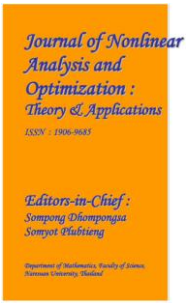
Journal of **N**onlinear **A**nalysis and **O**ptimization
Vol. 13, Issue. 2 : 2022
ISSN : **1906-9685**



EFFECTIVE PSNR VALUES AND GOOD QUALITY OF WATERMARKED IMAGE WITH A PAYLOAD BASED ON CRYPTOGRAPHY AND BIT PAIRS MATCHING

Venkata Pradeep Kumar Jonna, Assistant Professor, Department of Information Technology, Rishi MS Institute of Engineering and Technology for Women, Kukatpally, Hyderabad
Sireesha Chakravaram, Assistant Professor, Department of Information Technology, Rishi MS Institute of Engineering and Technology for Women, Kukatpally, Hyderabad
Ravi Kumar Pilli, Assistant Professor, Department of Information Technology, Rishi MS Institute of Engineering and Technology for Women, Kukatpally, Hyderabad
Maggidi Nikhitha UG Student, Department of Information Technology, Rishi MS Institute of Engineering and Techn**o**logy for Women, Kukatpally, Hyderabad

ABSTRACT
One of the most important methods for concealing digital information is watermarking, which may be used with encryption to increase the security of digital data. LSB substitution is frequently used on the cover image in image watermarking mechanisms to conceal the hidden watermark. In this work, a unique method based on symmetric key cryptography and bit pair matching is put forward. Pairs of pixels are used to organize the original image's pixels and the watermark's encrypted pixels. Following the suggested technique, the pixel bits are represented in pairs. Then, the encrypted watermark pixel bit pairs are compared to all of the bit pairs in the original picture, and as a result, the bit pairs are replaced with the corresponding matched pair's assigned number binary equivalent. If no match is foundthen go for replacing the 0th pair with watermark bits and replace the two LSB with the value of pair number 0. The proposed mechanism shows good quality of watermarked image along with good PSNR values with a good payload. By com- paring the results with some existing algorithms, the proposed scheme shows the valuable results.

Keywords:
PSNR, LSB, BIT pairs, pixel bits.

INTRODUCTION
A number of digital watermarking techniques have been developed for copyright protection of multimedia information, and these approaches are used to prevent the multimedia content from being misused. Any multimedia content, including images, sounds, and videos, can have a watermark for the copyright shield using one of two different ways. The frequency domain approach involves embedding the watermark in either of the transform domains, while the spatial domain method just adds the watermark directly to the data. While frequency domain watermarking is resilient, it nevertheless uses more resources in terms of power and slower processing speed than the spatial domain watermarking, which is quicker but less reliable. (Acken, 1998; Low etal., 1998; Macq and Pitas, 1998; Swanson et al., 1998).
It is better to go for the higher cost of computing to get the benefits of robustness of the watermark when maliciously attacked by the mechanisms of noise, filtering or compression. For the realizationof the watermarking mechanisms, the major areasof focus are imperceptibility, robustness, capacity, security, and trustworthiness. The perceptual transparency of the hidden data or information is the imperceptibility. Survival ofthe watermark information against intentional or unintentional attacks

http://doi.org/10.36893/JNAO.2022.V13I2.1859-1865

without significantdegradation of the quality of the original image is the robustness. The payload for the new signal is defined as the capacity and the undetectability of the watermark information on the corresponding media, which is defined as the security and all these turned to be very important considerations in case of invisible watermarking (Liu and Tan, 2002; Zhu et al., 2006; Gutab and Ghouti, 2007). A well-known survey of watermarking techniques can be found from (Kutter and Hartung, 1999; Mohanty, 1999; Altaibi et al., 2015). There is a trade-off between these parameters as an increase in robustness may appear at the expense of enhanced watermark signals visibility as well as reduced bandwidth. But, the perceptual distortion of the image, due towatermark embedding is not related directly to the magnitude of the watermark signal. It can be observed that the watermark signal of same strength is causing less visual distortion in busy areas of the image than the flat background. In the papers (Podilchuk and Wenjua, 1998; Hannigan et al., 2001) on watermarking, there is less effort to evaluate images in order to consider the upper limit of the power of the watermark signal without considerable visual distortion.These spatial domain methods neglect the significance of payload capacity and mostly focused on the imperceptibility factors. In Khan and Gutub (2007) the authors proposed an image based message concealment mechanism by use ofpunctuation marks to encode a secret messageand by using modified scytale cipher provides thebetter result as far as the security is concerned. In Al-Otaibi (2014) the author proposed a data hiding technique with two layers of the security system by including AES cryptography followed by image-based steganography to ensure high security. Methods of LSB matching is proposedin Sharp (2001), which also called ± embedding mechanism (Li et al., 2011). In this method, the cover image pixel value is increased or decreased randomly by one when the secret bit is not equal to the LSB of the pixel belonging to the cover image (Huang et al., 2014). The LSBM modifies both the histogram of an image and the correlation between the adjacent pixels, which helps the steganalysis methods to attack this method (Xia et al., 2016). In Sabeti et al. (2013) the authors proposed complexity based LSB matching scheme, where the LSB matching isused in order to enhance the security against possible attacks. This mechanism uses a local neighborhood analysis to determine the secure locations of an image and then LSB matchingused for the embedding process. In Parvez and Gutub (2011) the authors proposed one imagesteganography algorithm, which determines thenumber of secret message bits that each pixel of the cover image can store based on a partition scheme of color intensity range. This scheme provides high data hiding capacity and security for the host image.

