the following manner. The section II contains the literature survey and in section III we described the algorithm for encoding and decoding process. The section IV contains the results and discussion of our experiment and section V contains the conclusions. Finally the paper ended with acknowledgement and references.

II. LITERATURE SURVEY

As we know information hiding based on watermarking principle can be implemented for spatial domain as well as for frequency domain. In comparison with spatial domain Frequency domain techniques are more robust but spatial domain provides facility in terms of lower computational complexity, ease of hardware implementation and higher perceptual quality [19]. J. Mielikainen proposed a modification of basic LSB matching technique wherein fewer changes to the cover image resulted from same amount of information embedding compared to original LSB matching method. Thus making the technique more robust than the previous one [20].Some areas in cover image such as smooth areas, repetitive patterns and regions with linearly varying intensities of pixels are called fragile regions. As such, the method is not applicable in such region as small change can't be disguised. Further, the same method has been improved upon by Quinhue et al. [21]. They selected suitable regions where LSB embedding and it is found that the modification can resist histogram based steganalysis. Ling Xi et al. [22] proposed another improvement of LSB Matching algorithm based on modification of pixels with adjacent intensity. Since the modification in one pixel causes change in two adjacent bins of histograms which is undesirable as there are high chances of being detected. They improved the robustness, by embedding two bits in a pair of complimentary pixels by increasing 1 to the pixel with lower intensity and decreasing 1 from the pixel with higher intensity keeping histogram unchanged. Although there are some methods that can further reduce the numbers of modified pixels, the hiding capacity is not as great as in Mielikainen's method. For example, the numbers of modified pixels of Matrix Coding are lower than that of Mielikainen's method while embedding. The Matrix Coding was first proposed by Crandall [23]. Westfeld has implemented Matrix coding for colour images, in which the embedding algorithm has on the occurrences of close pairs of colors [24]. He also mentioned that the detector can be applied to grayscale images by converting gray pixels into the red, green, and blue (RGB) components of a single color pixel. However, the number of its hiding bits is only three-sevenths of the number of the cover pixels. Having a high embedding capacity and satisfied numbers of modified pixels makes Mielikainen's method superior to other methods. Furthermore, Zhang et al. [25] proposed their "Hamming+1" Scheme to reduce the number of modified pixels. However the embedding capacity is still lower than Mielikainen's method. Zhang and Wang [26] proposed their 'exploiting the modification direction' (EMD). In the special case of their method, each pixel can embed $\log_2 3$ secret bits. But this method changes secret data, which are represented as binary digits, to ternary digits. Secret data are usually represented as binary digits in the computer system. Ternary representation is not as convenient as binary representation. In [27], the authors proposed a method called Complexity Based LSB matching. The method employs the strategy of adaptively determination of secure locations of an image embedding in order to increase the security against attacks. An hybrid approach involving both LSB matching and LSB replacement presented in [6.28]. It was claimed that proposed approach stores two bits in a pixel and increase the level of security. In [29], a data hiding algorithm based on interpolation, LSB substitution, and histogram shifting was proposed by the authors. The interpolation is used to adjust embedding capacity with low image distortion; the embedding process is then applied using LSB substitution and histogram shifting methods. The LSB substitution is improved further by using a bit inversion technique[30]. The secret data is hidden after lossless compression of smooth areas of the image, which results in fewer number of modified cover image pixels. A bit inversion technique is then applied where certain LSBs of pixels are modified if they occur in a particular pattern. The detector of Lyu and Farid [31] will be to some extent effective, but it has not been evaluated against a pure LSB matching steganography scheme. Xiaomei Quan and Hongbin Zhang [32] proposed Lossless Data hiding scheme based on LSB Matching where message bit is embedded via LSB Matching instead of LSB replacement. The method gives better performance than existing methods. Andrew D. Ker [31] proposed a method for gray scale image where he used a Histogram Characteristic Function (HCF) introduced by Harmsen for the detection of steganography in color images but ineffective on grayscale images. Ker suggested that HCF scheme has bad performance in grayscale images since it is a lack of sparsity in the histogram. For applying HCF two novel ways are introduced: calibrating the output using a down-sampled image and computing the adjacency histogram instead of the usual histogram. This is also verified through rigorous experiments and performs consistently as compared to earlier detectors. Ker suggested that HCF scheme has inferior performance in greyscale images since it is a lack of sparsity in the histogram. For applying HCF two novel ways are introduced: calibrating the output using a down-sampled image and computing the adjacency histogram instead of the usual histogram. Which results is greatly improved and consistent as compared to earlier one. In [33], the authors have compared LSB Matching to a low pass filter through the histogram of the image and found that the number of high frequency components is very less in comparison with original cover image. But later in [34], it is found that for greyscale images this method will not be working well. As a remedy, the author has proposed techniques using down-sampled image and adjacency histogram instead of traditional histogram. The authors,

