Journal of Theoretical and Applied Information Technology
15th August 2022. Vol.100. No 15

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

IMPROVE THE EFFICIENCY FOR EMBEDDING IN LSB METHOD BASED DIGITAL IMAGE WATERMARKING

ALAA ABDULSALAM ALAROOD[1]

[1]College of Computer Sciences and Engineering of the University of Jeddah, Jeddah, Saudi Arabia

E-mail: [1]aasoleman@uj.edu.sa, alaa.alarood@gmail.com

ABSTRACT

The internet revolution has caused the current dramatic reform of multimedia applications. The progression of the internet has significantly eased the transfer of data/image, making the transfer faster and more accurate. However, such advancement has also facilitated modification and misuse of valuable information, by way of hacking. Digital watermarking has been proposed to protect the copyright of multimedia data. A watermark encompassing a form, image or text is embedded. Hiding information is an effective solution for the protection of copyright and confidentiality to allow a person to send the data in the middle of the cover image to a person without knowing any third party in this transmission, methods of delivering secret messages are very important. This research provides a way to hide data (which is a text file) after is encrypted adoption method (Keyword Mixed Transposition) to produce cipher text is included in Low–High coefficient wavelet transform and get a good quality image and the possibility of recovering fully embedded message and decoded without relying on the original image. Results have applied to the digital images to get inline images to the data with a high correlation coefficient when compared with the original images in addition to that they gave a few differences when calculating measurements (SNR, PSNR, MSE) This study demonstrates the implementation of watermarking technique, both the invisible using (Least Significant Bit) algorithm and visible forms. Further, image watermarking and various security issues are reviewed. Countless attacks were attempted on the watermarked images. Then, their effects on the quality of images were examined. Image Watermarking using Least Significant Bit (LSB) algorithm was applied for message/logo embedment into the image and the Experiments have shown that the proposed embedding process has increased the embedding efficiency as it does not require going through all bits to modify.

Keywords: *Watermarking, Least Significant Bit (LSB), Mean Square Error (MSE) and Peak Signal to Noise Ratio (PSNR).*

1. INTRODUCTION

Watermarking is a technique used for data concealment or for information identification in digital multimedia. Digital images, digital video, audio, and documents are among the commonly watermarked items, but digital image watermarking is the focus of this study. The use of digital watermarking is increasingly common, particularly on the appendage of imperceptible identifying marks, for instance, the author or copyright information. In the process of digital watermarking, a signal is embedded into the media in a manner that does not notably degrade the media's visual quality. Digital watermarking encompasses a process of embedding a type of information termed as 'watermark' and this watermark is embedded into various forms of media known as Cover Work. The process allows information to be concealed within a signal, and the third party cannot extract this information easily. Copyright protection of digital information is a very popular application of digital watermarking, and compared to encryption, it allows access, view and interpretation of the user to the signal, while the content ownership remains preserved. In digital watermarking a structure is embedded within a host signal with the purpose of ownership "marking." As digital watermarks are embedded within the information, the third party cannot take ownership of the said information. There are two forms of watermarks, namely visible watermarks and the more common ones, the invisible watermarks.

The advancement of information technology and the digitization era have intensified the reliance of man towards files in digital form, resulting in the need for a large space for storing such files. However, such need is costly as clients would have to purchase new devices, expand their storage spaces, or even purchase the external storage units

[1]. Fortunately, Cloud Computing seems to be the solution to the problem as it offers computing and storage space with no costly tools and equipment required for the storage of all the files and applications on the cloud. This solution is beneficial, but like most technology solutions, the issue of security is often overlooked. As such, the issue of security has to be taken into account. In this situation, the use of cloud file authentications protects the file from alteration, being copied, or being attacked during transmission or storing [2].

