ISSN: 2321-2152

IJMECE

International Journal of modern electronics and communication engineering

E-Mail
editor.ijmece@gmail.com
editor@ijmece.com

www.ijmece.com

ISSN2321-2152www.ijmece .com
Vol 10, Issue.2 April 2022

IMPLEMENTATION OF SECURED WATERMARKING MECHANISM BASED ON CRYPTOGRAPHY AND BIT PAIRS MATCHING.

JYOTHIRMAI BOLISHETTY[1] , MANASA MALIGIREDDY[2] , KAVYASRI SHETTY[3], DIVYA MANDALAPU[4], Dr.M.MURUGESAN
UG students[1,2,3,4] , Professor[5]

ABSTRACT: *Watermarking is one of the most vital digital information hiding technique, which can be used with cryptography mechanism for providing more security to digital data. In image watermarking mechanism mostly LSB substitution is used on the cover image for hiding the secret watermark. In this paper, a novel technique based on the matching of bit pairs and symmetric key cryptography is proposed. Pixel bits of original image and encrypted watermark image are arranged in pairs. The pixel bits are represented in pairs following the proposed algorithm, then the encrypted watermark pixel bit pairs are compared with all bit pairs of original image and accordingly the replacement of bit pairs takes place with the respective matched pair assigned number binary equivalent. If no match is found then 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 comparing the results with some existing algorithms, the proposed scheme shows the valuable results.*

I. INTRODUCTION

For copyright protection of multimedia information, a variety of digital watermarking techniques have been developed, which are used to protect the multimedia information from being abused. There are two categories of techniques of embedding the watermark for copyright shield in any multimedia information, be it the image, audio or video.

The spatial domain technique follows any particular algorithm for embedding of the watermark by directly adding it to the data, and the frequency domain method is to embed it in any of the transform domain. The spatial domain of watermarking is faster but fails in robustness while the frequency domain watermarking is robust but still consumes more resources in terms of power consumption and slower speed of computing (Acken, 1998, Low et al., 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 realization of the watermarking mechanisms, the major areas of focus are imperceptibility, robustness, capacity, security, and trustworthiness. The perceptual transparency of the hidden data or information is the imperceptibility. Survival of the watermark information against intentional or unintentional attacks without significant degradation 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 to watermark 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 2 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 of punctuation marks to encode a secret message and by using modified scytale cipher provides the better 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 proposed in 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 LSB-M 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 is used 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 matching used for the embedding process. In Parvez and Gutub (2011) the authors proposed one image steganography algorithm, which determines the number 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.

II. LITERATURE SURVEY

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 differencing mechanism 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 LSB replacement 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 random pixel manipulation methods and the stego key ones. 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 based LSB-M in which a complexity region is determined for embedding of data by using an 8-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 histogram mechanism. In Akhtar (2015) the authors suggested an improved LSB substitution mechanism. In this process, secret data is hidden after compressing the smooth areas of the image losslessly resulting in lesser number of modified cover image pixels. Then a bit inversion mechanism is applied where certain LSBs of pixels are modified if they occur in a specific format. 4 In Jung and Yoo (2015) the authors suggested a mechanism of semi reversible data hiding based on interpolation and LSB substitution. Initially, interpolation is used to scale up and down the cover image before hiding the secret watermark to achieve high embedding capacity with very low distortion of the image quality. In Al-Otaibi and Gutub (2014) the authors proposed an image 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 more randomization 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 a mechanism to hide the information bits in the less focused areas such as corners of the original cover image. But, the disadvantage of this mechanism is that the payload capacity is very low. In Luo et al. (2010) the author proposed a mechanism which uses a pseudo-random number generator with LSB matching to select the location for data hiding into the original cover image. This mechanism exploits sharper regions into the host image to hide 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 the pixels 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 matching watermarking 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.