used dynamic programming strategy to get the optimal solution, which has less computation complexity with improved performance [36]. Authors proposed a system to assess the performance of different orders for LSB matching. They adopted a method to search for a near-optimal solution among all the permutation orders. The proposed method can improve imperceptability of the stego image and thereby decrease the probability of detection [37].

III. PROPOSED METHOD OF EMBEDDING AND EXTRACTION

The approach of LSB Matching in this projected scheme is a modified version of the algorithm proposed by Jarno Mielikainen [35]. In the proposed method we use greyscale cover messages and same size copyright information as binary watermark. The embedding scheme is performed with two cover and watermark image pixels at a time. Let X_i and X_{i+1} are the pixels of cover image and M_i and M_{i+1} are the pixels of watermark image. In the addition or subtraction of message bit to the cover image is done by means of a binary function $f(l, n)$ is given by

$$f(l,n) = LSB(\lfloor \frac{l}{2} \rfloor + n) \quad (1)$$

Where l and n are two cover pixels which satisfies $f(l,n) \neq f(l,n+1), f(l-1,n) \neq f(l+1,n)$

Let I be the original grayscale original image with size of $a \times b$ and represented as

$I = X(i, j);\ 0 \leq i < a,\ 0 \leq j < b, X(i, j)\ \varepsilon\{0, \ldots 255\}$ (2)

Let W be the original grayscale watermark with size of $m \times n$ and characterized as:

$W = M\ (i, j);\ 0 \leq i < m,\ 0 \leq j < n,\ M\ (i, j)\ \varepsilon\ \{0, 255\}$ (3)

Then embedding is given by

$$If\ \sum_{i=0}^{255} M_{i+1} \neq f(X_i, X_{i+1}) \rightarrow Y_{i+1} = X_{i+1} + M_{i+1}\ \&\&\ \sum_{i=0}^{255} Y_i = X_i + M_i \quad (4)$$

$$If\ \sum_{i=0}^{255} M_{i+1} = f(X_i, X_{i+1}) \rightarrow Y_{i+1} = X_{i+1} - M_{i+1}\ \&\&\ \sum_{i=0}^{255} Y_{i+1} = X_{i+1} + M_{i+1} \quad (5)$$

$$If\ \sum_{i=0}^{255} M_{i+1} \neq f(X_i, X_{i+1}) \rightarrow Y_i = X_i + M_i\ \&\&\ \sum_{i=0}^{255} Y_{i+1} = X_{i+1} + M_{i+1} \quad (6)$$

$$If\ \sum_{i=0}^{255} M_{i+1} \neq f(X_{i-1}, X_{i+1}) \rightarrow Y_i = X_i + M_i\ \&\&\ \sum_{i=0}^{255} Y_{i+1} = X_{i+1} + M_{i+1} \quad (7)$$

