IMPLEMENTATION OF A SECURED WATERMARKING MECHANISM BASED ON CRYPTOGRAPHY AND BIT PAIR MATCHING

[1]A. Anitha Reddy, [2]Mareddy Sahani, [3]Guddanti Meghana, [4]Shaik Aslam Pasha, [5]Tarun Madhav Medi

Assistant Professor in Department of CSE Sreyas Institute Of Engineering And Technology

[2.3.4,5]UG Scholar in Department of CSE Sreyas Institute Of Engineering And Technology

Abstract

Watermarking is one of the most vital digital information hiding technique, which can be usedwith 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 the0th 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 valueswith a good payload. By com- paring the results with some existing algorithms, the proposed scheme shows the valuable results

Keywords: *Cryptography, Key Matching, Bit Pair Matching, Python*

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. watermarkingis a method for concealing data via transporter media, which utilizes an advanced medium. In general, watermarking is applied in noticeable media, for example, pictures and videos; however, in advanced watermarking the sign might be sounds, videos, text, and so forth.

Watermarking and fingerprinting are both advancements that are firmly connected with steganography. Watermarking are for the most part frightened with insurance of scholarly effects. In watermarking the whole item is “stamped.” Articles shroud the data when using watermarking, which commonly indicates establishment or ownership of copyright assurance. Be that as it may, in another way, different marks are inserted in various duplicatesof the transporter media. They are flexibly toward various shoppers in fingerprinting.

II LITERATURE SURVEY

Flexible stego-system for hiding text in images of personal computers based on user security priority:

It is suggested and put into practise to use a flexible security solution to conceal important text data on personal computers (PCs). The system gives the user security information so they may choose the coverimage for their PC based on how important security is to them. The user can test different graphics to conceal the same text because to the technique's adaptability.

The user then choose which image will be used as the cover image after considering the required level of security. The approach employs text-hidden in place of the least significant bit in each pixel, which is standard for image-based steganography. The study tests 30 alternative fixed size pictures withfascinating, appealing outcomes to evaluate data reliance and its security impacts.

Stego-system for hiding text in images of personal computers:

The capacity to involve a portion of the PC's accessible pictures as the cover media while tying down delicate text to be concealed inside pictures has an advantage. It's intriguing to take note of that choosing individual pictures can be thought to be totally private and known exclusively to the PC client. To get delicate text information, this safety effort of stowing away inside PC pictures was utilized as a genuineapplication behind picture-based steganography.

The security of the cover media, i.e., the PC's photographs, is predicated on the way that the information won't be quickly gotten to by means of regular techniques. A secure method to conceal the text on the cover picture was suggested and put into practise. The system for steganography uses standard image-based steganography to conceal data in the least significant bit (LSB).

Utilizing extension character 'Kashida' with pointed letters for arabic text digital watermarking:

This study takes advantage of the superfluous Kashida Arabic extension character. We suggest using Arabic text with pointed letters and a Kashida to hold the secret bit "one" and Arabic text with unpointed letters and a Kashida to hold "zero." The technique falls under the category of secrecy feature coding methods since it uses the inherited points of the letters to conceal secret information bits inside them. Other languages like Persian and Urdu, which have texts that are comparable to Arabic, also find this watermarking approach to be appealing.

Triple-A: secure RGB image steganography based on randomization:

This study proposes the triple-A calculation, an original picture based steganography technique. With more randomization in the determination of the quantity of pieces utilized and the variety channels that are utilized, it applies a similar LSB rule, where the mystery is concealed at all critical pieces of the pixels.

It is guessed that this randomization would support both the framework's ability and security. This technique can be utilized with RGB pictures, where every pixel's red, green, and blue powers are each addressed by three bytes.

Digital watermarking using improved human visual system model:

One goal of digital watermarking is to inject as much watermark signal as feasible without dramaticallylowering image quality. Utilizing the eye's masking ability, one may boost the signal in areas of crowded or high contrast imagery. Several writers have suggested using a model of the human visual system to apply to watermarking. However, if a straightforward contrast measurement is made, connected directional edges might start to exhibit an unfavorable ringing effect.

In this study, we present a technique for separating high frequency textured regions with no preferred edge direction from related directional edges. While the gain in high contrast textures is raised, the watermark gain on linked directional edges is decreased. Overall, this method allows for a stronger watermark to be used for the same amount of visual degradation since it is boosted in areas where it isnot genuinely disagreeable and reduced in those where it is.