III. PROPOSED SYSTEM

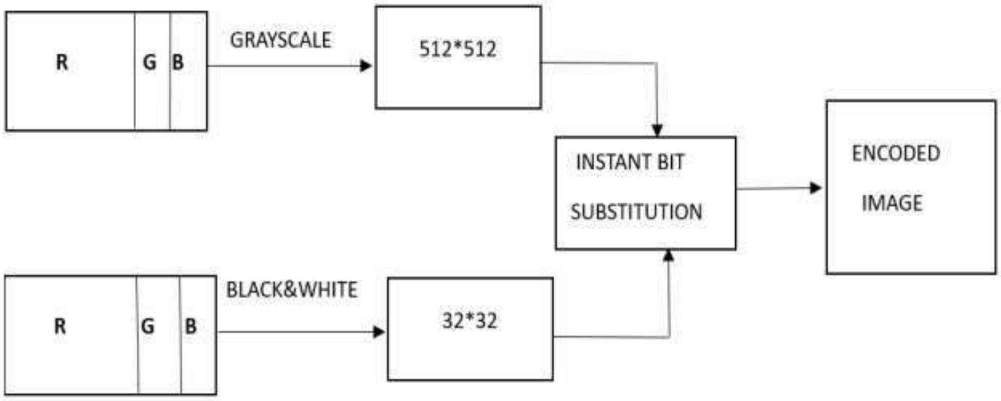
In this segment, we offer a brief review related to LSB matching and other mechanisms of LSB. The work in Wu and Tsai (2003) proposed pixel value differencing mechanism in which a pixel value differencing is used to differentiate between edge areas in comparison to smooth areas.

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 differencing mechanism in which a pixel value differencing is used to differentiate between edge areas in comparison to smooth areas.

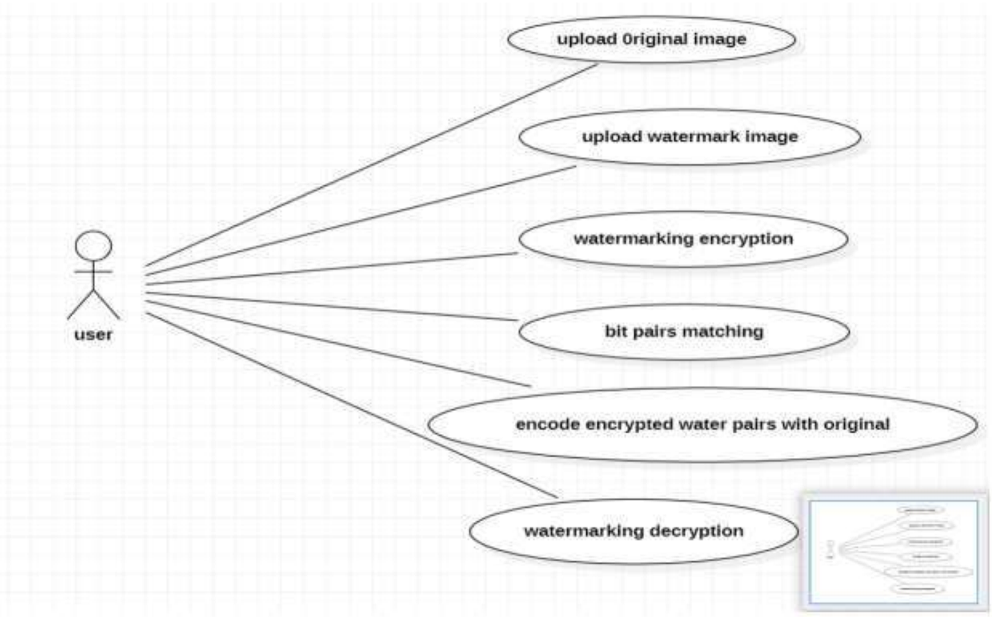
Advantages of proposed system :

