Journal of University of Babylon for Pure and Applied Sciences, Vol. (28), No. (3): 2020
Online ISSN: 2312-8135, Print ISSN: 1992-0652

Review Paper on Image and Video Based Steganography

Rusul Mohammed Neamah[1] **Saif M. Alghazaly**[2]

1. Depart. Computer Science, College of Science for Women, University of Babylon, Babylon, Iraq Wsci.rusul.moh@uobabylon.edu.iq
2. Depart. Physics, College of Science, University of Babylon, Babylon, Iraq, sci.saif.mohamed@uobabylon.edu.iq

Article Information
Submission date: 1 /11 / 2020
Acceptance date: 31/12/ 2020
Publication date: 31/ 12/ 2020

Abstract

With the great development in electronic and network information technologies, and in light of some circumstances that impose work on the Internet, which is considered to be an insecure environment for confidential information, therefore maintaining data security has become an important priority. The most important techniques used to maintain the confidentiality of the transferred data and not subject it to attackers are concealment and encryption, and these two technologies also depend on the medium that transmits the secret data, whether it is an image file, sound or video. Steganography is the science of embedding digital data in such a way no one can doubt its existence. Encryption is another technology used to protect data, when used with steganography increases the power of information protection. This paper provides an overview of techniques for hiding textual information within image and video files. This study aims to provide a summary of the method that is safer, more secure, and the ability of its payload to hide data.

Keywords: *Image steganography, Video steganography, Types of steganography.*

1. Introduction

The increasing use of the Internet for the purposes of transferring information and digital communications has resulted in endeavors to search for safer and more powerful ways to hide information. Steganography is the technique of embedding secrete data within any cover file. Steganography is frequently mistaken for cryptography on the grounds that the two are comparative in the manner that the two of them are utilized to ensure secret data. The contrast between the two is in the appearance in the handled yield; the yield of steganography activity isn't obvious however in cryptography the yield is mixed with the goal that it can draw consideration[1]. Steganlysis is procedure to distinguish of quality of steganography. Concealment strategies seek to conceal confidential information/data in a smart way so that it is not discovered within one of

the hosting media that act as a carrier of this information and to protect the security and privacy of the information transmitted or amended as required or intercepted from unauthorized interference. There are four different techniques for hiding information: image, text, video, and audio. The technology used in the four types of concealment is the least significant bit (LSB) technique that relies on manipulation and change in the less important bits and does not significantly affect the clarity of the carrier used to carry the data. The difference is the extent to which modification and development are made to the least significant bit (LSB) technology for a masking application. There are two ways to include confidential data in images in the spatial and frequency domain, and the spatial field is the most important in many concealment applications and this is what is indicated by the most recent research papers. To hide the information in the video files, the audio file is separated from the image in separate files, after which the information is hidden in one of these files, and upon completion, the audio and image files are merged back into the video file. To increase the security of the transferred data more, the encryption technology is used, whereby the secret data is encrypted with one of the encryption algorithms and then hidden inside the carrier data. The encryption process is done using a secret key and is agreed upon by the sender and recipient.

The general mechanism of information masking technology, as shown in Figure 1, which includes four main stages:

1- Media transporter: The medium used to hide confidential information known as a cover image or cover object, acts as a host to transmit the confidential information hidden inside.
2- Confidential data: confidential information may consist of text or image files and others.
3- Secret Key: A secret key called a secret key is used for encryption / decryption in decrypting the hidden information.
4- Stego (Y) media: Stego media is also called a stego object. This stage has arrived after the confidential information embedding process [2].