III EXISTING SYSTEM

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 frequencydomain 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 ofthe 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 asreduced 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 signalof same strength is causing less visual distortion in busy areas of the image than the flat background. Inthe papers (Podilchuk and Wenjua, 1998; Hannigan et al., 2001) on watermarking, there is less effort toevaluate 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 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 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). 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). 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 forlow 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 ofmodified cover image pixels. Then a bit inversion mechanism is applied where certain LSBs of pixels are modified if they occur in a specific format. 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 achievehigh 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 hiddentext. 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 truthtable based and determinate array on RGB indicator that uses pixel manipulation, shows amazing resultsin 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 changingthe remainder or value of modulus.

IV PROPOSED SYSTEM

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.

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 new mechanism of cryptography and bitpairs 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 watermark logo in encoding section as well as decrypt the 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 and store the quotient and remainder by dividing the reversed string by a key. The process of decryptionused the algorithm 2, in which the same key is used to receive the original image pixels (Roy et al., 2011)

V IMPLEMENTATION

To implement this project we have designed following modules

1) 1 Upload Original Image: using this module we will upload original cover image

2) Upload Watermark/Hide Images: using this module we will upload watermark or hiding image

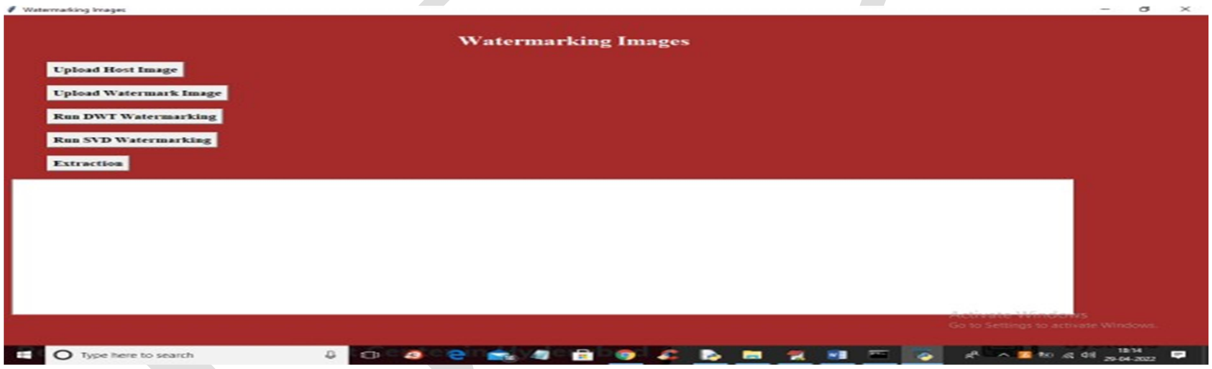
3) Run Watermark Encryption: using this module we will encrypt watermark/hidden image with symmetric key

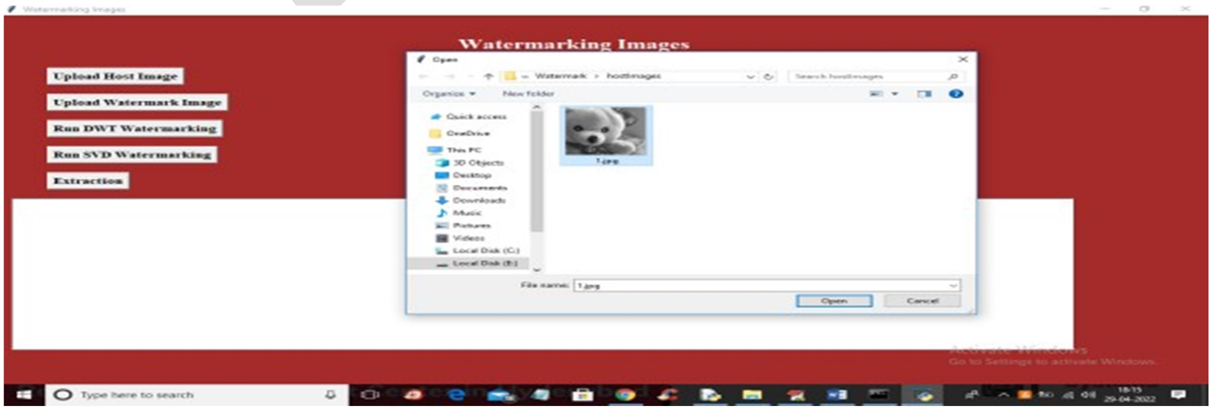
4) Encode Encrypted Watermark Pairs with Original Image: using this module we will extract pairs from both original and watermark image and then embed both pixels at same location in original image