- High accuracy
- High efficiency

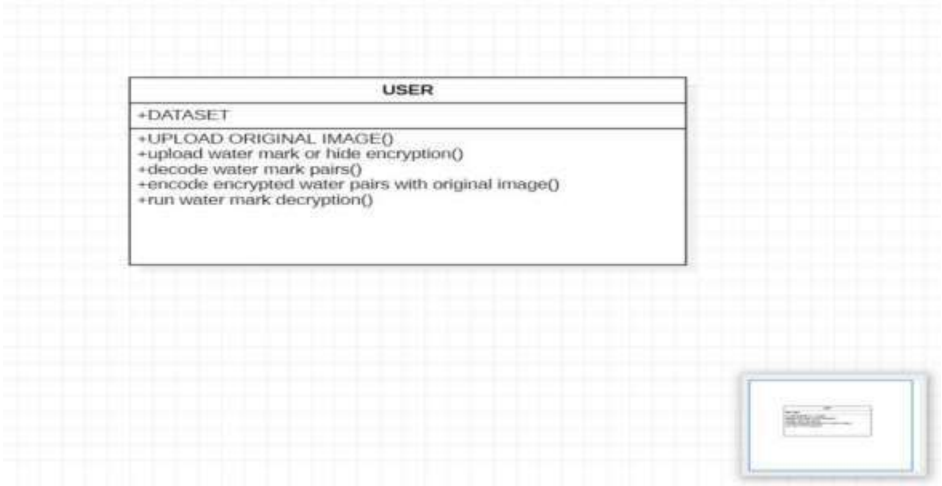
An architectural diagram is a visual representation that maps out the physical implementation for components of a software system. It shows the general structure of the software system and the associations, limitations, and boundaries between each element. A system architecture is the conceptual model that defines the structure, behavior, and more views of a system. An architecture description is a formal description and representation of a system, organized in a way that supports reasoning about the structures and behaviors of the system.



A use case diagram in the Unified Modeling Language (UML) is a type of behavioral diagram defined by and created from a Use-case analysis. Its purpose is to present a graphical overview of the functionality provided by a system in terms of actors, their goals (represented as use cases), and any dependencies between those use cases. The main purpose of a use case diagram is to show what system functions are performed for which actor. Roles of the actors in the system can be depicted.

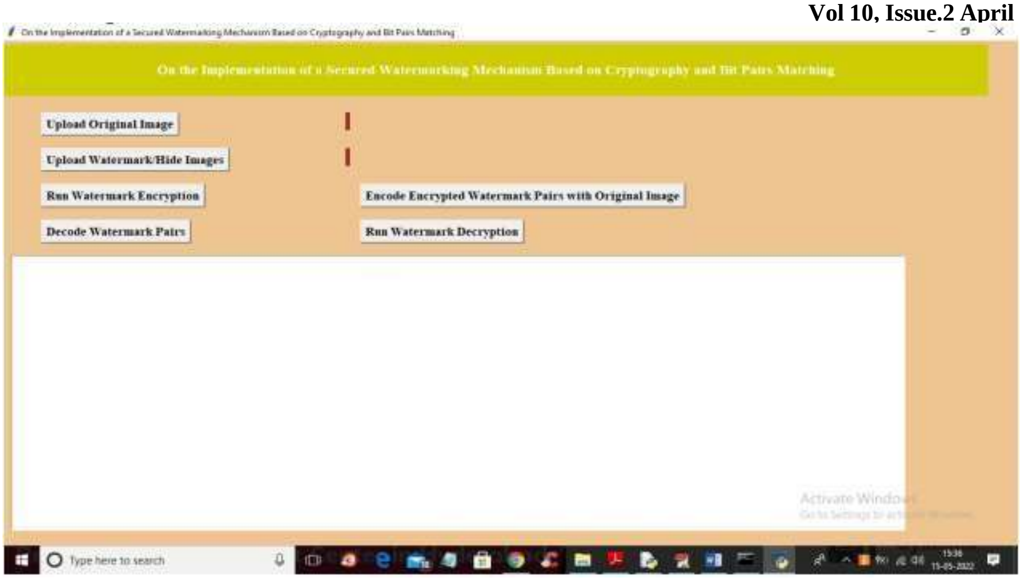


In software engineering, a class diagram in the Unified Modeling Language (UML) is a type of static structure diagram that describes the structure of a system by showing the system's classes, their attributes, operations (or methods), and the relationships among the classes. It explains which class contains information.