Journal of University of Babylon for Pure and Applied Sciences, Vol. (28), No. (3): 2020
Online ISSN: 2312-8135, Print ISSN: 1992-0652

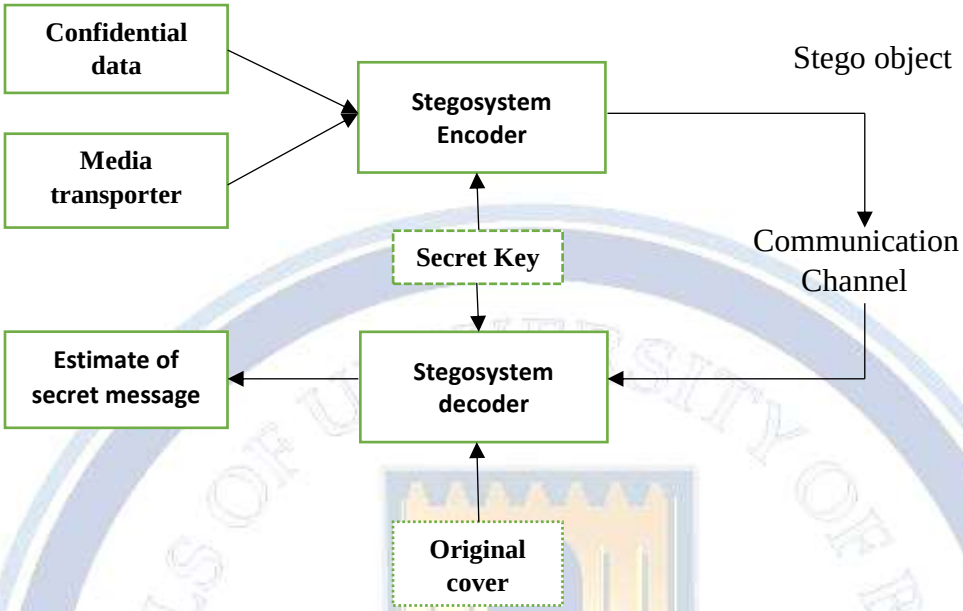

Figure 1: General Steganography Mechanism

2. Different Types of Steganography

Digital pictures are the preferred format for all digital media in Steganography because of its customary utilize and accessibility on the Internet, albeit all other digital file designs are also used [3]. Figure 2 shows the foure basic class designs for files that can be used to hide information

Figure 2: Kinds of Steganography

i. Image Steganography

Digital images are utilized to conceal confidential information, and it is the most common form of carrier/cover utilized to transmit information over the Internet. This method mainly depends on the intensity of the pixels used to hide confidential information are the most common images found on the Internet [4], [5].

Journal of University of Babylon for Pure and Applied Sciences, Vol. (28), No. (3): 2020
Online ISSN: 2312-8135, Print ISSN: 1992-0652

The technology used in this masking method is the least significant bit (LSB), and since this technique uses bits per pixel in the image, It is important to use lossless compression technology for the ability to restore data in its original form upon retrieval, because in the case of using a lossy compression technology that leads to damage and loss to the original data. It uses either grayscale or RGB images, and when using 24-bit color images the concealing process can be done for each color level (red, green, and blue) which means that we can use three bits per pixel and this is the opposite of gray images which uses one bit per pixel [6]. There are different types of image files like JPEG, PNG, BMP, etc. to hide confidential information [7].

In the technique of concealment in the spatial field, it is modified by adjusting the value of the least important bit from the image, because the less important bits have no significant impact on the image clarity and are almost non-existent and can be considered as random noise. Methods of concealment based on the use of the least significant bit (LSB) technique differ, some of which replace the least important bit of pixel with the data bit, or some of the increase or decrease the value of this randomly chosen pixel [8].

