International Journal of
Advances in Scientific Research and Engineering (ijasre)

E-ISSN : 2454-8006

DOI: 10.31695/IJASRE.2021.33985

Volume 7, Issue 3
March - 2021

Subject Review: Information Steganography Based on Different Methods

Amal Abdulbaqi Maryoosh[1], Zahraa Salah Dhaief [2] & Raniah Ali Mustafa[3]

[1-3]Computer Science Department

Collage of Education

Mustansiriyah University, Baghdad

Iraq

ABSTRACT

Today, huge amounts of information are transmitted over the communication networks, especially via the Internet. Therefore, many individuals are concerned with data security. Various methods were appeared to maintain data security, and the most common of these methods are cryptography. Encryption methods are exposed to many attacks, and if the attacker obtains the key, the data is decrypted, so many algorithms have emerged to hide the information within the multimedia. When the attacker gets the data, he will not suspect that this multimedia may contain other information. Data security may depend on the type of hiding algorithm used and sometimes encryption is used in conjunction with hiding to increase data security. The major aim of this work is reviewing and describing many approaches utilized for hiding data within multimedia and to create a comparison of these methods.

Key Words: *Steganography, Cryptography, LSB, DCT, DWT, SLT, IWD.*

1. INTRODUCTION

Nowadays people need to exchange large amounts of digital data (voice, image, video, and text) across different types of networks, which led to exposed these data to risks. Steganography and cryptography are of high importance in information security. Also, cryptography is a tool used to save information security by encrypting it. Steganography is a tool for saving information security by storing the information in a multimedia file in a way that is not known via anyone apart from the receiver and the sender. Cryptography and steganography have the same objective but achieved in different ways [1].

The concept of hiding data or steganography has been originally indicated in a work carried out via Johannes Trithemus (1462-1516) identified as “Steganographia”. In addition, the word “Steganography” is taken from 2 words in Greek language “Steganos” and “graphia” (στεγανό-ς, γραφ-ειν) which means “Covered” and “Writing”. There are various characteristics should be taken into account for designing a perfect data hiding system [2].

1. **Imperceptibility:** This is the complexity of detecting hidden information through Human Visual System (HVS)
2. **Security:** This is the technique’s resistance to attacks following realizing the secret data’s existence.
3. **Capacity:** This is considered as the amount of data which might be hidden in a cover object with no impact on its visual quality (hidden information’s efficiency).
4. **Robustness:** This is the capability of steganography object for resisting un-intentional actions such as rotation, compression, cropping, filtering and so on.
5. **Embedding complexity:** This is measuring the complexity related to data embedding algorithm.

In the latest decades, an increasing the use of steganography and cryptography for securing information transmission. This paper highlights the studies that used the steganography, and both steganography and cryptography, and we make a deep analysis and comparison among these studies. In this study, the remaining parts are arranged in the following way: The literature survey regarding a few schemes suggested in the last 10 years is provided in section 2. A comparative analysis regarding of schemes is provided in section 3. Lastly, conclusions are provided in section 4.

2. LITERATURE SURVEY

In the last 10 years, there were various approaches invented in steganography field, many types of covered and many encryption algorithms are used with them. In this section we discuss some of these studies.

Teoh Suk Kuan and Rosziati Ibrahim [3] proposed a novel method for data hiding inside cover image using steganography technique. They convert the text message to text file, then, they compressed it to zip file. After that convert the zipped text file to binary code. A method related to data hiding has been utilized by means of the series of binary codes regarding a zipped text file, whereas the key represented via a long random code. Through utilizing the method of data hiding, the last 2 binary codes from series have been encoded into an image pixel, after that, next 2 binary codes are encoded to next pixel in the image, the process has been repeated till encoding all the binary codes.

R. Das and T. Tuithung [4] presented a new approach for image steganography on the basis of Huffman Encoding. Also, there are two 8bit gray level images with size P X Q and M X N utilized as secret image and cover image. In addition, Huffman Encoding is carried out over secret image/message prior to embedding, while each one of the bits of Huffman code related to the secret image/message is embedded inside the cover image through changing the least significant bit (LSB) regarding every one of the pixel intensity values that are related to cover image. Also, the size of Huffman Table and the Huffman encoded bit stream was embedded in the cover image; thus, the Stego-image will be considered as a standalone information to receiver.

