Kerbala Journal of Computing and Technology 2025

Text Steganography in Videos Using Ascii Code Values

Ahmed Mahmoud Hassan[a], Hassan Abdulhadi Fadel[a] ,Mohammed Muntazir Rushdi Belibas[a], Mohammed Jassim Abdul Sada[a] ,

Estqlal Hammad Dhahi[b], Ashwan A. Abdulmunem[a], Zahraa A. Harjan[a]

[a]*Department of Computer Science, College of Computer Science and information Technology, University of Kerbala, Kerbala, Iraq*

[b]*Information Technolog y Centre, University of Kerbala,Kerbala,Iraq*

Received: 17 / 03 /2025
Accepted: 14 / 05 /2025
Published: 30 / 06 / 2025

Keywords:

Steganography, Text steganography, SHA512-ECC , CM-CSA

ABSTRACT

Text steganography is a technique used in digital video files to conceal text. Sensitive information, such passwords or messages from outside parties, has long been hidden using this method. Depending on the user's intention, text steganography can be used for both good and bad things. The procedure is adding brief textual captions to each frames in a video file without appreciably altering the film's overall size or look. Next, an algorithm is used to encrypt the embedded data, making it difficult for unauthorized users to access and perhaps intercept the transmission. This technique makes it possible to send encrypted messages securely via networks without being discovered by outsiders trying to obtain private data that is hidden in videos that they are not allowed to watch. Through digital media platforms like YouTube or Video, text steganography offers businesses and individuals alike an efficient method to safeguard their data while still securely sharing it with others. Because only people with the ability to decode secret texts will be able to access them once they are embedded into a video file format, it also gives them more control over the kind of content they publish online. In this paper a new approach for hiding ASCII code values in videos has been tested and evaluated which presents an acceptable result in this field.

1. Introduction

Nowadays, protecting data from an unauthorized user is the primary task of transmitting information over a communications network. To deal with this issue there are various mechanisms such as Steganography, Cryptography, Digital Watermarking, etc. The first two methods provide protection on the data, while the third method provides authentication of the data by using some tags or marking some objects such as text, audio, video, and image. Steganography is a powerful technology used in information security. Encryption was initially developed and used as a method of securing the confidentiality of information. But keeping the message's contents confidential is sometimes not enough. It may also be necessary to keep the message's existence secret and the concept responsible for this is Steganography. The word Steganography has a Greek origin and means hidden writing from the Greek words stegao meaning covered or protected, and graph in meaning writing. Hiding information is a way to hide confidential messages within any media. Which are categorized into hiding pictures, text, audio and video, and which are based on the cover media used to embed a confidential message. Most data masking systems take advantage of human perceptual weaknesses. The science of steganography is often confused with encryption because the two are

∗Corresponding Author: Hassan, Ahmed

Email addresses: m05141150@s.uokerbala.edu.iq

similar in the way they are used to protect confidential information. If both methods are used: encryption and concealment of information, the connection becomes double secure. The main difference between Steganography and cryptography is that cryptography focuses on preserving the confidentiality of the message contents while cryptography focuses on preserving the confidentiality of the message's existence. There are many works in steganography which applied on visual data. In this work we proposed a method based on ascii code to hide information "text" in video frames following sections will explain it in details.

2. Related Works

To get and hide the information in the video, a combination of cryptography and steganography using SHA512-ECC and CM-CSA was presented. Initially, ordinary text is used as an input, and it is subjected to IHE pressure and DNA encoding. The results showed that the suggested CM-CSA algorithm is superior than the SHA512-ECC technique for cover media steganography[1].

Steganography it's provided techniques by using the Zero Distortion Technique it's depending on the location of the bit is applied on gray as well as color image, in the color image can hide more data comparing with gray because color image contains RGB bands[2]. Another technology of steganography using (ACA) ant colony algorithm and LSB, this algorithm has shown to be exceptionally effective in producing the secret key by arriving at feeble pixels haphazardly [3].

It analyzes the LSB (least significant bit) to other popular methods. Generalized Gaussian Distribution (GGD) to identify the presence of hiding information in LSB. In color images, we compared the features of LSB to those of other HCFCOM and HOMMS, and in grayscale images, we compared the features of LSB to those of HCFHOM, HOMMS, A. HCFCOM, and C.A. HCFCOM[4].by utilizing the Least Significant Bit (LSB) procedure an Adaptive Random Inverted Pattern (ARIP) approach has endeavored to additional upgrade the nature of the stego-image. comparing the MSE and PSNR values of the image ensures the (PSNR) Peak Signal to Noise Ratio increasing for the ARIP technique yields 1 dB improvement [5]

Based on the Chinese remainder theorem (CRT) it suggests a new schema called (SIS) Secret image sharing to use steganography and it relies upon the number of pixels in the image. The schema can accomplish both the high PSNRs of the stego image. SIS extended to RESIS and the outcome proved the RESIS better than SIS, the outcome proves the schema is better existing methods [6]. While utilizing threshold PRASIS schema-based SIS under G F (28) into the AMBTC cover picture. the result its be good effectiveness and high accuracy [7]

A new text steganography method was proposed as an approach. The method involves mixing the ASCII value of a character with the RGB values of a pixel to store an individual character in a single pixel. The fundamental goal of this method is to give the highest possible payload capacity for an image, which is the total amount of pixels it includes [8]. This method was based on two basic concepts: (1) recognizing highly dynamic regions in video scenes and using them to hide data, and (2) finding the appropriate quantity of data to embed in the selected regions. The dynamics of the scenes were studied using motion hints from feature points, and then the regions of interest were chosen accordingly. The average embedding capacity and perceptual invisibility rate values obtained in the experiments are 0.52 bpp and 50.66 dB, respectively [9].