Accordingly, the focal point of this study is cloud image authentication. Cloud image authentication has been chosen owing to its significance is usage today. Also, images have been the most uploaded type of file on cloud. Therefore, it is necessary to enhance the security level of these images, and this can be achieved using digital watermarking technique [3]. Equally, digital watermarking technique has been an important topic in digital intellectual property, as it involves the copyright protection of cloud images. Considering that watermarking allows the embedment of ownership data to multimedia data, the data could be extracted later in the authentication of multimedia ownership. The use of watermarking could inhibit copying or proscribed image distribution over the internet, in addition to guaranteeing the originality of the images [4].

This Paper hence demonstrates the application of watermarking technology to the uploaded images in Cloud web. Common cloud attack is executed on the images to evaluate the image watermarking in terms of its efficiency.

In this paper a improve the efficiency of watermark technology by LSB based is proposed. In the presented scheme using a LSB representation of digital images, embedding key and extracting key from image. This paper is organized as follows: The next section introduces Background of watermarking by LSB based embedding image steganography algorithm Our proposed in Section 5 presents the software simulation of embedding and extracting. Finally, a short conclusion is given in Section 8.

2. BACKGROUND

Nowadays digital multimedia is traveling all over cyberspace to their owners especially with the massive usage of cloud computing.

2.1 Cloud computing

The multi-purpose cloud computing is regarded as an on-demand delivery platform of resources with the internet as the medium, and Cloud computing allows various data related activities to be carried out including web applications, data backup, disaster recovery, and more [5].

Many great features can be found in cloud computing, and therefore, high level of Privacy and Data Security is needed in this form of computing. Cloud privacy is established through various supporting pillars including Data Integrity, Data Segregation, Legal Compliance, just to name a few, and their lack can severely affect organizations (R. Velumadhava Rao and K. Selvamani).

Cloud computing is used mainly for multimedia storage. However, during transmission, these media are at risk of being copied, modified, or attacked by other users and they could assign them to themselves.

2.2 Watermarking

The digital watermarking technology encompasses information concealment and embedment concept, with the purpose of guaranteeing the rightful users their intellectual property rights [5].

The technique of watermarking generally takes two phases. The watermark is embedded in the first phase, and the watermark is then extracted in the second phase (refer Figure 2.2). The process of embedding involves the encoding of watermark into the cover image. A key is used, whereby it generates the watermarked image to be transmitted to the receiver. Meanwhile, the process of extracting occurs during transmission whereby the watermark is extracted from the watermarked image. Accordingly, to comprehensively understand the mechanisms of Cloud and the issues associated with Cloud, this section reviews and analyses past relevant studies on cloud authentication techniques.

2.3 Types of watermarking attacks

Various challenges have been facing digital watermarking and cyberattacks have been the major ones. Among the common types of cyberattacks are simple attacks as can be exemplified by the activities of cropping, removal attacks as can be exemplified by the activities of compression and copy attacks [6].

As one form of cyberattack, simple attack encompasses an effort of manipulating the watermarked image by removing the embedded data from the initial image. Compression and cropping are examples of simple attack. Meanwhile, removal attack encompasses an effort

of analyzing and separating the watermarked data from the host image. In this attack, the watermark is ruined but the security of the watermark algorithm is unaltered. Contrariwise in copy attack, the watermark is not affected at all because this type of attack simply copies the watermark for the purpose of allowing the authentication of an unauthentic image [6].

2.4 Performance of Watermarking

In the applications of digital image processing, image quality evaluation is important. There are two main methods of quality evaluation namely the subjective evaluation method and the objective evaluation method, whereby the former utilizes human judgment with no specific criteria used, while the latter involves comparisons and the use of numerical criteria as in PSNR, SSIM, and BER, as briefly explained below [7]:

- PSNR or Peak to Signal Ratio is a commonly used instrument in image quality measurement. PSNR is simple and easy, making it a popular choice among users. PSNR evaluates the watermarked images concerning their imperceptibility following watermarked image extraction. The measurement involves the use of mean squared error between the cover image value and the watermarked image pixels [8].

- SSIM or Structural Similarity Index Measure is an instrument that measures image quality through the discovery of resemblance between two images. SSIM is a popular instrument among users.