Mazhar Tayel, et al. [5] suggested an algorithm to hide sound, text or image. The suggested algorithm on the basis of coordinating the data in image dimensions with the use of chaos distribution arrangements. Also, the data is embedded with the original image in in pixels' LSBs; thus, it won't appear within the image. When the image received the embedded data was separated and re-arranged with the use of initial condition regarding chaos coordination.

Kshetrimayum J. Devi [6] purposed image based steganography that LSB approaches and pseudo random encoding method on images for enhancing the communication's security. With regard to LSB technique, the major idea is replacing cover image's LSB with the message bits to be hidden without significantly damaging the cover image property. In terms of the Pseudo Random method, a random-key has been utilized as one of the seeds for Pseudo Random Number Generator required in the process of embedding. The two approaches utilized Stego-key, whereas embedding the messages in cover image. Through utilizing the key, the possibility to get attacked via attacker is decreased.

N. Sathisha et al. [7] proposed spatial domain steganography approach to embed secret information on the conditional basis utilizing 1bit of Most Significant Bit (MSB). In addition, the cover image is decomposed to 8x8 matrix size block, whereas the first block related to cover image is embedded with the 8 bits regarding lower band and upper bound values needed to retrieve the payload at destination. The median values' mean and the difference between consecutive pixels regarding every one of the 8*8 blocks of the cover image is specified for embedding the payload in 3-bits of LSB and 1-bit of MSB on the basis of prefixed conditions. Furthermore, it has been indicated that the security and capacity is enhanced in comparison to current approaches with adequate PSNR.

A new algorithm for image steganography had been suggested by Nameer N. El Emam and Odai M. Al-Shatanawi [8] for hiding large amounts of the secret data provided via a secret color image. The proposed algorithm was on the basis of modified least significant bits (MLSB) and different size image segmentations (DSIS), in which the DSIS algorithm is utilized for randomly embedding a secret image rather than sequentially; such method is utilized prior to the process of embedding. Also, the number of bits being replaced at each one of the bytes is non-uniform, it bases upon byte properties via developing an efficient hypothesis. Furthermore, the simulation results are justifying that the suggested method has been effectively used and it satisfies high imperceptible with high payload capacity which reach 4 bits for each byte.

Atheer Alaa and Marwa Jaleel [9] proposed an algorithm to hide encrypted secret images in grayscale and color images. The proposed algorithm first analyzes the secret image with the use of 1level -DWT and SLT. It was encrypted the low-frequency components related to secret image only with the use of AES approach and after that embedded in the insensitive mid as well as high sub bands obtained from the cover image in a wake of utilized 2level- SLT and DWT on it, whereas the embedding approach utilized in this study is LSB, the subsequent image is referred to as Stego-image form various algorithms were after that put to comparison. By means of the suggested algorithms, the capacity related to hidden secret data and Stego image quality have been enhanced. Furthermore, the embedding image reach half the size of cover image at the same time when PSNR reach 62 dB and MSE about 0.36.

DOI: 10.31695/IJASRE.2021.33985

In Saja M. and Aser M. proposed an enhanced approach combining AES for steganography and cryptography and benefiting from utilizing high frequency coefficients related to cover image via using DWT. Also, the suggested approach has been used for studying the impact of hiding an encrypted secret message in 24bit RGB image. Furthermore, the performance related to the suggested approach has been measured regarding histogram distribution analysis, payload embedding capacity and PSNR analysis. The experimental results specifies that the suggested approach provides a secure approach for data hiding and showing robustness against many attacks [10].