EXICITING SYSTEM

In this segment, we offer a brief review related to LSB matching and other mechanisms of LSB. The work in Wu and Tsai (2003) proposed pixel value differencingmechanism in which a pixel value differencing is used to differentiate between edge areas in comparison to smooth areas.Consequently, the payload of the embedded data is higher in edge areas than that of areas of smooth. Recently the authors proposed certain mechanisms combining PVD and LSBreplacement for better embedding efficiency (Chang and Tseng, 2004). A number of methods were proposed by combining PVD and LSB replacement mechanisms (Mahjabin et al., 2012; Khodaei and Faez, 2012; Mandal and Das, 2012). In Gutub et al. (2009) the authors proposed a good algorithm on steganography by merging the idea of randompixel manipulation methods and the stego keyones. This mechanism shows good outcomes of hiding capacity with relation to the RGB image pixels. In the paper (Sumathi et al.,2014) a mechanism developed called LSB-MR(Least Significant Bit Matching Revisited). In this method, the embedding process is carried on a cover pixel pair at a time to embed the secret bit pair. The corresponding stego pixel pair can be formed by keeping that cover pixel pair unaltered or by increasing or decreasing the value by one. A function is used here to evaluate the need for alteration to cover pixel values. Practically this mechanism reflected poor embedding rate. To generalize this mechanism a LSB-M(Matching) method was proposed in Li et al. (2009). To enhance the security of both LSB-M and GLSBM, a content adaptive mechanism proposed by the authors (Wang et al., 2010). In Sabeti et al. (2013) the authors proposed a LSB-M adaptive algorithm called complexity basedLSB-M in which a complexity region is determined for embedding of data by using an8-neighborhood of a pixel. The disadvantage of this mechanism was low embedding capacity. In the paper (Tsai et al., 2016) the mechanism based on interpolation, LSB substitution, and histogram

shifting. The interpolation process is used to adjust embedding capacity for low distortion of the image, the embedding is then applied using LSB substitution and shifting of histogrammechanism.
In Akhtar (2015) the authors suggestedan improved LSB substitution mechanism. In this process, secret data is hidden aftercompressing the smooth areas of the image losslessly resulting in lesser number of modified cover image pixels. Then a bit inversion mechanism is applied where certainLSBs of pixels are modified if they occur in aspecific format. In Jung and Yoo (2015) the authors suggested a mechanism of semireversible data hiding based on interpolation and LSB substitution. Initially, interpolationis used to scale up and down the cover image before hiding the secret watermark to achieve high embedding capacity with very lowdistortion of the image quality. In Al-Otaibi and Gutub (2014) the authors proposed animage based steganography replacing the pixel, least significant bit with hidden text. The scheme experimentally explores the data dependency and its security issues with attractive results. In Abu-marie et al. (2010) the authors proposed a LSB replacement based technique using truth table based and determinate array on RGB indicator that uses pixel manipulation, shows amazing results in data hiding capacity. In Gutub et al. (2009)the authors suggested an image based steganography technique called triple-A, using LSB bits of image pixels with morerandomization in the selection of a number of bits and using color channels. This mechanism adds more security to data hiding process. In Yang et al. (2008) the authors proposed the edge based LSB mechanism with high embedding capacity, but the security issue was very poor. In the paper(Hempstalk, 2006) the authors suggested amechanism to hide the information bits in the less focused areas such as corners of the original cover image. But, the disadvantage ofthis mechanism is that the payload capacity isvery low. In Luo et al. (2010) the author proposed a mechanism which uses a pseudo- random number generator with LSB matchingto select the location for data hiding into the original cover image. This mechanism exploits sharper regions into the host image tohide more data bits as compared to smoother areas. In the paper (Wang et al., 2008) the authors used the PVD and LSB mechanisms to hide fewer data bits in the cover images. This mechanism uses the difference in thepixels and a modulus function to secure data bits by changing the remainder or value of modulus.
In this paper, we proposed a cryptography-based bit pairs matchingwatermarking mechanism in the spatial domain and used the symmetric key cryptography (Menezes et al., 1996; Roy et al., 2011) to encrypt the watermark to protect the information from the intruder during transmission. The objective of the proposed mechanism is to improve the robustness of enhanced payload and security while maintaining the imperceptibility.