- BER or Bit Error Rate entails the number of bit errors/time. Equally, it entails the division of the number of bit errors by all bits transferred during a given time interval [8]).

Manuscripts must be in English (all figures and text) and prepared on Letter size paper (8.5 X 11 inches) in two column-format with 1.3 margins from top and .6 from bottom, and 1.25cm from left and right, leaving a gutter width of 0.2 between columns.

3. OVERVIEW OF RELATED WORK

This section explores several past related studies on cloud authentication. Techniques for cloud authentication are various and among them include Cryptography, hashing and watermarking – these techniques will be reviewed in this section.

As multimedia is expanding, image authentication becomes a pressing issue in cloud environments as images are being transmitted via non-secured environments like the internet. It is thus important for these images to be protected so that they would not be manipulated, copied, or attacked [9].

A system to secure cloud computing was proposed by Dheyab and Ibrahim (2019). The system involved the use of two-level encryption, using DES algorithm and RSA algorithm for secret data encoding. In the system, after the encoding process, steganography was applied to conceal the encrypted data via the use of LSB algorithm. Using this system, the encrypted secret data are concealed in the image and the data are kept in the cloud data center, to be retrieved when there is a need for it [10].

A system of Visual Cryptography was proposed by Mbarek, Ali and Hassan (2017) with the objective of protecting the integrity, confidentiality, and data ownership of medical images stored within Cloud, without the use of complex mathematical computations. In this system, the secret image is broken down into several shares and each share is then then sent to a different Cloud, increasing data privacy. Hence, for secret medical image retrieval, client must obtain the encrypted image shares from various clouds and overlay them to generate the full usable image [11].

A system known as Cloud-centric, multi-level authentication CMULA was proposed in Ismail, Melike, Burak, and Houbing (2016) to ease the application of public safety. To produce the digital signature and verification between user and cloud service provider (CSP), the system applies Elliptic Curve Digital Signature Algorithm (ECDSA), while the exchange of secret message authentication code is made possible using Elliptic Curve Diffie Hellman (ECDH) [12].

The use of two-factor authentication (TFA) was proposed and demonstrated by Lonel, Adrian, and Alin (2019). TFA is used for user authentication in private cloud for instance, in CloudStack or in Eucalyptus. TFA provides an extra level of security, through its requirement of two variable factors namely the knowledge factor involving the requirement of user presence and password, and the possession factor involving the use of a device for producing the code of TFA [13].

The application of a Text-image watermarking method using integer wavelet transform (IWT) and discrete cosine transform (DCT) was proposed and demonstrated in Reem and Lamiaa (2019). In the proposed method, IWT was used on the cover image while DCT was embedded to the LL sub-band. The watermarked image was inserted to DCT in order to increase robustness and imperceptibility [14].

The aim of this paper is to develop an embedding algorithm in LSB method that embed the message entered the image in a fast and efficient manner without going through all the image bits and this reduces the time in embedding.

The issue of hiding and encrypting information is one of the topics that were worked on early and developed quickly and advanced with the entry into the world of digital images, which was the focus of the attention of many researchers. Below are several studies in this field:

The researcher Alarood (2022) describes a new steganography algorithm for encoding secret messages in MP3 audio files using an improved least significant bit (LSB) technique with high embedding capacity. Test results obtained shows that the efficiency of this technique is higher compared to other LSB techniques [15].

The researcher Eman (2018) suggested a way to hide the data in binary images, as the points are first identified The optical image that can be flipped without visible distortions in the embedded image, by using A set of laws by which all points adjacent to the center point of each irregular sector are examined And then the central point is changed only if the sector matches these conditions and this property allows By detecting the embedded data without referring to the original image, experiments have shown different results for images different binary[16].

Researcher A. A. Abdul Latef (2008) method of masking in color images by dividing them into Four equal parts, each part consists of three channels (Blue, Green, Red) (choose one of these Channels for each part depending on the high color ratio in that part, then the wavelet transform is applied on the selected part, and the message to be hidden is also divided into four parts and DCT is applied to it Then each part of it is embedded in the high frequencies of the wavelet transformation of one of the parts of the cover images to obtain on the secret photo[17].