The choice of addition or subtraction for both even and odd valued regions is performed separately. In both the regions the increment or decrement selection is made to minimize the absolute value of differences between cover and stego images, which avoids imbalance of LSB replacement. The extraction algorithm is same as embedding algorithm only the difference is given below

$$If\ \sum_{i=0}^{255} M_{i+1} = f(X_i, X_{i+1}) \rightarrow M_{i+1} = Y_{i+1} - X_{i+1}\ \&\&\ \sum_{i=0}^{255} M_i = Y_i - X_i \quad (8)$$

$$If\ \sum_{i=0}^{255} M_{i+1} \neq f(X_i, X_{i+1}) \rightarrow Y_{i+1} = Y_{i+1} - X_{i+1}\ \&\&\ \sum_{i=0}^{255} M_i = Y_i - X_i \quad (9)$$

$$If\ \sum_{i=0}^{255} M_{i+1} = f(X_{i-1}, X_{i+1}) \rightarrow Y_i = X_i - Y_i\ \&\&\ \sum_{i=0}^{255} M_{i+1} = Y_{i+1} - X_{i-1} \quad (10)$$

$$If\ \sum_{i=0}^{255} M_{i+1} \neq f(X_{i-1}, X_{i+1}) \rightarrow Y_i = Y_i - X_i\ \&\&\ \sum_{i=0}^{255} Y_{i+1} = Y_{i+1} - X_{i-1} \quad (11)$$

A. SYMMETRIC KEY CRYPTOGRAPHY

IV. To improve the security of the proposed approach an encryption algorithm is added by means of Symmetric Key Cryptography. The watermark is encrypted via Symmetric Key Cryptography, which protects the information content from attackers. The encryption algorithm uses a single key to encrypt the greyscale logo as well as the same key is used in decryption the algorithm in order to decrypt the logo in decoder section. The encryption algorithm used in this approach converts each pixel of watermark into binary, reverse it and store the quotient and reminder by dividing the reversed string by a key. The same key is used in the decryption to get the original value of watermark [38].

Let *'p'* be a pixel of greyscale logo used as watermark and 'Ψ_k' be the encryption cipher, where '*k*' is the key. If '*q*' is the cipher, then

$$q = \Psi_k(p) \quad (12)$$

To decrypt the cipher we use the decryption cipher, ξ_k.

$$V.\ \xi_k(q) = \xi_k(\Psi_k(p)) = p \quad (13)$$

This is because decryption is essentially an inverse operation of encryption, that is

$$\xi_k = \Psi_k - 1 \quad (14)$$

A. ENCODER AND DECODER

For G be the original grayscale cover image with size of a × b and represented as

$G = C\ (u, v)\ ;\ 0 \leq u < a,\ 0 \leq v < b, C\ (u, v)\ \varepsilon\{0, \cdots 255\}.$ (15)

Let 'L' be the original grayscale watermark with size of c × d and characterized as

$L = Y\ (u, v)\ ;\ 0 \leq u < c,\ 0 \leq v < d,\ Y\ (u, v)\ \varepsilon\ \{0, \cdots 255\}\ .$ (16)

After encryption by applying Symmetric Key Cryptography method the watermark changed to L_E and defined as

$L_E = Y_E\ (u, v)\ ;\ 0 \leq u < r,\ 0 \leq v < s,\ Y\ (u, v)\ \varepsilon\ \{0, \cdots 255\}\ .$ (17)

Based on the LSB Matching technique the watermark is embedded within the image and is given by

$$\boldsymbol{F}_{encoder:} \quad \sum_{u=0}^{p-1} \sum_{v=0}^{q-1} G(u,v).f(D_b, q, L_E, B_d) \rightarrow G_E \quad (18)$$

Where G_E is the watermarked image with same dimension of original image, D_b and B_d are decimal to binary and Binary to decimal function. The same process is followed during the extraction of the watermark and it is defined as.