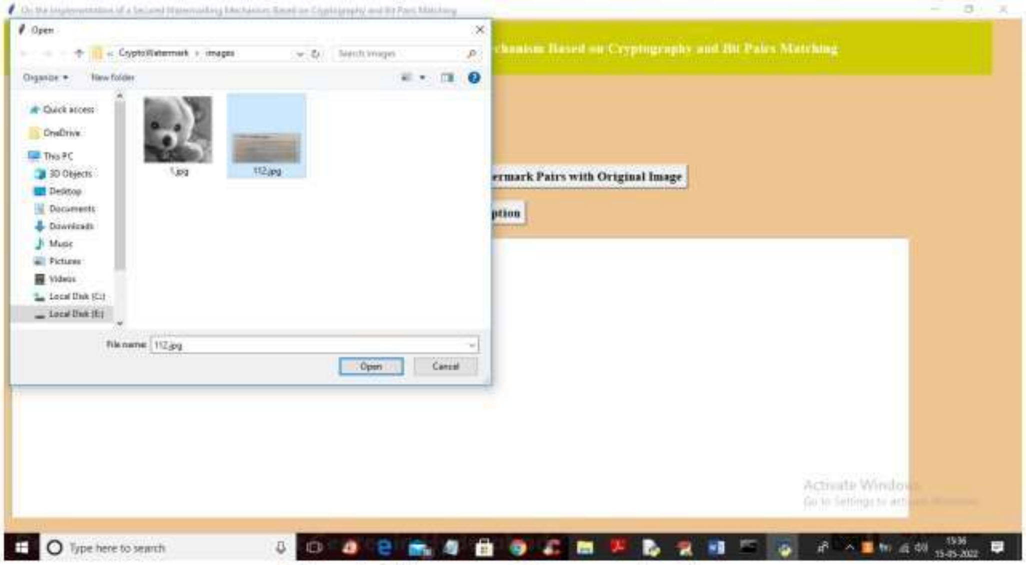

USER
+DATASET
+UPLOAD ORIGINAL IMAGE()
+upload water mark or hide encryption()
+decode water mark pairs()
+encode encrypted water pairs with original image()
+run water mark decryption()

IV. RESULTS

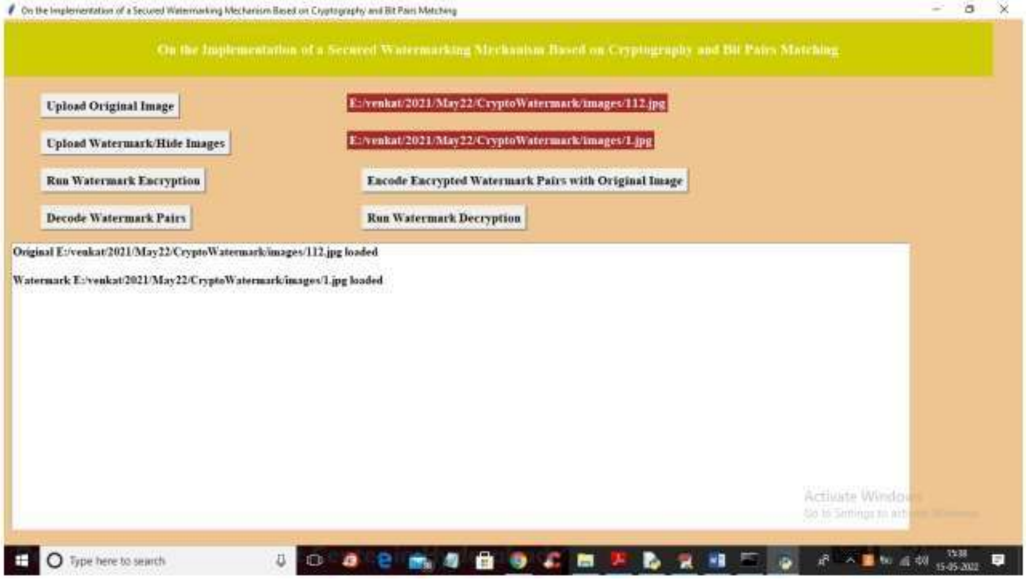
OUTPUT SCREENS


On the Implementation of a Secured Watermarking Mechanism Based on Cryptography and Bit Pairs Matching
On the Implementation of a Secured Watermarking Mechanism Based on Cryptography and Bit Pairs Matching
Upload Original Image
Upload Watermark/Hide Images
Run Watermark Encryption
Encode Encrypted Watermark Pairs with Original Image
Decode Watermark Pairs
Run Watermark Decryption
Type here to search