As for the technique of concealment in the field of transform, it has the advantage of being more powerful against unauthorized attacks, and most of the work is based on taking advantage of the frequency in the DCT field and there are algorithms that use the frequency domain [8],[9].

ii. **Audio Steganography**

Digital audio that has been included in confidential data is known as voice concealment, which the computer uses as the basis for its operating system. The slight tweaking of the duo in an audio system allows confidential information to be included in it. Some of the programs available to conceal the audio that is presently available are a tool that enables the implying of confidential information, which allows concealing data in audio files like AU, WAV, and MP3 [10]. The mission of hiding confidential data in the digital audio files is harder to confront the same mission that is performed in other media formats such as pictures in digital shapes. Different technologies have been introduced to include information in digital sound and have been introduced in the sound environment to culminate in an operating system that conceals confidential data better. These different technologies operate on a spectrum that consists of entering information through the form of signal noise through the use of an uncomplicated algorithm, which reaches robust technologies such as the use of higher technical mechanisms to hide information [11].

iii. Video Steganography

Concealing confidential data in the shape of a video form is called concealing information with a video. Video files contain a set of pictures and sounds. Usually, a large number of recommended technologies can be applied to pictures and sound on video files as well. It is the most appropriate format for a picture file when compared to other multimedia files. This is due to the amount of space within the video format that can accommodate and hide a large amount of

information, which people can discover as a result of the endless flow of data. Different kinds of video files that can be utilized are AVI (Audio Video Interleave) was created by Microsoft long ago, when computers could play video clips when it was great. MP4 is simply a media container that is developed to hold data that is encoded by MPEG4. It does not deal with the actual video, thus it does not affect the quality of the output. MPEG is the video encoding algorithm and that is actually responsible for how images are compressed and converted into data. H.264 codec was developed from the MPEG group and made it a standard in 2003, and it aims to provide a single codec for devices with limited network messaging and limited processing capacity (i.e. mobile phones), and for devices that have large network messaging and excellent processing power (such as modern computers), And anything that falls in between., or other video styles [12][13].

iv. Text Steganography

Concealing confidential data within a text file is described as text Steganography. It has tiny memory size, thus it is only able to be store for text format only. There are many formats used utilizing this technique. The tabs, capital letters and number of white spaces are used to conceal data in Text Steganography. It is rarely used as text files keep a huge amount of excess surplus information [14], [15].

3. Literature Survey

Hassanain Raheem Kareem et al. [16] are suggested to hide the text of the secret file to the image after dividing it into 8 * 8 blocks, so that the image is compressed before hiding the secret data in it to reduce the data sent over the network where it suggested a random key that specifies the location of hiding the confidential information in the picture and then the picture is encrypted with the data Hidden inside it to increase safety, the results of this method were on Lina's picture with a dimension 256x256 where PSNR= 52.0235 and MSE=0.10024.

R. Varalakshmi [17] has proposed a method was based on artificial intelligence as Karhunen-Loeve Transform relies to communicate with the confidential data taken as an entry to include it in an RGB type image, and this encrypted image is decoded using the DES decoding algorithm to retrieve the secret message.

V. Lokeswara Reddy et al. [18] proposed encrypt secret data using DES algorithm after that embedded cipher text into multimedia file (image, audio or video) and sent to target receiver.

G.S.Sravanthi et al. [19] are suggested instead of storing the confidential data in each of the least important bits in the pixel, rather using more than one bit of the pixel bit, this does not affect the change in the appearance of the host / carrier image and this method is a plane bit substitution method, and the confidential data is included after encoding.

Mahesh Kumar and Munesh Yadav [20] have suggested a method for converting the carrier/host image from RGB to gray scale, then convert it to the frequency domain by applying the wave transform technique and dividing it into partial images 2x2. Confidential data, whether text or image, is included by specifying the location of the embedded by using a random generation function. The three least important bits of each pixel are converted to the decimal value and stored into a decimal array 2x2 and every three bits of the confidential message bits, are converted to a decimal value and the value and signe are specified. If the signe is negative, the value is added to one of the pixels of the partial picture and if it is positive it is subtracted the value from the pixel of the partial image.