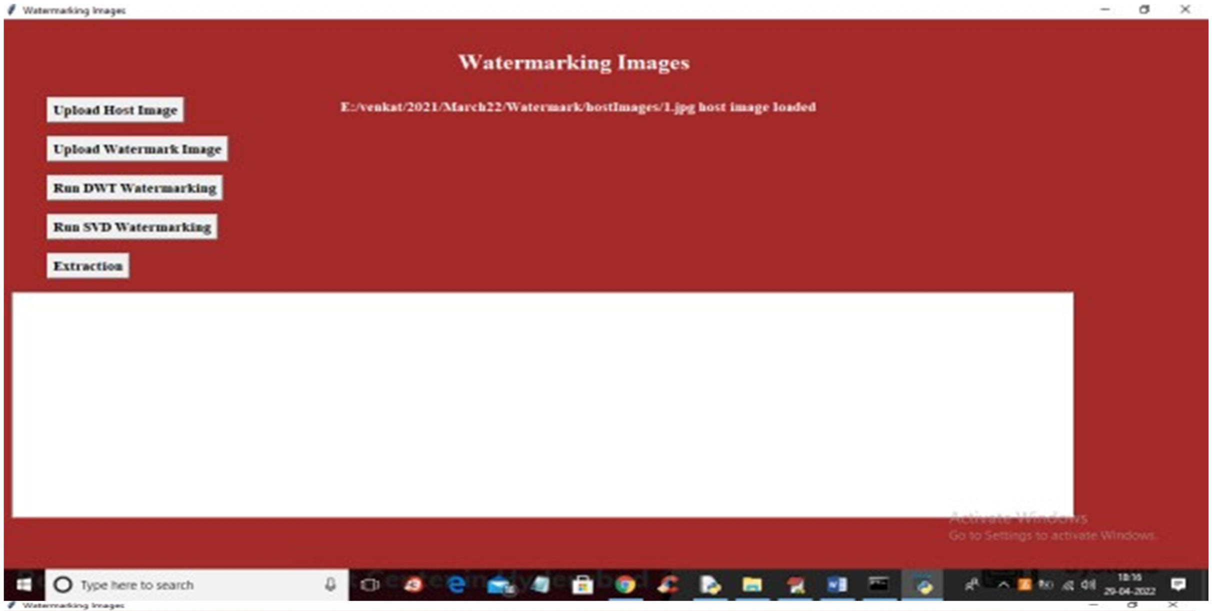
5) Decode Watermark Pairs: using this module we will take out hidden encrypted watermark imagefrom the original image

6) Run Watermark Decryption: using this module we will decrypt extracted hidden image and then calculate PSNR, SSIM and MSE between extracted image and original hidden image