As for the researcher Yong (2011) he proposed a scheme to hide the secret data inside the image using a transform curvelet where the image to be hidden is encoded using a Radon transform (and using. parameters). High frequency curvelet transform to include data [18].

The researchers Abdelwahab and Hassan (2008) suggested using the first level of wavelet transformations in data hiding and embedding but the extracted data was not entirely the same as the embedded version [19].

As for this study, it dealt with a new algorithm through which texts are included within the gray images, and this algorithm relied on embedding the data directly inside the image, the most important section is to find the number of binaries that will be included within the section The least important of the point, and this algorithm was characterized by increasing the amount of data that can be hidden, and the ability to retrieve the written text without errors, and it gave a higher degree of reliability to ensure the integrity of the image before retrieving its contents, and the data inside the image was randomly included, which gave it a higher security And resistant to extraction by vandals.

4. PROPOSED METHOD

Following the LSB technique, new watermarking algorithm is proposed in this study whereby it encompasses the application of high performance first LSB for concealment of data within an image. The framework of the method is presented in Figure 2. The process begins with the selection of a grayscale image, followed by the transmission of data to binary value after typing it. Using the proposed algorithm, the data is then concealed within the image. The embedding algorithm in MATLAB can be viewed in part A. Next, the watermarked image is obtained, and the receiver will retrieve the data again. The extracting algorithm in MATLAB. The data will be extracted from the watermarked image.

Journal of Theoretical and Applied Information Technology
15th August 2022. Vol.100. No 15

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

4.1 Embedding Algorithm

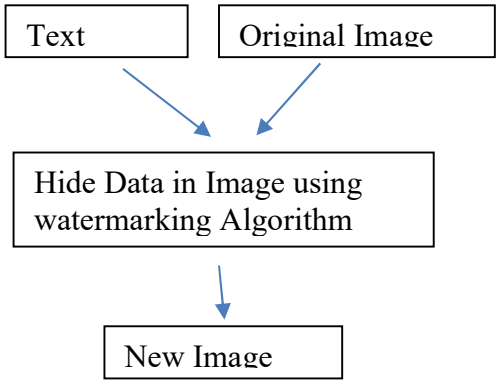

Figure 1: The Framework Of The Proposed Method

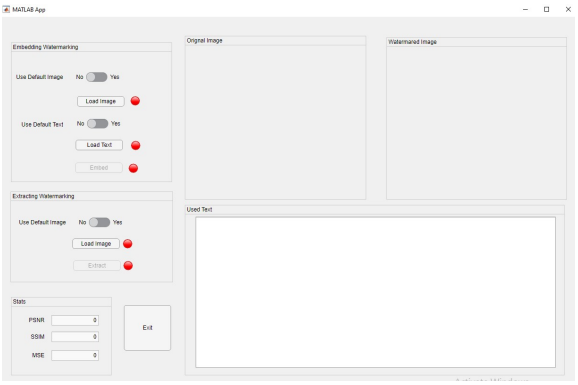

Figure 2: The Framework Of The Proposed Method

The present section provides the illustration of the mechanism of embedding algorithm. After the image is chosen and the secret data is typed, the secret data is then transmitted to binary values. Here, the image coordinates of which the data will be embedded will be determined. As the first step, file length will be appended at the beginning, and then, both file sizes are tested and then converted from char to binary. Here, the bits will be determined, either to be set to 1 or 0. This will increase the performance of embedding bit from text to the image. Next, the correct bits are set to 1 and 0, while the remaining are left as is. Then, the watermarked image will be generated and then saved. The following Figure 3 displays the embedding algorithm.