$$\boldsymbol{F}_{decoder:} \quad \sum_{u=0}^{p-1} \sum_{v=0}^{q-1} G_E(u,v).f(D_b, q, L_E, B_d) \rightarrow L_E \quad (19)$$

VI. RESULTS AND DISCUSSION

Fig. 1 *Gray Scale Watermark*

Fig.2 *Original grayscale images*

Fig. 3 *Encrypted Watermark*

Fig. 4 *Watermarked Images*

This segment describes the results of the proposed scheme by means of imperceptibility and Robustness. Moreover, the outcomes are assessed with some state of the art techniques to judge the performance of the scheme. To validate the performance of the scheme, a set of standard grayscale images of size 255× 255 and one grayscale watermark of size 255× 255 are used. The grayscale watermark image is given in ***Figure 1*** and the test grayscale images are given in ***Figure 2***, the encrypted watermark and watermarked images are given in **Figure *3*** and ***4***. For straightforwardness of illustration only four sample images are presented to prove the accuracy of the proposed scheme. The watermark is embedded within the images using LSB Matching technique. As a result of embedding, original image experiences quality loss which is evaluated through some well-known quality measures to ensure the invisibility of the embedded watermarks in terms of imperceptibility. Figure 5 shows the result of imperceptibility by comparing original image and watermarked Image using bar chart. From the result of Mean Square Error it can be observed that all the values lie below 1.52 which conforms less probability of quality loss.

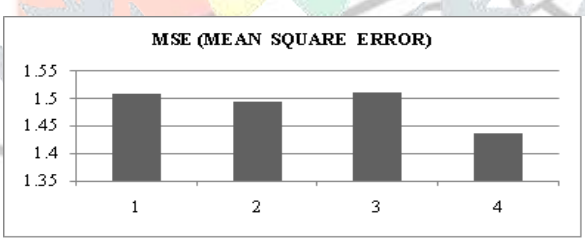

Fig.5 *Performance analysis of Mean Square Error (MSE)*

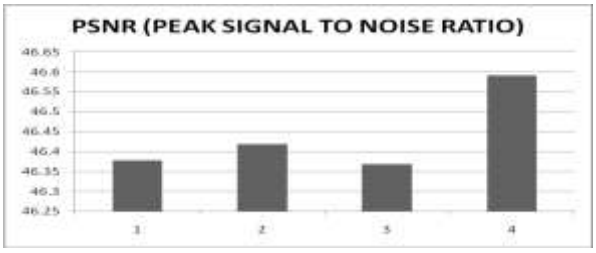

Fig. 6 *Performance analysis of PSNR*

The peak signal to noise ratio (PSNR) value of original image verses watermarked image in figure 6 ranged from 46.35dB to 46.59 dB. This shows higher degrees of imperceptibility have been achieved. The SNR value for original image verses watermarked image in Figure 7 varies from 39dB to 40 dB. High degree of imperceptibility has been established in figure7. The maximum value for Universal image Quality Index (UIQI) in figure 8 is one, in projected approach all the values are close to 1 which indicates superior quality of stego image i.e minimal difference between watermarked image and original image. The structural similarity between the watermarked image and original image are very close to and utmost value for both Structural

Similarity Index Measure (SSIM) and Mean Structural similarity Measure (MSSIM) given in Figure 9 and 10 is 1. In the present scheme both the values are approaching one for different images under our investigation .

Robustness of the present work is tested against different intentional and unintentional attacks like, Rotation, Scaling, Cropping, Noise Addition, JPEG Compression and so forth. The outcome against different kind of signal impairments is presented using bar charts in Figure 11, which signifies the successful retrieval of the embedded bits and their quality. Robustness analysis shows the quality of the recovered bits which can be achieved by measuring Weighted Peak Signal-to-Noise Ratio (WPSNR) , Normalized Cross-Correlation (NCC), and Bit Error Rate (BER). From the results of robustness one can observe that the value of WPSNR is good for different type of attack and the highest value is around 51 dB.