Watermark embedding and extraction:
In this segment, the process of watermarking is explained. The aim of this work is to increase the watermark strength by embedding the watermark following a newmechanism of cryptography and bit pairs matching.

Symmetric key cryptography:
The security of the projected mechanism is enhanced by adding encryption. The watermark is encrypted by using symmetric key cryptography, which protects the contents of multimedia information from attackers. This encryption mechanism uses a single key to encrypt the grayscale watermarklogo in encoding section as well as decryptthe watermark logo in decoding section. During the encryption process, the algorithm 1 is used here to convert each pixel of the watermark logo into binary, reverse it andstore the quotient and remainder by dividing the reversed string by a key. The process of decryption used the algorithm 2, in which the same key is used to receive the original imagepixels (Roy et al., 2011).

http://doi.org/10.36893/JNAO.2022.V13I2.1859-1865

Algorithm 1: Watermark Encryption

Input: Grayscale image
1: Consider the grayscale image W.
2: Generate the decimal value for each pixel (P_i) of W.
3: Find out the corresponding binary value (B_v) of each P_i.
4: Reverse that 8 digit's binary number B_v to get R_v.
5: Consider a 4 digit divisor as the Key (K_e).
6: Now divide the reversed number R_v with the divisor K_e.
7: Next store the remainder and quotient in an 8-bit string. If required, add the number of 0s on the left-hand side of remainder and quotient bits to complete the 8-bit string. This leads to being the encrypted data (ED).
Output: Encrypted image

Algorithm 2: Watermark Decryption

Input: Encrypted image data (ED) and the key (K_e)
1: Multiply the quotient bits of the encrypted data (ED) by the Key (K_e) to produce F.
2: Add the remainder bits of the encrypted data (ED) with the result produced in the above step (F) to get G.
3: If the result produced (G) in the previous step i.e. step 2 is not an 8-bit number, then we require, making it an 8-bit number.
4: Reverse the number G to get the decrypted data (DD).
Output: Decrypted image

PROPOSED SYSTEM

This segment reflects the proposed method bymeans of imperceptibility and capacity of data hiding. To judge the performance of the system certain outcomes are assessed with some state of the art mechanisms.

To authenticate the performance of the method, a number of standard grayscaleimages of size 512 512 and one grayscale watermark of size 32 32 are used. The grayscale watermark image is given in Fig. 4 and the test grayscale images are given in Fig.

6. To proof, the accuracy of the scheme fifteen sample images is taken for illustration.Below we have given the images with results.

The watermark after applying encryption given in Fig. 5 and Fig. 7 shows thewatermarked Images.

The encrypted watermark is embeddedmultiple times within the original grayscale image as per the bit pairs matching using the adaptive bits pair replacement. As the resultof embedding, the original image suffers aloss in quality which is calculated by meansof some well-known and good quality metricsto check the invisibility of the embedded watermarks for imperceptibility.

Results of imperceptibility:

Fig 8 shows the bar chart where the original image and watermarked image compared to give the result of imperceptibility.

From the above Fig. (i) Mean Squared Error result, all the value lies in between 0.0031 to 0.0034. This confirms less probability of loss of quality.

From Fig. (ii) shows the PSNR value for original image verses watermarked image ranged from 51.2948 dB to 52.9925 dB. This indicates achievement of a higher degree of imperceptibility.

Fig. (iii) indicates the maximum value forUIQI is one. In the projected method all the values are close to 1(.98 to .99), which indicates the least difference between watermarked image and original image or indicates superior quality.

From Figs. (iv) and (v), the structural similarity between the watermarked image and original image are very close and maximum value for both SSIM and MSSIMis approximately 1. In the present mechanism both the values are approaching one for fifteen different images.