Step 1: Read Image
Watermared_Image = imread(Original_Image_Name);
Step 2: calculate file size of text
fid = fopen(text_file_name).
text = fread(fid).
Step 3: Read Text
fid = fopen('UserName.txt').
UserName = fread(fid).
Step4: Add file length at the beginning
text = [num2str(length(text) + length (UserName) + 1) " UserName " text];

Step 5: Test both file sizes
assert(numel(Watermared_Image)>numel (text)*8, 'Insufficient number of pixels');
Step 6: Convert from char to binary
Binary_Text = transpose(dec2bin(text,8)).
Step 7: Find which bits should be set to 1 or 0
ind_0 = find (Binary_Text == '0');
ind_1 = find (Binary_Text == '1');
Step 8: Set the appropriate bits to 1 and 0 and leave the rest alone
Watermared_Image(ind_0)=bitset(Watermared_Image(ind_0),1,0);
Watermared_Image(ind_1) = bitset (Watermared_Image(ind_1),1,1);
Imwrite (Watermared_Image,'Watermared_Image.bmp').
Step 9: end

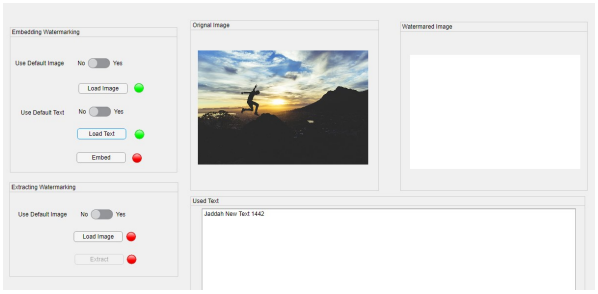

Figure 3: The Framework Of The Proposed Method

4.2 Extract Algorithm

The current section presents the details of the extracting algorithm. Following receipt of the watermarked image, the secret data LSB length will be attained beginning from the established coordinates. Secret data can be attained as well in binary values which will then be transferred to characters that will be displayed as the secret data. The extracting algorithm can be viewed in Figure 4.

Step 1: Read Image
Watermared_image = imread(Watermared_image_name);
Step 2: Get File Length and Extract the LSB from a set of 8 bytes in the image
File_Length = [].
for pixel_index = 1:8: numel(Watermared_image)-7= bitget(Watermared_image(pixel_index:pixel_index+7),1);

Step 3: Convert from binary to decimal
C = bin2dec(num2str(C)).
Step 4: Check the space character
If (C == ' ') break.
Else File_Length(end+1) = C;
File_Length = char (File_Length).
Num_size= (length (File_Length) +1);
K=str2num (File_Length) + Num_size;
n=1.
Step 5: Get Text
text_back = [].
while(K~=0)
Step 6: Extract the LSB from a set of 8 bytes in the image
C = bitget(Watermared_image(n:n+7),1);
Step 7: Convert from binary to decimal
C = bin2dec(num2str(C));
Text_back(end+1) = C;
n=n+8;
K=K-1;
Step 8; end
Before extract the file version of text must Convert from double to text and delete file length from the beginning finally Save to text file
text_back = char(text_back).
text_back(1: Num_size)=[];
fid = fopen('Text_Dec.txt', 'w');
fwrite(fid,text_back);
fclose(fid)