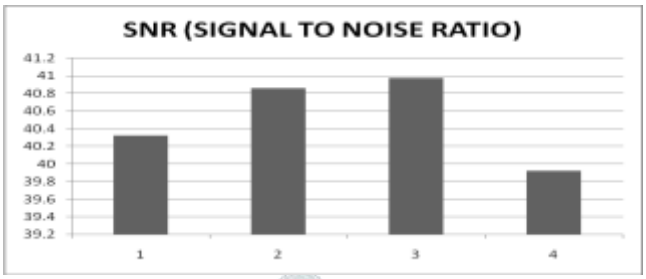

Fig.7 *Performance analysis by SNR*

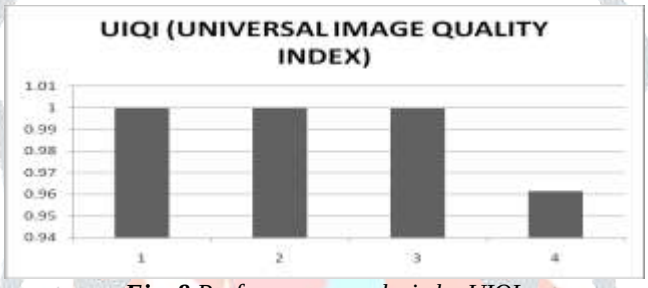

Fig. 8 *Performance analysis by UIQI*

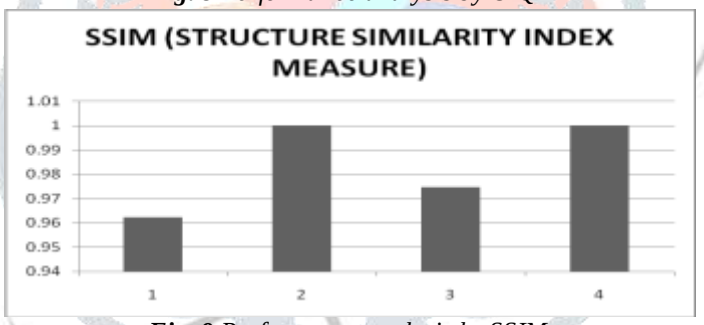

Fig. 9 *Performance analysis by SSIM*

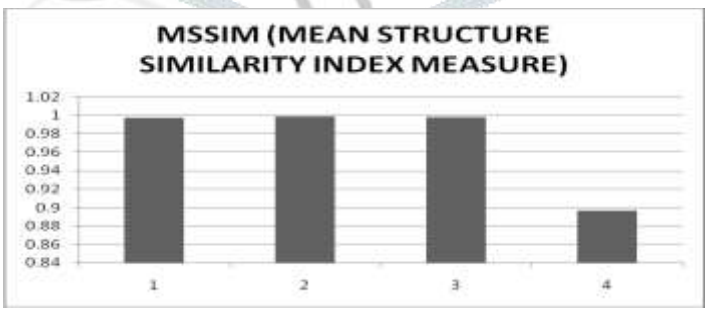

Fig.10 *Performance analysis by MSSIM*

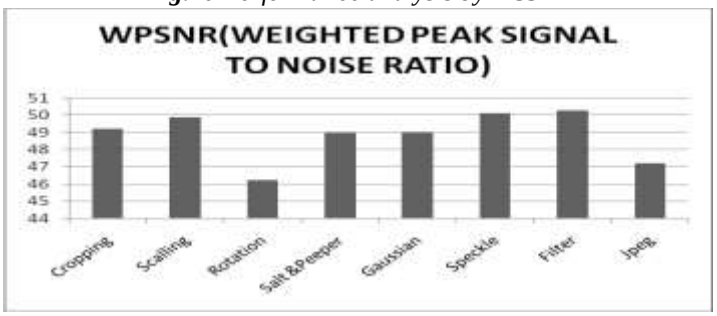

Fig.11 (i) *Performance analysis of WPSNR*

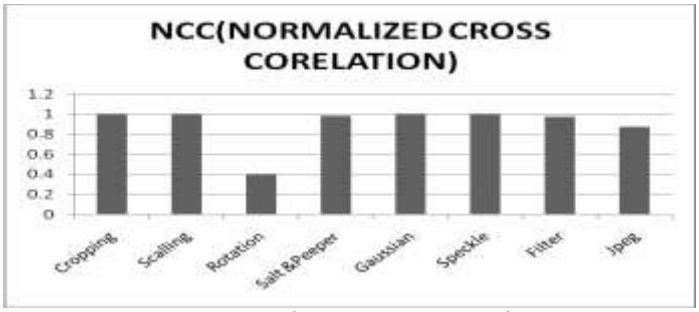

Fig.11 (ii) *Performance analysis of NCC*

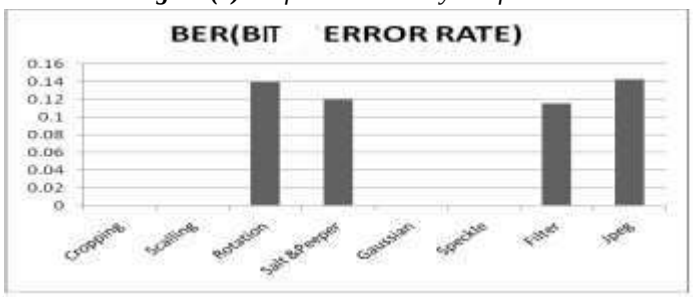

Fig.11 (iii) *Performance analysis of BER*

								
Original Water mark	Cropping	Scaling	Rotation	Salt & Pepper	Gaussian noise	Speckle	Filter	Jpeg

Fig.12 *Recovered watermark after different attacks.*

The Normalized cross correlation (NCC) values are also very high except in the cases of the JPEG and Scaling attack. In addition to the superior value of structural similarity (SSIM & MSSIM) ,the bit error rate(BER) is also very low except rotation and Gaussian noise attack. In short the proposed scheme is robust against most of the intentional and unintentional impairments. Figure 12 shows recovered watermarks after applying different attacks in decrypted form. To validate the performance of the projected technique, an assessment among few state of the art algorithms is presented in Table 1. The result of comparison confirms better imperceptibility and enhanced capacity of the scheme. In Table1 shows the result of comparison which confirms better imperceptibility and enhanced embedding capacity of the scheme.

Table 1*. Performance Comparison of Results with other methods*

Method	PSNR(dB)
Proposed Method	45.37
Mielikainen's Method [35]	33.05
Optimal LSB substitution by dynamic programming [36]	38.34
Pair wise LSB matching by immune programming[37]	38.05

VII. CONCLUSION

In this paper a spatial domain LSB matching technique for gray scale image is proposed. The ease of implementation and low computation complexity in spatial domain is reason for choice of embedding domain. LSB matching is an widely accepted method for cryptography but it is not intentional or unintentional attach resistant. This technique embeds encrypted watermark by taking two cover and encrypted watermark image pixels at a time. This method offer very less amount of distortions to the host image after embedding the watermark to the host images. The PSNR value of original image verses watermarked image ranged from 46.35dB to 46.59 dB. So a higher degree of imperceptibility has been achieved without much sacrificing the robustness against attack. The enhancement of security of the scheme is further improved by the addition of encryption of watermark. Furthermore

Comparison with some other recent algorithm recommends the superiority of the scheme for copyright protection of digital documents.