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



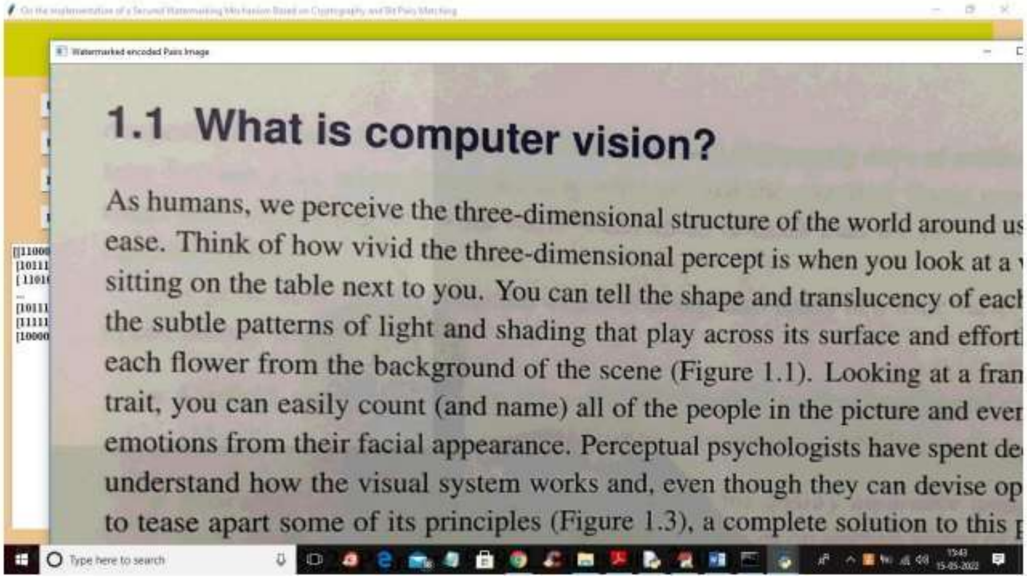
In above screen selecting and uploading '1.jpg' as watermark image and then click on 'Open' button to load image and get below screen


On the Implementation of a Secured Watermarking Mechanism Based on Cryptography and Bit Pairs Matching
On the Implementation of a Secured Watermarking Mechanism Based on Cryptography and Bit Pairs Matching
Upload Original Image
E:/venkat/2021/May22/CryptoWatermark/images/112.jpg
Upload Watermark/Hide Images
E:/venkat/2021/May22/CryptoWatermark/images/1.jpg
Run Watermark Encryption
Encode Encrypted Watermark Pairs with Original Image
Decode Watermark Pairs
Run Watermark Decryption
Type here to search

```
Original E:/venkat/2021/May22/CryptoWatermark/images/112.jpg loaded

Watermark E:/venkat/2021/May22/CryptoWatermark/images/1.jpg loaded
```