Mohammed J. Bawaneh [11] used the Intelligent Water Drop (IWD) algorithm with the Least Significant Bit (LSB) technique to construct a novel framework for the bitmap images. The proposed system works with a different format of images by transforming them into virtual grayscale 24 bitmap ones. It used the IWD algorithm to construct a path of pixel locations that was employed in the embedding process. The path was built from the virtual host image based on the secret message size. After that, the secret message bytes were encrypted and divided into bits. Later on, the secret bits were hidden inside the host image by using LSB such that each bit was stored within each color of the selected pixel in order to make the hidden data unnoticeable for intruders or analysts. The Extraction process requires a huge correct knowledge about the image transformation process. This knowledge can be summarized by IWD parameters, the key of the cryptography method, message length, message extension, and parameters updating functions. In experimental results, the proposed IWD system satisfied most of the main requirements for steganography; little mean square error (MSE), high visual appearance, high capacity, and robustness against extraction or detection. The maximum capacity of the embedding process gives a MSE value equals to 0.063 and visual appearance compared to the host image.

A novel steganography method was proposed by S. Berres and A. Soria-Lorente [12]. This method is on the basis of the compression standard depending on Joint Photographic Expert Group as well as the Entropy Threshold method. Also, the steganography algorithm utilized single private key and single public key for generating a binary sequence regarding the pseudo-random numbers indicating where the binary sequence elements of a secret message are going to be inserted. Eventually, the insertion occurs at the first 7 AC coefficients in transformed DCT domain. Prior to image insertion, the image is undergoing many transformations. Following insertion, the inverse transformations have been utilized in a reverse order to original transformations. In addition, the insertion occurs in the case when the entropy threshold regarding the corresponding block has been satisfied and in the case when the pseudo-random number is indicating to do this. Furthermore, the experimental works on the validation of the algorithm includes the PSNR calculation, the differences, also the histogram analysis, correlation distortion metrics, also the relative entropy, putting to comparison the same properties for the Stego and cover images. The suggested algorithm enhances the imperceptibility level examined via PSNR values. A steganalysis experiment indicates that the suggested algorithm showed high resistance to Chi-square attack.

Abdullah M. Hamdan and Ala Hamarsheh [13] proposed a novel approach for hiding text-in-text messages. The suggested approach utilized the omega network structure for hiding and extracting the secret messages. Also, the secret message generation is made in the following way, taking each original message's letter, utilizing the omega network for generating 2 associated letters from the chosen letter, and lastly, searching the dictionary for adequate English cover word for hiding the generated 2 letters. For the purpose of increasing the chances of finding adequate word, the created 2 letters must not be adjacent in cover word. Thus, white space steganography is utilized for hiding the positions regarding 2 letters in the chosen cover word.

K. Rosemary and M. Mary [14] focuses on hiding data in DCT based on JPEG images with the goal of increasing storage capacity and security. In this method, the researcher was proposed to embed the secret message inside a JPEG image by using a modified quantization table and matrix encoding process. In order to reach this goal, an algorithm was proposed in which the standard quantization table was modified to increase the storage capacity and a matrix encoding is used to reduce the distortion.

Srilekha Mukherjee et al. [15] was used Arnold's transformation and the Mid Position Value (MPV) for hiding the secret data. Arnold's transformation was imposed upon the selected cover image in first stage. This results in data bit scrambling, thereby resulting in the disruption of normal pixel orientation. Thereafter, the Mid Position Value (MPV) method was applied for the purpose of embedding the bits of the data from the private image in scrambled cover. Finally, the inverse Arnold's transformation has been implemented in the image above. Which leads to an operation of de-scrambling, in other words, returning back to normal orientation. Hereafter, the stego has been created. Each one of experimental results analyzes the results of full method. Which is why, numerous qualitative and quantitative benchmark analyses that pertain to that method were done. All results have shown that the secret data imperceptibility, in other words, undetectability is well guaranteed. In addition to that, payload is high with insignificant distortions in the quality of the image.