VIII. ACKNOWLEDGMENT

Authors thankfully acknowledge the financial support for this research work obtained from UGC UPE-II "Mobile computing and innovative applications [Code: MIAJRF-1]"

IX. REFERENCES

[1] Alexander Herringel, Joseph Ó Ruanaidh, Holger Petersen, Shelby Pereira, Thierry Pun, "Secure Copyright Protection Techniques for Digital Images", 2nd Information Hiding Workshop, 1998
[2] F. Huang, Y. Zhong, and J. Huang, "Improved algorithm of edge adaptive image steganography based on LSB matching revisited algorithm", Lecture Notes in Computer Science, Springer Berlin Heidelberg, vol.8389, pp. 19–31, 2014.
[3] B. Mohd, S. Abed, B. Na'ami, and T. Hayajneh, "Hierarchical steganography using novel optimum quantization technique", Signal, Image and Video Processing (SIViP), vol. 7, no. 6, pp. 1029–1040, 2013
[4] A. Odeh, K. Elleithy, and M. Faezipour, "Steganography in text by using MS word symbols". Proc. Zone 1 Conference of the American Society for Engineering Education (ASEE Zone 1), Bridgeport, CT, USA, 2014, pp. 1–5.
[5] P. Pathak, A. Chattopadhyay, and A. Nag, "A new audio steganography scheme based on location selection with enhanced security". Proc. International Conference on Automation, Control, Energy and Systems (ACES), Hooghy, India, 2014, pp. 1–4.
[6] M. Beno, A. George, I. Valarmathi, and S. Swamy, "Hybrid optimization model of video steganography technique with the aid of bi orthogonal wavelet transform", Journal of Theoretical and Applied Information Technology, vol. 63, no. 1, pp. 190–199, 2014.
[7] W. Mazurczyk, P. Szaga, and K. Szczypiorski, "Using transcoding for hidden communication in IP telephony", Multimedia Tools and Applications, vol. 70, no. 3, pp. 2139–2165, 2014.
[8] Neil F. Johnson, Sushil Jajodia, George Mason University, "Exploring Steganography: Seeing the Unseen", IEEE Computers, February 1998, pp. 26-34
[9] W. Bender, D. Gruhl, N. Morimoto, A. Lu, "Techniques for Data Hiding" IBM Systems Journal, Vol. 35 Nos 3&4, 1996
[10] Neil F. Johnson, Sushil Jajodia, Center for Secure Information System, George Mason University, "Steganalisys of Images Created Using Current Steganography Software", http://isse.gmu.edu/~csis
[11] CS Chan, "On using LSB matching function for data hiding in pixels", Fundamenta Informaticae, 2009
[12] AD Ker "Steganalysis of LSB matching in greyscale images",IEEE signal processing letters, 2005
[13] A Rashid , "Experimental analysis and comparison of LSB substitution and LSB matching method of information security" , International Journal of Computer Science Issues ,2015
[14] Ross J. Anderson, Fabien A.P. Petitcolas, "On the limits of steganography"
[15] Lisa M. Marvel, Charles G. Boncelet, and Charles T. Retter, "Reliable Blind Information Hiding for Images", 2nd Information Hiding Workshop, 1998
[16] Jiri Fridrich, 2 Lt Arnold C. Baldoza and Richard J. Simard, "Robust Digital Watermarking based on Key-dependent Basis Functions", 2nd Information Hiding Workshop, 1998
[17] Fabien A. P. Petitcolas, Ross J. Anderson, and Markus J. Kuhn, "Attacks on copyright marking systems", 2nd Information Hiding Workshop, 1998
[18] Jack Lacy, Schuyler R. Quackenbush, Amy Reibman, James H. Snyder, "Intellectual property protection systems and Digital Watermarking" , 2nd Information Hiding Workshop, 1998
[19] Megalingam, R.K., Nair, M.M., Srikumar, R., Balasubramanian, V.K., Sarma, V.S.V., "PerformanceComparison of Novel, Robust Spatial Domain Digital Image" , Published in: Signal Acquisition and Processing, 2010. ICSAP '10. 9-10 Feb. 2010
[20] A. Ker, "Improved detection of LSB steganography in gray scale images," in Proc. Inf. Hiding Workshop, Springer LNCS, vol. 3200, 2004, pp. 97–115.
[21] Quinhue Huang, Weimin Ouyang "Protect Fragile Regions in Steganography LSB Embedding", 3rd International Symposium on Knowledge Acquisition and Modelling, 2010. pp.175-178.
[22] Ling Xi, Xijian Ping, Tao Zhang. Improved LSB Matching Steganography Resisting Histogram Attacks, IEEE 2010, pp.203
[23] Crandall, R.: Some Notes on Steganography, posted on Steganography Mailing List, http://os.inf.tu-dresden.de/ westfeld/crandall.pdf, 1998.
[24] A. Westfeld, "Detecting low embedding rates," in Proc. Inf. Hiding Workshop, Springer LNCS, vol. 2578, 2002, pp. 324–339.
[25] Zhang, W., Wang, S.,Zhang, X. "Improving Embedding Efficiency of Covering Codes for Applications in Steganography", IEEE Communications Letters, 11(8), 2007, 680-682.
[26] Zhang, X., Wang, S. "Efficient Steganographic Embedding by Exploiting Modification Direction", IEEE Communications Letters, 10(11), 2006, 781-783.
[27] V. Sabeti, S. Samavi, and S. Shirani, "An adaptive LSB matchingsteganography based on octonary complexity measure", Multimedia tools and applications, vol. 64, no. 3, pp. 777–793, 2013.