Results of robustness:

To show the Robustness of the projected mechanism different attacks like Rotation, Scaling, Crop, Noise Addition, and JPEG Compression is tested. The bar chart in Figs. 9i–iv shows the outcomes against differentkind of impairments, which signifies the revival of the embedded bits and their quality. Here the metrics like Weighted Peak Signalto Noise Ratio (WPSNR), Normalized Cross Correlation (NCC), Similarity measurement(SM), Bit Error Rate (BER) used to show the quality of recovered bits to prove the robustness of the mechanism.

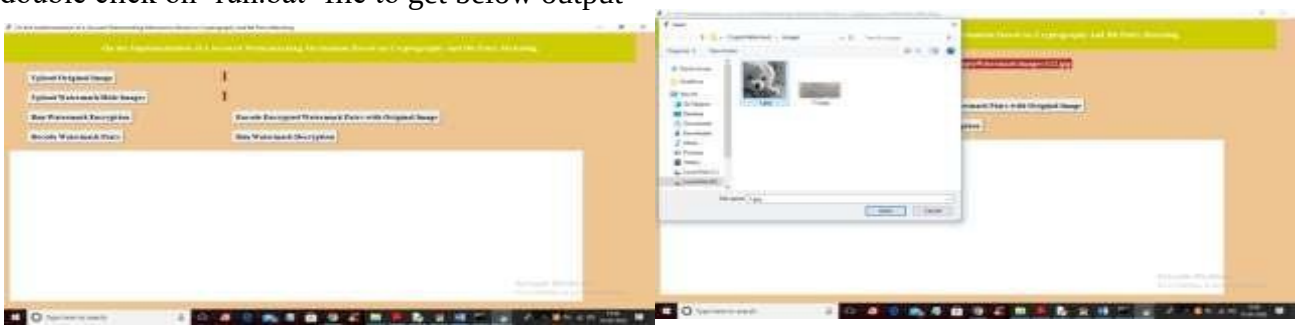
http://doi.org/10.36893/JNAO.2022.V13I2.1859-1865

METHODOLOGY

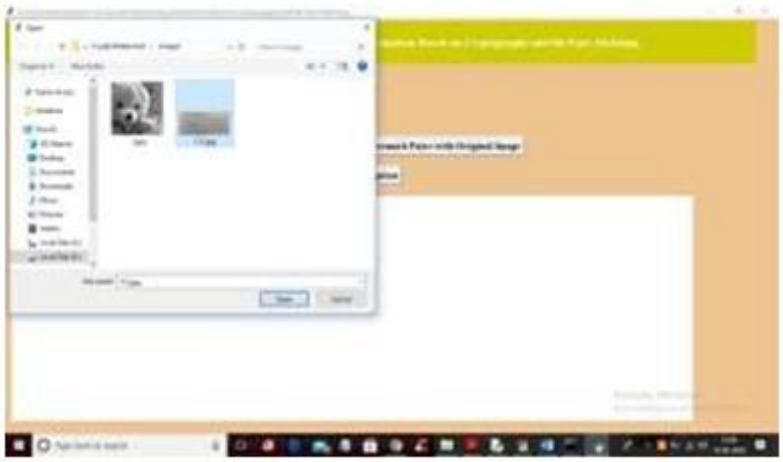
To implement this project we have designed following modules

1. 1 Upload Original Image: using thismodule we will upload original cover image
2. Upload Watermark/Hide Images: using this module we will upload watermark or hiding image
3. Run Watermark Encryption: using this module we will encrypt watermark/hidden image with symmetric key
4. Encode Encrypted Watermark Pairs with Original Image: using this module we willextract pairs from both original and watermark image and then embed bothpixels at same location in original image
5. Decode Watermark Pairs: using this module we will take out hidden encryptedwatermark image from the original image

Run Watermark Decryption: using this modulewe will decrypt extracted hidden image and then calculate PSNR, SSIM and MSE between extracted image and original hidden image To run project double click on 'run.bat' file to get below output



In above screen click on 'Upload Original Image'button to upload any image as original like below screen



In above screen selecting and uploading 112.jpg file as original image and then click on 'Open' button to get below output

In above screen original image is loaded and nowclick on 'Upload Watermark/Hide Image' button to upload watermark image