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

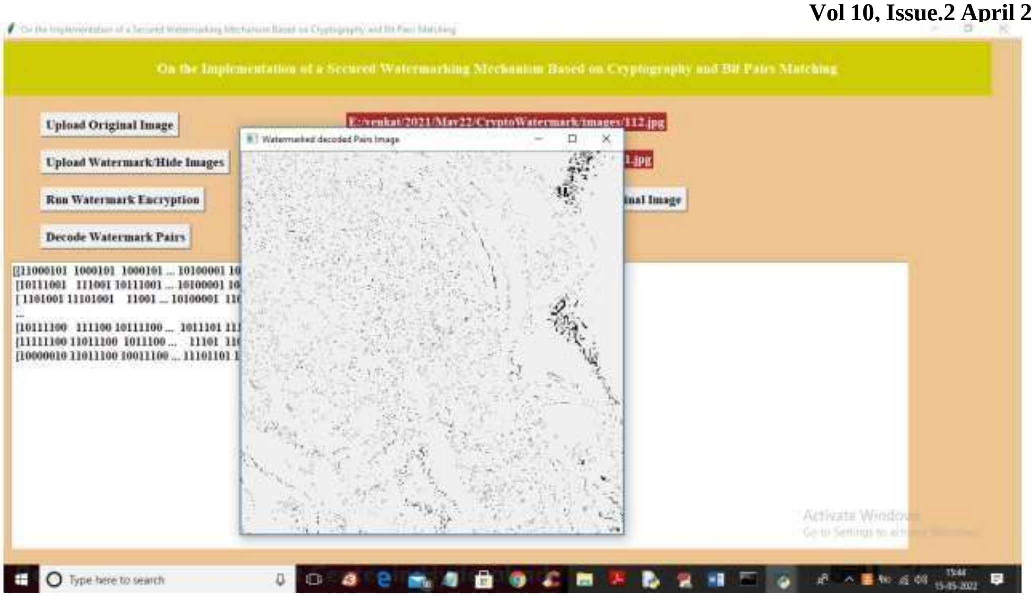

On the Implementation of a Secured Watermarking Mechanism Based on Cryptography and Bit Pairs Matching
Watermarked encoded Pairs Image
Type here to search

```
[[11000
 [10111
 [11010
 ...
 [10111
 [11111
 [10000
```

1.1 What is computer vision?

As humans, we perceive the three-dimensional structure of the world around us
ease. Think of how vivid the three-dimensional percept is when you look at a
sitting on the table next to you. You can tell the shape and translucency of each
the subtle patterns of light and shading that play across its surface and effort
each flower from the background of the scene (Figure 1.1). Looking at a fran
trait, you can easily count (and name) all of the people in the picture and ever
emotions from their facial appearance. Perceptual psychologists have spent de
understand how the visual system works and, even though they can devise op
to tease apart some of its principles (Figure 1.3), a complete solution to this

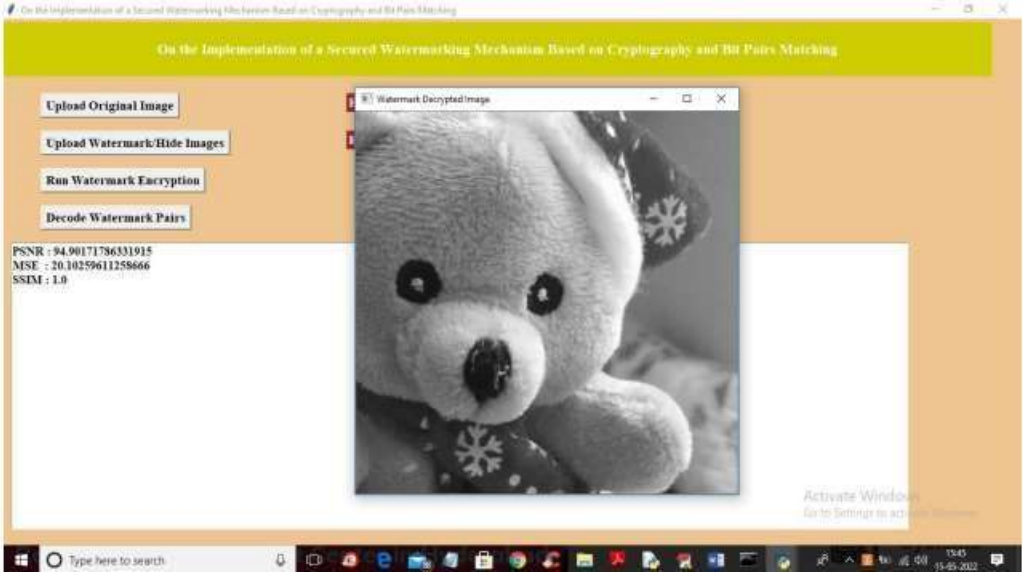
In above original image watermark image is hidden and now to extract hidden image back then click on ‘Decode Watermark Pairs’ button to get below output


On the Implementation of a Secured Watermarking Mechanism Based on Cryptography and Bit Pairs Matching
On the Implementation of a Secured Watermarking Mechanism Based on Cryptography and Bit Pairs Matching
Upload Original Image
Upload Watermark/Hide Images
Run Watermark Encryption
Decode Watermark Pairs
Watermarked decoded Pairs Image
inal Image
Activate Windows
Type here to search