Kamaldeep Joshi et al. [16] proposed an image coding approach, which hides information along a chosen pixel and on the following value of chosen pixel, which is, pixel + 1. One bit has been hidden at chosen pixel, and the other bit has been hidden on the value of pixel +1. Based on 7th bit of the image pixels, a mathematical function has been implemented at the pixels'7th bits,

DOI: 10.31695/IJASRE.2021.33985

generating a temporary variable (pixel + 1). The 7th bit of chosen pixel and 7th bit of the pixel + 1 has been utilized for the purpose of hiding and extraction of the information. According to a combination of those 2 values, 2 message bits may be hidden on every one of the pixels.

Ambika et al. [17] proposed an encryption-based steganographic method. The cover image was separated to RGB components in a separate manner. Multi-level DWT has been implemented over transformed components of the image. The optimum pixels have been chosen with the use of the Multi-Objective Whale Optimization. The private image has been split to the components of the RGB. Encryptions with the use of the DES, AES, and Signcryption algorithms has been carried out over the separated components of R, G and B, respectively. The image that has been embedded within the cover image's chosen pixel point.

Ashraful Tauhid et al. [18] have suggested an innovate method for the data steganography and cryptography for the purpose of ensuring higher security communications. The suggested approach combined LSB replacement, AES and DCT for the purpose of improving data security. AES in spatial domain of cover image and the LSB replacement in transformed domain of same image was utilized after conducting the DCT on pixels. One more security layer was proposed through the application of the XOR process on the message that has been encrypted using AES with the cover image pixel values.

Pyung-Han Kim et al. [19] proposed a new approach of data hiding with the use of the multi-directional differencing of the pixel-value that has the ability of embedding the provate data in 2 or 3 directions on the colour images. The colour cover image has been split to non-overlapping parts, and pixels of every one of the blocks have been de-composed to R, G, & B channels. Every block's pixels perform re-grouping, and after that, the minimal value of the pixels in every one of the blocks has been chosen. Private data may be included within 2 or 3 directions, according to minimal pixel value with the use of the block difference value. The pairs of the pixel with embedded private data are separately included within 2 stego images for the extraction of the private data on the sides of the receiver. In the procedure of the extraction, private data may be obtained with the use of 2 stego image difference values.

Jingzhi Lin et al. [20] proposed an innovative steganographic approach for the hiding of the data in dynamic Graphics Interchange Format (i.e. GIF) images. In the case of the use of Syndrome-Trellis Codes (i.e. STC) model, the new cost assignment algorithm based on dynamic GIF image properties, which include image palette and inter-frame associations. Initially, they have performed the re-ordering of the GIF image palettes for the purpose of reducing the alterations on the pixel values in the case of the modification of index values. Due to the fact that the various alterations on the index values would have different effects upon the pixel values, they give elements that have lower degree of the impact upon the pixel values small embedding cost values. In the meantime, the small costs of embedding have been given as well to elements in areas where inter-frame variations have been sufficiently high. In addition to that, with embedding likelihoods on various frames, they have also assigned various payload values for every one of the frames for the purpose of achieving greater level of security.

Zeyad Safaa and Ghada Thanoon [21] proposed a data hiding approach in the videos with the use of LSB approach and enhancing it through the use of knight tour algorithm to conceal data within AVI video file and utilizing a key function encryption approach to encrypt the private data. Initially, the private message undergoes the encryption with the use of a mathematical formula. The key that has been utilized in that formula represents a collection of the random numbers, which are different in every one of the implementations for the purpose of warranting the hidden message safety and for the purpose of increasing the private message's security. After that, the cover video has been transformed from a group of the frames to separate images for the purpose of benefitting from the large video file size. After that, knight tour algorithm has been used for randomly choosing pixels within the frame that has been used to embed the private message in it for the purpose of overcoming the drawbacks that are related to traditional approach of the LSB, which has used the serial pixel selection and for the purpose of increasing the suggested approach's security and robustness. Afterwards, the encrypted private message is included within the chosen pixels with the use of LSB approach in bits (7&8). The observational results concluded that the suggested approach presented a better efficiency in comparison with the previous approach of steganography concerning quality by minimal 0.2578 MSE and a high 67.3638dB PSNR. In addition to that, this approach has resulted in preserving security where private message can't be concluded without the knowledge of the rules of decoding.