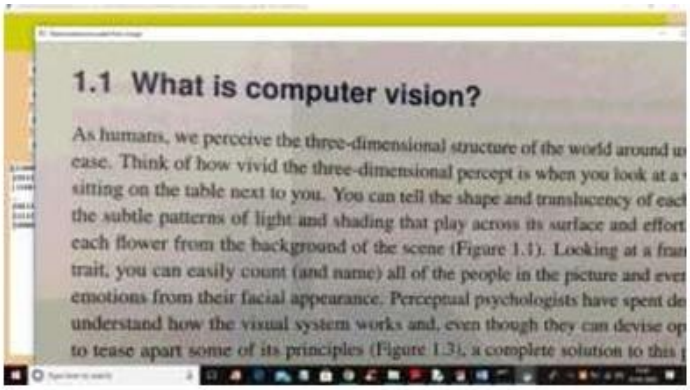
http://doi.org/10.36893/JNAO.2022.V13I2.1859-1865

In above screen selecting and uploading '1.jpg' aswatermark image and then click on 'Open' buttonto load image and get below screen

In above screen both original and watermark images loaded and now click on 'Run Watermark Encryption' button to encrypt watermark image and get below output

In above screen we can see original image and encrypted image from watermark image and now close above images to get below output

In above screen we can see binary values extracted from watermark images and then click on 'Encode Encrypted Watermark Pairs with Original Image' button to hide encrypted watermark image in original image



In above original image watermark image is hidden and now to extract hidden image backthen click on 'Decode Watermark Pairs' button toget below output

http://doi.org/10.36893/JNAO.2022.V13I2.1859-1865

In above screen encrypted watermarked imageextracted from original image and now click on 'Run Watermark Decryption' button to decrypt watermark image and get below output

In above screen we successfully decrypted watermark image and similarly we can uploadand see output for any other images. In above screen we can see PSNR, MSE and SSIM values. The lower then MSE and PSNR the better is the image and higher the SSIM the high quality is theimage.

CONCLUSION

In this paper bit pairs similarity based LSB replacement watermarking mechanism is proposed. This mechanism is a new concept and which is different from all the previous mechanisms because its main focus is on bit pairssimilarity. In this technique to make the watermark more secured, symmetric key cryptography is used and the data bits are arranged in pairs following the proposed scheme, which is different from all the existingtechniques. The proposed technique is applied to 15 different grayscale test images. The proposed scheme is more secure, robust and higher payloadbased on good factors of imperceptibility proved from the results of the experiments we have done.

REFERENCES

1. Al-Otaibi, N.A., Gutub, A.A.A., 2014. Flexible stego-system for hiding text in images of personal computers based on user security priority. In: Proceedings of 2014 International Conference on Advanced Engineering Technologies (AET-2014), Dubai UAE, pp. 250–256.
2. Altaibi, N.A., Gutub, A.A., Khan, E.A., 2015. Stego-system for hiding text in images of personal computers. In: The 12th Learning and Technology Conference: Wearable Tech/Wearable Learning, Effat University, Jeddah, Kingdom of Saudi Arabia.
3. Gutab, A.A.A., Ghouti, L., 2007. Utilizing extension character 'Kashida' with pointed lettersfor arabic text digital watermarking. In: International Conference on Security and Cryptography (SECRYPT), Barcelona, Spain.
4. Gutub, A., Al-Qahtani, A., Tabakh, A., 2009. Triple-A: secure RGB image steganography based on randomization. In: The 7th ACS/IEEE International Conference on Computer Systems and Applications (AICCSA-2009), Rabat, Morocco, pp. 400–403
5. Hannigan, B.T., Reed, A., Bradley, B., 2001. Digital watermarking using improved humanvisual system model. In: Ping Wah Wong,Edward J. Delp (Eds.), Proc. SPIE. 4314, 468- 474, Security and Watermarking of Multimedia Contents III.
6. Hempstalk, K., 2006. Hiding behind corners: using edges in images for better steganography. In: Proceedings of the Computing Women's Congress, Hamilton, New Zealand, pp. 11–19
7. Khan, F., Gutub, A.A.A., 2007. Message concealment techniques using image based steganography. In: The 4th IEEE GCC Conference and Exhibition, Gulf International Convention Centre, Manamah, Bahrain.
8. Kutter, M., Hartung, F., 1999. Image watermarking techniques. In: Proceedings of the IEEE, Special Issue on Identification and Protection of Multimedia Information.
9. Mahjabin, T., Hossain, S., Haque, M., 2012. A block based data hiding method in images using pixel value differencing and LSB substitution method. In: Proc. International Conference on Computer and Information Technology (ICCIT). Chittagong. Bangladesh, pp. 168–172.
10. roy, B., Rakshit, G., Singha, P., Majumder, A.,Datta, D., 2011. An improved symmetric key cryptography with DNA based strong cipher. Int. Conf. Devices Commun. India 1–5. https://doi.org/10.1109/ICDECOM.2011.5738553