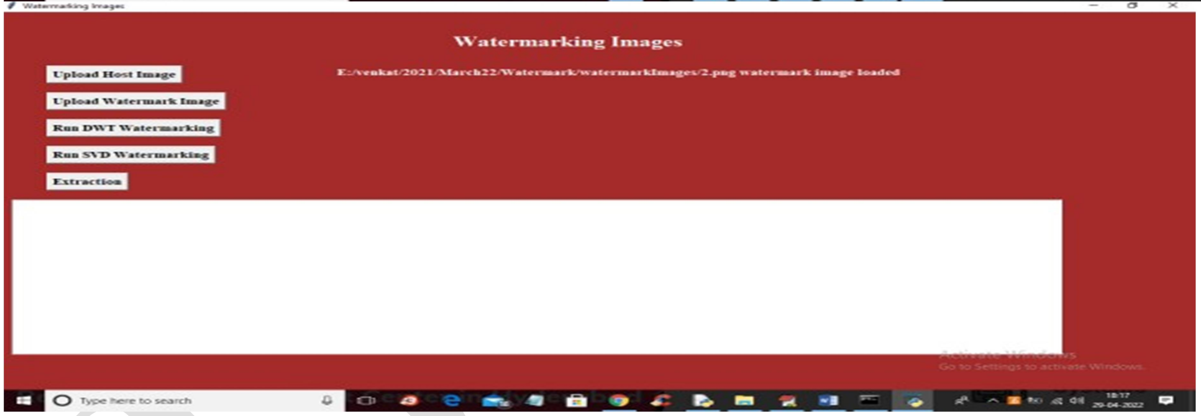
VI RESULTS



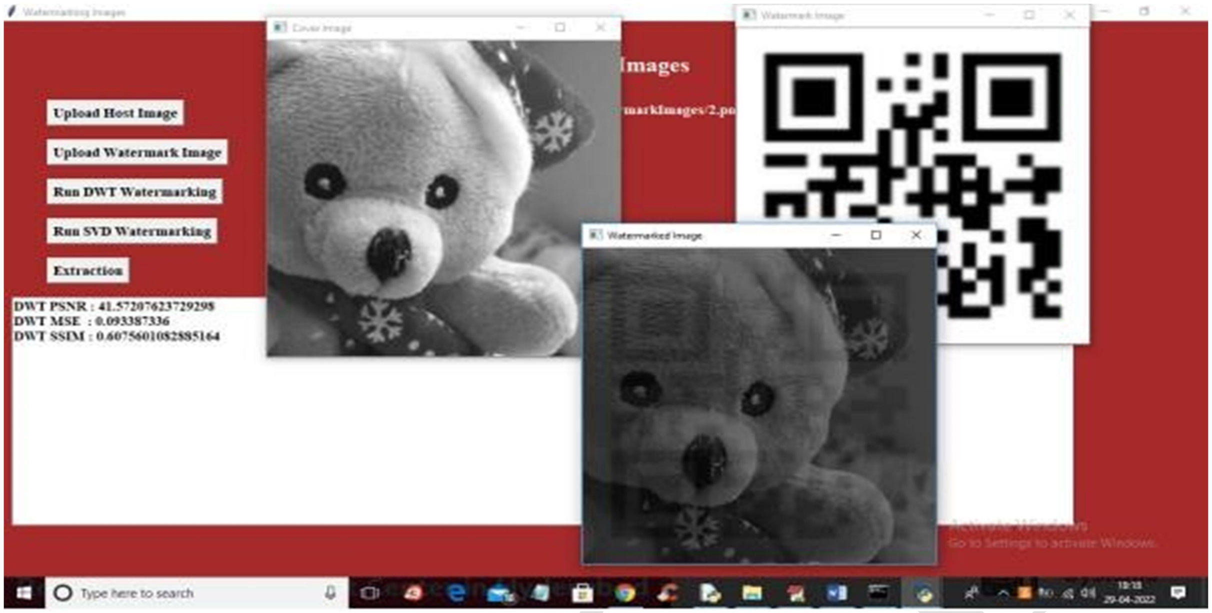




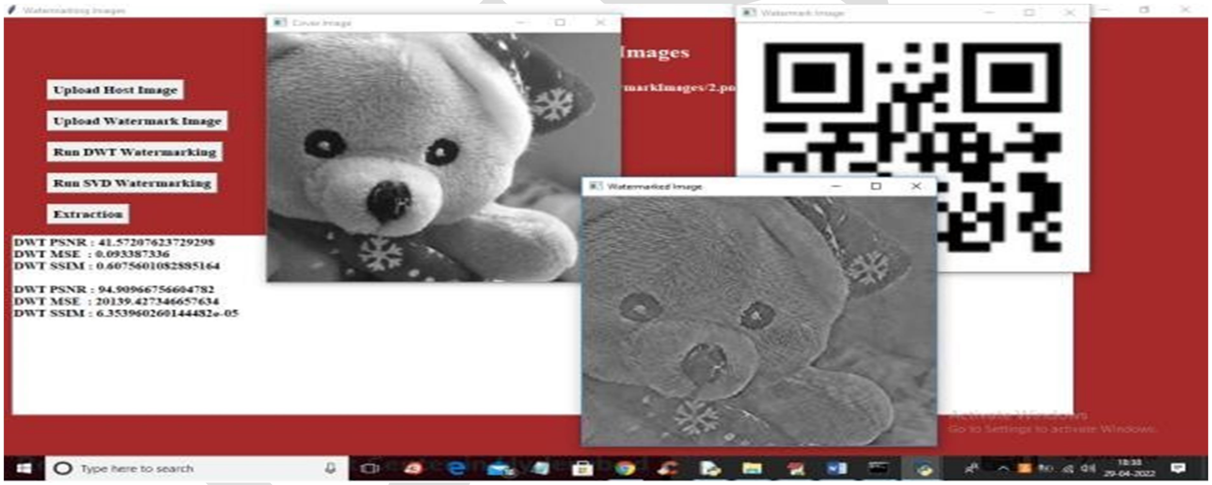
E:/venkat/2021/March22/Watermark/hostImages/1.jpg host image loaded



E:/venkat/2021/March22/Watermark/watermarkImages/2.png watermark image loaded



```
DWT PSNR : 41.57207623729298
DWT MSE  : 0.093387336
DWT SSIM : 0.6075601082885164
```



```
DWT PSNR : 41.57207623729298
DWT MSE  : 0.093387336
DWT SSIM : 0.6075601082885164

DWT PSNR : 94.90966756604782
DWT MSE  : 20139.427346657634
DWT SSIM : 6.353960260144482e-05
```

VII 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 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 we have done.

REFERENCES

1. Al-Otaibi, N.A., Gutub, A.A.A., 2014. Flexible stego-system for hiding text in images of personalcomputers 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 letters forarabic 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 basedon 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 human visual system model. In: Ping Wah Wong, Edward J. Delp (Eds.), Proc. SPIE. 4314, 468-474, Security andWatermarking 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 ConventionCentre, Manamah, Bahrain.