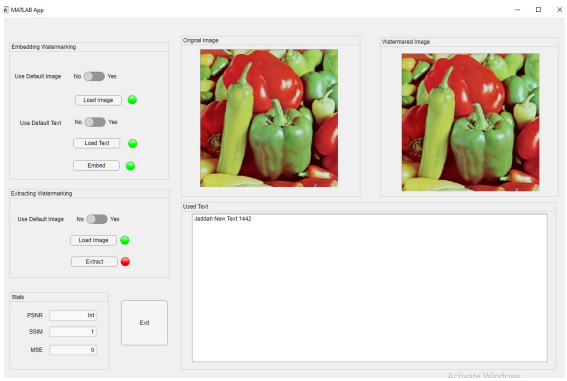

Figure 4: The Framework Of The Extract Method

5. EXPERIMENTAL RESULTS

As displayed in Figure 5, the experimental results of this study involved the use of four 512x512 grayscale images applied as cover images. Similar secret data of 128 bytes in determined pixels were embedded within the fourth and third LSB, resulting in watermarked images with no perceptible alteration. To see the difference between the original and the watermarked image, the secret data were extracted from the image and comparison was then made to both images. Similar process was repeated but using secret data of 1023 bytes. Accordingly, Figure 6 displays the watermarked images and the difference between the original and the watermarked images. Examining the difference between the original image and the watermarked image, black image was perceived owing to the change in the 3rd and 4th LSB. As shown, values of the 3rd and 4th LSB are 4 and 8, and therefore, the maximum difference of the pixels between the two images will be 12, while the value 12 in grayscale images is almost black (refer Figure 6).

6. DISCUSSION

The results demonstrate no difference between the original and watermarked images as there was no discernible distortion to the watermarked images. Accordingly, Peak signal-to-noise ratio (PSNR) was computed to ascertain the quality of the watermarked images. The use of PSNR is common in measuring the reconstruction quality in image compression [4], and PSNR can be interpreted very easily using the Mean Squared Error (MSE) whereby for two mXn images I and K, one image is deemed as a noisy estimate of the other. Accordingly, MSE is expressed in equation (2) while PSNR is expressed in equation (1).

The PSNR of the proposed algorithm was computed using equations (1) and (2). Specifically, the computation results, which are provided in Table 1, will demonstrate the quality of the watermarked images.

In general, the obtained values of PSNR will be in the range between 30dB and 40dB [4], and the PSNR value of watermarked image of greater than 30 means that the differences in the cover image cannot be seen by the naked eye. Accordingly, Figure 5 displays the cover images while Figure 6 displays the watermarked images and the difference between them alongside the original images. It is clear from the results that the watermark generated using the proposed system has good invisibility. Also, the original and the watermarked images are indistinguishable by the naked eye (human visibility system (HVS). Further, results of PSNR computation can be observed in Table 1, and as shown, the four images scored PSNR value of greater than 52 for the embedment of 1023 byte as a secret data, while the embedment of secret data of smaller size (128 bytes) yielded better PSNR value of 61.

In this paper, the presented embedding method has increased the effectiveness of the embedding process in an effective manner without referring to all the bits in the images, as all researchers require going through all the bits in the images to include the message.

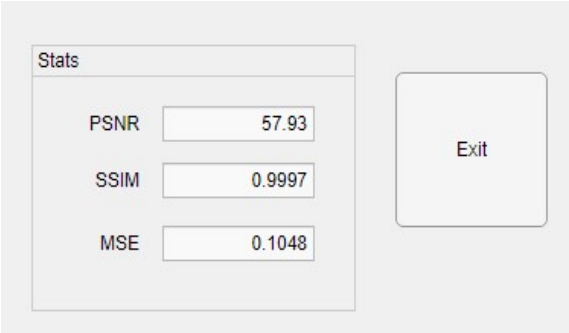

Figure 5: The Framework Of The Extract Method

7. CONCLUSION

The essential goal of watermarking is to resist not only the geometric distortion attack but also the signal processing attack. The performance of a watermarking method is depended on various parameters to be considered. In classical information there is no watermarking procedure resists all types of attack. But still many researchers are working on finding better technique which will give more robust. In this paper, Improve the performance for embedding in LSB method Based Digital Image Watermarking is presented in which through embedding key by the original owner of the carrier image. In this scheme to represent the algorithm to embedded key in images, the Algorithm presented by LSB based watermarking indicates that only the legal owner of the original carrier image knows the extracting key. Furthermore, by analyzing the histogram graphs one can see that the histogram graphs of the original images and the corresponding watermarked images are in a good agreement and the original cover image, and the watermarked signal are perceptually indistinguishable. The embedding of secret data by LSB method in the image was to determine the coordinates, and the resulting watermarked image showed no discernible distortion. Hence, the proposed digital watermarking algorithm has proven its sound ability in concealing data within an image.

The study shows, after applying the proposed algorithm on image of different sizes of secret message the embedding process took less than 3 seconds, and therefore the efficiency was working in an exciting way.