E:/venkat/2021/May22/CryptoWatermark/images/112.jpg

```
[[11000101  1000101  1000101 ... 10100001 10
 [10111001   111001 10111001 ... 10100001 10
 [ 1101001 11101001    11001 ... 10100001  11
 ...
 [10111100   111100 10111100 ...  1011101 11
 [11111100 11011100  1011100 ...    11101  11
 [10000010 11011100 10011100 ... 11101101 1
```

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


On the Implementation of a Secured Watermarking Mechanism Based on Cryptography and Bit Pairs Matching
On the Implementation of a Secured Watermarking Mechanism Based on Cryptography and Bit Pairs Matching
Upload Original Image
Upload Watermark/Hide Images
Run Watermark Encryption
Decode Watermark Pairs
Watermark Decrypted Image
Activate Windows
Type here to search

```
PSNR : 94.90171786331915
MSE  : 20.10259611258666
SSIM : 1.0
```

In above screen we successfully decrypted watermark image and similarly we can upload and 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 the image

V. CONCLUSION

In this paper bit pairs similarity based LSB replacement water- marking 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 pairs similarity. 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 existing techniques. The proposed technique is applied to 15 different grayscale test images. The proposed scheme is more secure, robust and higher payload based on good factors of imperceptibility proved from the results of the experiments.

REFERENCE

[1] T. K. Das, D. P. Acharjya, and M. R. Patra, ‘‘Opinion mining about a product by analyzing public tweets in Twitter,’’ in Proc. Int. Conf. Comput. Commun. Informat., Jan. 2014, pp.1-4.

[2] H. Watanabe, M. Bouazizi, and T. Ohtsuki, ‘‘Hate speech on Twitter: A pragmatic approach to collect hateful and offensive expressions and perform hate speech detection,’’ IEEE Access, vol. 6, pp. 13825–13835, 2018.

[3] O. Oriola and E. Kotze, ‘‘Evaluating machine learning techniques for detecting offensive and hate speech in South African tweets,’’ IEEE Access, vol. 8, pp. 21496–21509, 2020 .

[4] K. Weller, A. Bruns, J. Burgess, M. Mahrt, and C. Puschmann, Twitter and Society, vol. 89, P. Lang, Ed. Cham, Switzerland: Peter Lang Publishing, 2014.

[5] F. Del Vigna12, A. Cimino23, F. Dell’Orletta, M. Petrocchi, and M. Tesconi, ‘‘Hate me, hate me not: Hate speech detection on Facebook,’’ in Proc. 1st Italian Conf. Cybersecur. (ITASEC), 2017, pp. 86–95.

[6] C. Stokel-Walker, ‘‘Alt-right’s ‘Twitter’ is hate-speech hub,’’ New Scientist, vol. 237, no. 3167, p. 15, Mar. 2018.

[7] P. Charitidis, S. Doropoulos, S. Vologiannidis, I. Papastergiou, and S. Karakeva, ‘‘Towards countering hate speech against journalists on social media,’’ Online Social Netw. Media, vol. 17, pp. 1–10, May 2020. [8] T. Davidson, D. Warmsley, M. Macy, and I. Weber, ‘‘Automated hate speech detection and the problem of offensive language,’’ in Proc. 11th Int. AAAI

Conf. Web Social Media, 2017, pp. 512–515. 29

[9] Z. Waseem, ‘‘Are you a racist or am i seeing things? Annotator influence on hate speech detection on Twitter,’’ in Proc. 1st Workshop NLP Comput. Social Sci., 2016, pp. 138–142.

[10] L. Gao and R. Huang, ‘‘Detecting online hate speech using con- text aware models,’’ 2017, arXiv:1710.07395. [Online]. Available:

[11] P. Badjatiya, S. Gupta, M. Gupta, and V. Varma, ‘‘Deep learning for hate speech detection in tweets,’’ in Proc. 26th Int. Conf. World Wide Web Companion - WWW Companion, 2017, pp. 759–760.

[12] B. Gambäck and U. K. Sikdar, ‘‘Using convolutional neural networks to classify hatespeech,’’ in Proc. 1st Workshop Abusive Lang. Online, 2017, pp. 85–90.

[13] Z. Zhang and L. Luo, ‘‘Hate speech detection: A solved problem? The challenging case of long tail on Twitter,’’ Semantic Web, vol. 10, no. 5, pp. 925–945, Sep. 2019