Monika S. Shirbhate and S.S. Kulkarni [21] the proposed method depends on input the video file and testing whether it is compressed or not if it is not compressed. The frames and the audio file are extracted from it. Then we define the extracted audio file and verify a header, then we select a key to choose the sound file samples, we define the secret data and encode it using a symmetric key, then hide the data Encoded in the 4^{th} LSB bit position for the selected samples so that a stego sound file is produced which is then added to the AVI video and thus produces the AVI video with confidential information.

Dimple Lalwani et al. [22] proposed method depends on hiding the confidential data in the video file, which is a combination of sound and pictures by taking advantage of the forensic technology as a tool of credibility as the chief goal of the method is to conceal the confidential data behind images and sound from the video file and the AES algorithm was used to increase data security and use an algorithm 4LSB to hide.

Shahd Abdul-Rhman Hasso [23] proposed to read any type of video files and isolate the audio file from the frames so that each frame is a three-dimensional matrix RGB, then convert all the content of the frame to a two-dimensional matrix, after which the length of the text is included in a specific frame according to a key and then includes the rest of the text on the basis of another key after completing the inclusion The confidential data is then the image file is stored with the audio file to the video and transmission file.

G. Prashanti and K. Sandhyarani [24] have proposed a method to hide secret message in picture using LSB technique. They worked on improve concealing capacity, powerful and uneasy to detect on concealed data. They used gray image scale to include secrete message and including other image of the same size. They stored secrete message in random positions of the image.

Gulve and Joshi (2015) [25] have suggested a manner based on hiding secret data in grayscale images using spatial field technique, after analyzing it into four partitions bands utilizing "2D Haar Integer Wavelet Transform". When completing the analysis of the image, the spatial domain technique was utilized to conceal the confidential data through the variation of the pixel value where all four sub-bands are used to hide.

Gulve and Joshi (2014) [26] have suggested a manner to enhance the safety of the confidential data utilizing the five-pixels couple variance method. The carrier picture is parceled into lumps of 2 × 3 pixels to configure lumps. The confidential information is concealed in the sets

Journal of University of Babylon for Pure and Applied Sciences, Vol. (28), No. (3): 2020
Online ISSN: 2312-8135, Print ISSN: 1992-0652

utilizing the divergence value of pixels in this couple. Rather than concealing M bits in the couple utilizing the divergence value, bits $\leq N$ are concealed in a couple where N is a moderate of bits that can be concealed in every couple of the lumps. Thus, in statues of fail of the hidden technique, it gets hard to appraise the precise number of bits concealed in every couple of the lumps. Another degree of safety to the confidential data be submitted by changing the confidential data in its gray code structure. To every couple in the lump, and approaches' transforms bits of confidential data in the gray code structure and then includes those bits in this couple.

To enhance a concealing amplitude of the carrier picture and goodness of the stego-picture, other improve approach be submitted dependent on the PVD approach by Ko-Chin Chang et al. [27][28]. In this approach, information be concealed in vertical and diametrical brinks along with the level brinks. A carrier picture parceled into lumps of 2 * 2 pixel lumps. Keeping in mind that x and y to be the pixel positions, each 2 * 2 lump contains four pixels $P1_{(x,y)}$, $P2_{(x+1,y)}$, $P3_{(x,y+1)}$, and $P4_{(x+1,y+1)}$. Pixel $p1_{(x,y)}$, which is combined with the residual three pixels in the lump to compose three-pixel pairs. These three couples are known as $PP0$, $PP1$, and $PP2$ where $PP0$= ($P1_{(x,y)}$, $P2_{(x+1,y)}$), $PP1$= ($P1_{(x,y)}$, $P3_{(x,y+1)}$), and $PP2$=($P1_{(x,y)}$, $P4_{(x+1,y+1)}$), respectively. Using the PVD method, the confidential data is included in each pair, thus the value of two pixels in each pair is adjusted, and thus, the original difference value d_i is adjusted to a new difference value d'_i. The new pixel values in each couple are various from their authentic ones. This means that three different pixel values are obtained for the pixel $P1_{(x,)}$. Nevertheless, pixel $P1_{(x,)}$ can have only one value. Thus, one of the PP'_i is chosen as the reference pair to compensation the residual two pixel values. That is, two pixel values of reference pair are utilized to tune the pixel values of another couple and create a new 2 x 2 lump. The built-in confidential data is not affected because the values of the new differences, d'_i, have not changed. Through retrieval, the divergence value d'_i is utilized to elicitation an unobserved (hidden) data. $|d'_i|$ is utilized for determine an appropriate band R_k. The decimal values for the confidential data concealed in the pair are given by $|d'_i| - l_k$ which then turns into a sequence of binary bits.