3. COMPARATIVE ANALYSIS OF THE SCHEMES

In this section, we will make a comparative analysis among the previous steganographic techniques depending on the cover that used in hiding data and, the steganographic techniques that used in each study, also the PSNR and MSE value. Table 1 explain the comparison among previous systems.

Table1.1. Comparative analysis of the schemes

DOI: 10.31695/IJASRE.2021.33985

Ref.	Steganography technique	Hidden data	Cover type	PSNR			MSE		
[3]	Binary coding and least significant bit	Text	Colored image	76.15			NA		
[4]	Huffman encoding and least significant bit	Gray image	Gray image	+57.43			NA		
[5]	Chaos theory and least significant bit	image, text, sound	Gray image	image	text	sound	image	text	sound
				57.6872	58.7404	58.3189	7.3150	5.7401	6.3252
[6]	pseudo random encoding(PRE) and least significant bit(LSB)	Text	Colored and gray image		Color image	Gray image		Color image	Gray image
				PRE	58.5346	61.6065	PRE	0.0911	0.0449
				LSB	58.5311	61.4733	LSB	0.0912	0.0463
[7]	Mean of Median, least significant bit, and chaos theory	Gray image	Gray image	43.82			NA		
[8]	modified least significant bit, and different size image segmentations	Colored image	Colored image	44.2470			NA		
[9]	1level –DWT, Slatlet Transform (SLT), and least significant bit	Colored and gray image	Colored and gray image	Gray	DWT	68.5329	Gray	DWT	0.0157
					SLT	74.1455		SLT	0.0040
				Color	DWT	67.4092	Color	DWT	0.0172
					SLT	71.0478		SLT	0.0062
[10]	Discrete Wavelet Transform, Pixel indicator technique, and least significant bit	Text, Colored and gray image	Colored and gray image	68.5244			0.0091		
[11]	Intelligent Water Drop (IWD) algorithm and least significant bit	Text	Gray image	80.0084			0.0006		
[12]	Discrete Cosine Transform	Colored image	Colored image	63.5			NA		
[14]	Discrete Cosine Transform	Text	Colored image	54.43			0 .4861		
[15]	Arnold transformation, Mid Position Value (MPV) technique	Colored image	Colored image	45.84			NA		

4. CONCLUSION

In this paper, we review data steganography methods based on different techniques within the period (2011-2020). At the present time, steganography has become an urgent need due to the development in the field of information technology. The most suitable way to hiding the data can be chosen by taking into account many variables such as the size of the data to be included, security requirements, and the environment in which the data is sent. For greater security, data steganography and cryptography methods can be used together. the summary of the present research, all of those approaches are advantageous for the process of the data steganography. Each one of the schemes is matchless in its own approach, which may be appropriate for various implementations. Recently, most suggested data hiding methods are increasing the level of security through the provision more than one method of security such as data hiding and encryption. Each one of the technologies has some advantages and disadvantages, which is why, new technologies were presented.

REFERENCES

[1] Sandeep Singh and Aman Singh, “A Review on the Various Recent Steganography Techniques”, *International Journal of Computer Science and Network*, December 2013, Volume 2, Issue 6.

[2] Ahmad Shaik, V. Thanikaiselvan and Rengarajan Amitharajan, “Data Security Through Data Hiding in Images: A Review”, *Journal of Artificial Intelligence*, 2017, 10 (1):1-21.

[3] Rosziati Ibrahim and Teoh Suk Kuan, “Steganography Algorithm to Hide Secret Message inside an Image”, *Computer Technology and Application* 2 (2011) 102-108.

[4] Rig Das and Themrichon Tuithung, “A Novel Steganography Method for Image Based on Huffman Encoding”, *IEEE*, 2012.

[5] Mazhar Tayel, Hamed Shawky and Alaa El-Din Sayed Hafez, “A New Chaos Steganography Algorithm for Hiding Multimedia Data”, *ICACT2012*, Feb. 2012, pp.19-22.