[28] Hazem Hiary , Khair Eddin Sabri, Mohammed S. Mohammed , Ahlam Al-Dhamari "A Hybrid Steganography System based on LSB Matching and Replacement" International Journal of Advanced Computer Science and Applications, Vol. 7, No. 9, 2016

[29] Y. Tsai, Y. Huang, R. Lin, and C. Chan, "An Adjustable Interpolation-based Data Hiding Algorithm Based on LSB Substitution and Histogram Shifting", International Journal of Digital Crime and Forensics, vol. 8,no. 2, pp. 48–61, 2016.

[30] N. Akhtar, "An LSB Substitution with Bit Inversion Steganography Method", Smart Innovation, Systems and Technologies, Springer India, vol. 43, pp 515–521, 2015.

[31] S. Lyu and H. Farid, "Steganalysis using color wavelet statistics and one class vector support machines," in Proc. SPIE Security, Steganography, Watermarking Multimedia Contents, vol. 5306, E. J. Delp III and P. W. Wong, Eds., 2004, pp. 35–45.

[32] Xiaomei Quan and Hongbin Zhang "Lossless data hiding scheme based on LSB matching" ISBN: 978-0-9891305-0-9 ©2013 SDIWC 209

[33] Andrew D. Ker "Steganalysis of LSB Matching in Grayscale Images " IEEE signal processing letters, vol. 12, no. 6, june 2005

[34] Xiaomei Quan and Hongbin Zhang "Lossless data hiding scheme based on LSB matching" ISBN: 978-0-9891305-0-9 ©2013 SDIWC 209

[35] Jarno Mielikainen "LSB Matching Revisited" IEEE signal processing letters, vol. 13, no. 5, may 2006

[36] Chang, C. C., Hsiao, J. Y., and Chan, C. S. ," Finding optimal least significant-bit substitution in image hiding by dynamic programming strategy", Pattern Recognition, 36, 1583–1595, 2003.

[37] Xu, H., Wanga, J., and Kim, H. J., "Near-optimal solution to pairwise LSB matching via an immune programming strategy", Information Sciences, 180, 1201–1217, 2010.

[38] Roy, B., Rakshit, G., Singha, P., Majumder, A., & Datta, D. An improved Symmetric key cryptography with DNA based strong cipher. International Conference on Devices and communications,India,1–5. doi:10.1109/ ICDECOM.2011.5738553, 2011.