Gulve Avinash K. and Joshi M.S. [29] are suggested a technique to increases security of embedding confidential data without affecting the host's image quality. The cover image is parceled into lumps of 2 × 3 pixels to create five pairs. The position of the general pixel is determined utilizing the picture information. As a result, are utilized the data from last few rows. Since the general pixel is alter randomly depends on data of the picture, it is hard to elicitation the confidential information from stego picture even if hidden method failure.

Ramalingam and et al. [30] have clarified the process of detaching four sub-ranges utilizing Haar Integer Wavelet Transform. The first phase Integer Wavelet Transform (IWT) is calculated by

Journal of University of Babylon for Pure and Applied Sciences, Vol. (28), No. (3): 2020
Online ISSN: 2312-8135, Print ISSN: 1992-0652

$$\left.\begin{aligned} H &= C_o - C_e \\ L &= C_e + \left\lfloor \frac{H}{2} \right\rfloor \end{aligned}\right\} \quad (1)$$

Where C_o exemplify pixels in even column and C_e exemplify pixels in even column. In the following stage, the Integer Wavelet Transform (IWT) parameters are computed utilizing low-pass and high-pass filter. This process configures four sub-ranges: high-high (HH), high-low (HL), low-high (LH), and low-low (LL). The second phase Integer Wavelet Transform (IWT) is calculated by

$$LH = L_{odd} - L_{even},$$

$$LL = L_{even} + \left\lfloor \frac{LH}{2} \right\rfloor$$

$$HL = H_{odd} - H_{even} \quad (2)$$

$$HH = H_{even} + \left\lfloor \frac{HL}{2} \right\rfloor$$

Where H_{odd} exemplify H band's odd row, L_{odd} exemplify L band's odd row, H_{even} exemplify H band's even row, and L_{even} exemplify L band's even row.

Kamred Udham Singh [31] has suggested a method based on isolating the frames and the audio file from the video file (AVI). Then the frames, which are RGB type images, are used to hide the confidential information using LSB technique, where storage locations are determined according to the function in the following equation

$$S_i = \int_0^n a.et|\, T(i+1)s - T(if)| \quad (3)$$

Where T(i+1)s represents stating time of next frame, T(if) represents starting time of current frame, t represent starting time of sample, a represents amplitude of sample, S_i represents audio sample between frames and total video is given by

$$V_i = S_i + f \quad (4)$$

As each pixel hides three bits of the secret message, and upon completion of the hiding process, the frames are combined with the audio file to return the Audio Video Interleave file (AVI) and send to the target.

Rajalakshmi K., and K. Mahesh [12] have suggested a flexible φ-correction filtering method (is created as a pre-processing technique to eliminate commotion data on the cover and conceal video by examining the pixel esteem as far as Fast Fourier Transform (FFT) after playing out the pixel streamlining with the assistance of various limit coefficient esteem.) with a Blind

Pixel Algorithm (BPA) to hide confidential information without distortion. Using a value parameter for different parameters, the pixel optimization process is performed, and then the pixel value analysis is made by Fast Fourier Transform (FFT) to remove noise from the cover and the secret video, using a developed method for flexible φ-correction filtering. The confidential message data are included in the cover pixel value using the Blind Pixel Algorithm based on the least significant bit (LSB) technology.