[6] Kshetrimayum Jenita Devi, Bachelor thesis, “A Sesure Image Steganography Using LSB Technique and Pseudo Random Encoding Technique”, *Department of Computer Science and Engineering National Institute of Technology-Rourkela Odisha*, 2013.

[7] N Sathisha et al., “CONDITIONAL ENTRENCH SPATIAL DOMAIN STEGANOGRAPHY”, *Signal & Image Processing: An International Journal (SIPIJ)*, June 2014 Vol.5, No.3.

[8] Odai M. Al-Shatanawi and Nameer N. El. Emam, “A NEW IMAGE STEGANOGRAPHY ALGORITHM BASED ON MLSB METHOD WITH RANDOM PIXELS SELECTION”, *International Journal of Network Security & Its Applications (IJNSA)*, March 2015 Vol.7, No.2.

[9] Atheer Alaa Sabri and Marwa Jaleel Mohsin, “A New Algorithm for a Steganography System”, *Eng. &Tech.Journal*, 2015, Vol.33, Part (A), No.8.

[10] Saja M. Saraireh and Aser M. Matarneh, “HIGHER LEVEL SECURITY APPROACH FOR DATA COMMUNICATION SYSTEM BASED ON AES CRYPTOGRAPHY AND DWT STEGANOGRAPHY”, *Jordanian Journal of Computers and Information Technology (JJCIT)*, December 2016, Vol. 2, No. 3.

[11] Mohammed J. Bawaneh, “A Preferential Virtual Gray Scale Image Steganography Using Intelligent Water Drop”, *International Journal of Computer Science and Information Security (IJCSIS)*, November 2016, Vol. 14, No. 11.

[12] A. Soria-Lorente and S. Berres, “A Secure Steganographic Algorithm Based on Frequency Domain for the Transmission of Hidden Information”, *Security and Communication Networks*, Volume 2017.

[13] Abdullah M. Hamdan and Ala Hamarsheh, “AH4S: an algorithm of text in text steganography using the structure of omega network”, *SECURITY AND COMMUNICATION NETWORKS*, February 2017, 9:6004–6016.

[14] K.Rosemary Euphrasia and M. Mary Shanthi Rani, “Steganography in DCT-based compressed images through Modified Quantization and Matrix Encoding”, *International Journal of Computer Science and Information Security (IJCSIS)*, February 2017, Vol. 15, No. 2.

[15] Srilekha Mukherjee et al., “Image Steganography Using Mid Position Value Technique”, *International Conference on Computational Intelligence and Data Science (ICCIDS 2018), Procedia Computer Science* 132 (2018) 461–468.

DOI: 10.31695/IJASRE.2021.33985

[16] Kamaldeep Joshi et al., “A New Method of Image Steganography Using 7th Bit of a Pixel as Indicator by Introducing the Successive Temporary Pixel in the Gray Scale Image”, *Hindawi, Journal of Computer Networks and Communications*, Volume 2018.

[17] Ambika, Rajkumar L. Biradar and Vishwanath Burkpalli, “Encryption-based steganography of images by multiobjective whale optimal pixel Selection”, *INTERNATIONAL JOURNAL OF COMPUTERS AND APPLICATIONS*, 2019.

[18] Ashraful Tauhid et al., “A Secure Image Steganography Using Advanced Encryption Standard and Discrete Cosine Transform”, *Journal of Information Security*, 2019, 10, 117-129.

[19] Pyung-Han Kim et al., “Data-Hiding Scheme Using Multidirectional Pixel-Value Differencing on Colour Images”, *Hindawi, Security and Communication Networks*, Volume 2019.

[20] Jingzhi Lin et al., “A New Steganography Method for Dynamic GIF Images Based on Palette Sort”, *Hindawi,Wireless Communications and Mobile Computing*, Volume 2020.

[21] Zeyad Safaa Younus and Ghada Thanoon Younus, “Video Steganography Using Knight Tour Algorithm and LSB Method for Encrypted Data”, *J. Intell. Syst*. 2020; 29(1): pp.1216–1225.

DOI: 10.31695/IJASRE.2021.33985