REFERENCES:

[1] Author No.1, Author No 2 Onward, "Paper Title Here", *Proceedings of xxx Conference or Journal (ABCD)*, Institution name (Country), February 21-23, year, pp. 626-632.

[1] Srinivas, J., K. Venkata Subba Reddy, and A. MOIZ Qyser. "*Cloud computing basics.*" International journal of advanced research in computer and communication engineering 1.5 (2012): 343-347.

[2] Mirashe, Dr-Shivaji, and N. Kalyankar. Cloud Computing. Mar. 2010.

[3] S. Bharati, et al. Analysis of DWT, DCT, BFO PBFO Algorithm for the Purpose of Medical Image Watermarking. 2018, pp. 1–6, doi:10.1109/CIET.2018.8660796.

[4] Lala, Hina. "*Digital Image Watermarking Using Discrete Wavelet Transform*." International Research Journal of Engineering and Technology, vol. 4, 1, 2017, pp. 1682–85.

[5] Cox, Ingemar, et al. Digital watermarking and steganography. Morgan kaufmann, 2007.

[6] Khaleghparast, Reza. Image Authentication and Rightful Ownership Watermarking Method for the Cloud Environment. Diss. Auckland University of Technology, 2017.

[7] A. Horé, and D. Ziou. Image Quality Metrics: PSNR vs. SSIM. 2010, pp. 2366–2369.

[8] Khajanchi, Neha, and Vishakha Nagrale. "*To Apply Watermarking Technique In Cloud Computing To Enhance Cloud Data Security*.". IJSDR, July 2019.

[9] Haouzia, Adil, and Rita Noumeir. "*Methods for Image Authentication: A Survey*." Multimedia Tools and Applications, vol. 39, no. 1, Aug. 2007, pp. 1–46, doi:10.1007/s11042-007-0154-3

[10] Ibrahim, Dheyab Salman. "Enhancing Cloud Computing Security using Cryptography & Steganography." Iraqi Journal of Information Technology. V 9.3 (2019): 2018.

[11] Marwan, Mbarek, Ali Kartit, and Hassan Ouahmane. "*Protecting medical images in cloud using visual cryptography scheme*." 2017 3rd International Conference of Cloud Computing Technologies and Applications (CloudTech). IEEE, 2017

[12] Butun, Ismail, et al. "*Cloud-centric multi-level authentication as a service for secure public*

safety device networks." IEEE Communications Magazine 54.4 (2016): 47-53.

[13] Gordin, Ionel, Adrian Graur, and Alin Potorac. "*Two-factor authentication framework for private cloud*." 2019 23rd International Conference on System Theory, Control and Computing (ICSTCC). IEEE, 2019.

[14] Alotaibi, Reem A, and Lamiaa a Elrefaei. "*Text-Image Watermarking Based on Integer Wavelet Transform (IWT) and Discrete Cosine Transform (DCT)*." Applied Computing and Informatics, vol. 15, 2019, pp. 191–202.

[15] Alarood, Ala and teal. "*Audio Steganography Method Using Least Significant Bit (Lsb) Encoding Technique."* IJCSNS International Journal of Computer Science and Network Security VOL.22 No.7, July 2022.

[16] Eman Th. Sedeek Al-obaidy,(2008), *"An Algorithm for Data Hiding in Binary Images*", Raf. J. of Comp. & Math's., Vol. 5, No. 2, 8.

[17] A.A. Abdul Latef, (2011), "*Color Image Steganography Based on Discrete Wavelet and Discrete Cosine Transforms"*, IBN AL-HAITHAM J. FOR PURE & APPL. SCI.VOL.24 (3).

[18] Yong Hong Zhang, (2011), *"Digital Image hiding using curvelet transform*", IEEE Conference.

[19] A.A. Abdelwahab, L.A. Hassan, (2018), "*A discrete wavelet transform based technique for image data hiding"*, in: Proceedings of 25th National Radio Science Conference, Egypt.