Manisha S., and T. Sree Sharmila [13] have suggested a picture containing confidential information be hidden into the frames of the video file after it has been divided into frames and hidden in the video. The quality of the secret picture and video does not change before and after hiding.

4. Discussion and Recommendations

After reviewing a number of different papers in the field of concealment of information, it was noted that the most used technique to hide confidential information is images, provided that we do not forget that the main goals of concealment are to hide secret information in the cover object so that it is less clear, more secure, and protection from unauthorized arrive with an increase in capacity payload the data. To secure the concealment process more broadly, it is desirable over utilize an effective encryption algorithm.

The masking in the images is either in the grayscale pictures or color images, and the masking technique relies on hiding the confidential data, whether text or image inside the cover image. It is easy to attack data masking techniques in the spatial domain, so it needs to improve security by integrating it with one of the encryption technologies. The technologies that hide data in the frequency domain also have the strength and ability to hide data, but not as in the spatial domain. Concealment may be within one of the video files, and the techniques of concealing information in high-resolution AVI files are better because the distortion rate is very small and invisible and is characterized by its ability to store large amounts of confidential information. Table 1 shows the PSNR values for some of the methods covered in this research.

Journal of University of Babylon for Pure and Applied Sciences, Vol. (28), No. (3): 2020
Online ISSN: 2312-8135, Print ISSN: 1992-0652

Table 1 shows for some suggested methods

Carrier Type	Capacity	PSNR	Ref.
Color Image	256x256 pixels	52.0235	Method 1. [16]
Video File(AVI)/Frame	240x320 pixels	68.8595	Method 2. [23]
Gray Image	81236	39.84	Method 3. [25]
Gray Image	81305	42.86	Method 4. [26]
Gray Image	75836	38.89	Method 5.[32]
Gray Image	76346	42.87	Method 6.[29]

5. Conclusion

In this paper, presented a review on the technique of hiding confidential information inside an image file and a video file to provide appropriate protection for the data during its transmission on public channels such as the Internet. It was noted that video files are best suited for storing large amounts of confidential data and thus produce stego -video with few distortions which leads to more durability, better security and a high ability to include data (large capacity).

Conflict of interests.

There are non-conflicts of interest.

References

[1] Beant Singh, Kul Bhusan Agnihotri (2015)," A Method to Hide Secret Information: Steganography" International Journal of Recent Advances in Engineering & Technology (IJRAET) 2347 - 2812, Volume-3, Issue -10, 2015.

[2] Mohammed Sabri Abuali, C.B.M. Rashidi, Muataz H. Salih, R. A. A. Raof, and Safa Saad Hussein (2019) "Digital Image Steganography in Spatial Domain a Comprehensive Review" Journal of Theoretical and Applied Information Technology 15th October 2019. Vol.97. No 19.

[3] Mahdi, Mohammed Hashim, et al."Improvement of Image SteganographyScheme Based on LSB Value with TwoControl Random Parameters and Multi-levelEncryption." IOP Conference Series:Materials Science and Engineering. Vol. 518. No. 5. IOP Publishing, 2019.

[4] Zlii Li,Yang S. A. F. , Xian Y (2003)," A LSB Steganography Detection Algorithm", The 14th IEEE 2003 International Symposium on Persona1,lndoor and Mobile Radio Communication Proceedings.pp.2780-2783.

[5] Yadav, Gyan Singh, and Aparajita Ojha. "Improved security in the genetic algorithmbased image steganography scheme using Hilbert space-filling curve." The Imaging Science Journal (2019): 1-11.

[6] Kim S. M, Cheng Z and Yoo K.Y (2009) , "A New Steganography Scheme based on an Index color Image", 2009 Sixth International Conference on Information Technology: New Generations, pp.376-381.
[7] Pooyan M, Delforouzi A (2007), "LSB-based Audio Steganography Method Based on Lifting Wavelet Transform", 2007 IEEE International Symposium on Signal Processing and information technology, pp.600-603.
[8] Pooyan M, Delforouzi A (2007), "LSB-based Audio Steganography Method Based on Lifting Wavelet Transform", 2007 IEEE International Symposium on Signal Processing and information technology, pp.600-603.
[9] Shahreza M. S and Shahreza M. H. S (2007), "Text Steganography in SMS", International Conference on Convergence Information Technology, pp.2260-2265.
[10] Han, Chunling, et al. "A new audio steganalysis method based on linear prediction." Multimedia Tools and Applications (2018): pp. 1-25.
[11] Nasrullah, Mohammed A. "LSB based audio steganography preserving minimum sample SNR." International Journal of Electronic Security and Digital Forensics 10.3 (2018): 311-321.
[12] Rajalakshmi, K., and K. Mahesh. "Robust secure video steganography using reversible patch-wise code-based embedding." Multimedia Tools and Applications 77.20 (2018): 27427-27445.
[13] Manisha, S., and T. Sree Sharmila. "A two level secure data hiding algorithm for video steganography." Multidimensional Systems and Signal Processing (2018):pp. 1-14.
[14] Din, Roshidi, et al. "Evaluating the Feature- Based Technique of Text Steganography Based on Capacity and Time Processing Parameters." Advanced Science Letters 24.10 (2018): 7355-7359.
[15] Ciptaningtyas, Henning Titi, Radityo Anggoro, and Muhsin Bayu Aji Fadhillah. "Text Steganography on Sundanese Script using Improved Line Shift Coding." 2018 International Electronics Symposium on Knowledge Creation and Intelligent Computing (IES-KCIC). IEEE, 2018.
[16] Hassanain Raheem Kareem, Hadi Hussein Madhi and Keyan Abdul-Aziz Mutlaq " Hiding encrypted text in image steganography" Periodicals of Engineering and Natural Sciences, Vol. 8, No. 2, June 2020, pp.703-707.
[17] R. Varalakshmi "Digital Steganography For Preventing Cybercrime Using Artificial Intelligence Technology" Journal of Critical Reviews, Vol 7, Issue 6, 2020.
[18] V. Lokeswara Reddy, A.Subramanyam and P. Chenna Reddy" A Novel Approach for Hiding Encrypted Data in Image, Audio and Video using Steganography" International Journal of Computer Applications, Volume 69– No.15, May 2013.
[19] G.S.Sravanthi, B.Sunitha Devi, S.M.Riyazoddin and M.Janga Reddy "A Spatial Domain Image Steganography Technique Based on Plane Bit Substitution Method", Global Journal of Computer Science and Technology Graphics & Vision, Volume 12 Issue 15 Version 1.0 Year 2012.

[20] Mahesh Kumar and Munesh Yadav" Image Steganography Using Frequency Domain", International Journal Of Scientific & Technology Research Volume 3, Issue 9, September 2014.
[21] Monika S. Shirbhate and S.S. Kulkarni "Hiding and Extracting Secrete Data in VideoFile with Noise Compression" International Journal Of Computer Science And Applications , Vol. 6, No.2, Apr 2013.
[22] Dimple Lalwani, Manasi Sawant, Mitali Rane, Vandana Jogdande and S.B.Ware" Secure Data Hiding in Audio-Video Steganalysis by Anti-Forensic Technique" International Journal Of Engineering And Computer Science ,Volume -5 Issue - 3 March, 2016 Page No. 15996-16000.
[23] Shahd Abdul-Rhman Hasso "Steganography in Video Files" IJCSI International Journal of Computer Science Issues, Volume 13, Issue 1, January 2016.
[24] Prashanti G, Sandhyarani K. "A New Approach for Data Hiding with LSB Steganography", In: Satapathy S., Govardhan A., Raju K., Mandal J. (eds) Emerging ICT for Bridging the Future - Proceedings of the 49th Annual Convention of the Computer Society of India CSI Volume 2. Advances in Intelligent Systems and Computing; 2015; 338. Springer.
[25] A. K. Gulve and M. S. Joshi " An Image Steganography Method Hiding Secret Data into Coefficients of Integer Wavelet Transform Using Pixel Value Differencing Approach", Hindawi Publishing Corporation Mathematical Problems in Engineering ,Volume 2015, Article ID 684824, 11 pages.
[25] A. K. Gulve and M. S. Joshi, "An image steganography algorithm with five pixel pair differencing and gray code conversion," International Journal of Image, Graphics and Signal Processing, vol. 6, no. 3, pp. 12–20, 2014.
[27] K. C. Chang, P. S. Huang, T. M. Tu, and C. P. Chang, "Image steganographic scheme using tri-way pixel-value differencing and adaptive rules," in Proceedings of the IEEE International Conference on Intelligent Information Hiding and Multimedia Signal Processing, pp. 449–452, Kaohsiung, Taiwan, 2007.
[28] K.-C. Chang, C.-P. Chang, P. S. Huang, and T.-M. Tu, "A novel image steganographic method using tri-way pixel-value differencing," Journal of Multimedia, vol. 3, no. 2, pp. 37–44, 2008.
[29] A. K. Gulve and M. S. Joshi, "A secured image steganography algorithm with five pixel pair differencing by selecting the common pixel randomly," in Proceedings of the 3rd International Conference on Computational Intelligence and Information Technology (CIIT '13), pp. 55–61, Elseveir, Mumbai, India, 2013.
[30] B. Ramalingam, R. Amirtharajan, and J. B. B. Rayappan, "Stego on FPGA: an IWT approach," The Scientific World Journal, vol. 2014, Article ID192512, 9 pages, 2014.
[31] Kamred Udham Singh "Video Steganography: Text Hiding in Video by LSB Substitution", Int. Journal of Engineering Research and Applications, Vol. 4, Issue 5(Version 1), May 2014, pp.105-108.
[32] K.-C. Chang, P. S. Huang, T.-M. Tu, and C.-P. Chang, "Adaptive image steganographic scheme based on tri-way pixel-value differencing," in Proceedings of the IEEE International Conference on Systems, Man, and Cybernetics (SMC '07), pp. 1165–1170, Montreal, Canada, October 2007.

Journal of University of Babylon for Pure and Applied Sciences, Vol. (28), No. (3): 2020
Online ISSN: 2312-8135, Print ISSN: 1992-0652

الخلاصة

مع التطور الكبير في تقنيات المعلومات الإلكترونية والشبكات ، وفي ضوء بعض الظروف التي تفرض العمل على الإنترنت ، والتي تعتبر بيئة غير آمنة للمعلومات السرية ، أصبح الحفاظ على أمن البيانات ذات أولوية مهمة. من أهم التقنيات المستخدمة للحفاظ على سرية البيانات المنقولة وعدم إخضاعها للمهاجمين هي الإخفاء والتشفير ، وتعتمد هاتان التقنيتان أيضًا على الوسيط الذي ينقل البيانات السرية ، سواء كان ملف صورة أو صوت أو فيديو. علم إخفاء المعلومات هو علم دمج البيانات الرقمية بطريقة لا يمكن لأحد الشك في وجودها. التشفير هو تقنية أخرى تستخدم لحماية البيانات ، عند استخدامه مع إخفاء المعلومات يزيد من قوة حماية المعلومات. تقدم هذه الورقة لمحة عامة عن تقنيات إخفاء المعلومات النصية داخل ملفات الصور والفيديو. تهدف هذه الدراسة إلى تقديم ملخص للطريقة الأكثر أمانًا وأمانًا وقدرة حمولتها على إخفاء البيانات.

الكلمات الدالة: إخفاء المعلومات في الصور، إخفاء المعلومات في الفيديو، انواع الاخفاء.