Proposed a new video data hiding approach that takes advantage of the capacity of repeat accumulate codes to remedy errors as well as the superiority of forbidden zone data hiding (FZDH). FZDH was used to ensure that no changes are made to the data while it is being hidden [10]. On text, image, audio, and video as a media, they covered the numerous forms and approaches of steganography [11][12]. They were discussing Some of the techniques of text steganography has been discussed along with characteristics and working.

A research work presented that looked at three approaches based on least significant bit (LSB) algorithms. They provided a new method for LSB-based image steganography. Reduce the length of the secret message using the Deflate method, which combines the LZ77 and Huffman algorithms to provide a lossless data compression algorithm. The AES (Advanced Encryption Standard) algorithm was used to safeguard the decreased hidden data [13].

Another work proposed steganography technique based on Optical Character Recognition (OCR), where in the cover of the image the message was embedded. There from images character level features extracted which contain the

textual message, and in the cover, image embed these features. the results was validated on an English Printed Character dataset (Chars74K Dataset) [14]. In the edge of the frames of the AVI video, the secret message (English text) was hidden, without changing the details of frames. In the frames 38,39,40,41 and 42 the secret message was embedded because these frames have sufficient edge point details the reason of selecting those frames. the secret message has been represented with a message comprised of 300 characters, and the cover frame image is represented by a 120 frames size 120* 160.The results obtained the Peak Signal to Noise Ratio (PSNR) value ranges from 74.5293dB to 75.9123 dB [15].

The method used was ASCII coding to hiding the secret message, if someone understands its applicability the CASE method has a security issue that, so it is easy to attack. To overcome its limitations the DSTS algorithm is applied by using UTF-16 coding and the security of CASE is enhances with a one-time pad (OTP) which is a theoretically unbreakable cryptographic method. The average hiding capacity was degrades in a PHM from 2.06% to 1% due to UTF-16 coding. The MDSTS and the CMPHM is improved by 6.49% and 7.76% hiding capacity [16].

There were those who suggested relying on the use GA to protect stego text from suspicion due to the efficiency and effectiveness used in other media. To avoid third parties detecting the existence of secret message therefore Suspiciousness against stego text is very important in steganography [17].

Text-based steganography methods could be employed in Web page texts as well as plain text. The ability to broadcast messages (e.g., HTML codes and Hashtags on social media) was the same whether hidden information is there or not. The secret message was hidden in the content or the code of a Web page by using its properties. To improve the security of Persian messages sent across networks, certain text steganography methods were proposed [18].

To improve the capacity of hidden data in social media communications. An approach was devised in which any simple piece of text, such as a news item, a letter, or common messages, was used as the cover text. Extended Line will be used to enhance the capacity of a text, followed by White Space between lines [19].

By taking into account good visual quality, some had suggested a way to improve the LSB technique's capacity. Rather of replacing LSB with secret data, the secret data was used for embedding. First, the minimum and maximum values in the secret data are calculated, and then all values in the secret data are subtracted from this maximum value. Finally, after creating a division for the results, insert the new results into the cover image to obtain the stego image. When compared to earlier approaches, the end outcome was good but unnoticeable [20].

There were those who used a technique to hide secret data in the media cover. In order to get an optimum position to hide the data the GA is Applied to the audio samples of cover file encoded the secret data into its ASCII, finally to secret data LSB is used to embed the ASCII codes [21]. A number of researchers presented an overview of the existing techniques for hiding text and its classifications, and a comparison between these techniques, looking at the use of text document in organizations on a large scale, using text document as a cover medium might be a best choice in such environment [22].

To hide secret messages in a video, use Discrete Wavelet Transform (DWT) and Advanced Encryption Standard (AES). AES used to be message encrypted more secure. From the experiments the value ranges from 39 to 40 dB of PSNR value and close to 1 of SSIM value, which means does not cause large noise due to insertion [23]. There are a number of researchers who have presented a comprehensive study of the methods of modern text steganography and their classification. Among the researchers, the methods of hiding text are divided into three categories: linguistics methods, random and statistical generation, and format-based [24].

When the hiding uses encryption and steganography techniques to provide greater protection for data sent over insecure channels. The encryption method based on the genetic algorithm gave good results, which increased the strength of the encryption, as unauthorized people could not know the key without knowing the random seeds that generated using this algorithm. The embedding of even and single-layer frames also makes the video look natural and uninterrupted. The experimental results of this method showed that the inclusion was of high quality and the metric

values were close to the ideal value. This indicates that this method fulfills the lack of feeling of the inclusion in the video. In the end, the results provide a high capacity, which the result PSNR is 63 [25].

3. Proposed Method

Because video streams have a significant degree of spatial and temporal redundancy in representation and have extensive uses in daily life, they are thought to be suitable candidates for hiding data. Video steganography can then be used in a variety of practical applications. One use is for military and intelligence services to employ video steganography in their communications. Another use is to employ video steganography to send supplementary data, such as subtitles.In general, video steganography is an extension of visual steganography. A video file can be seen as a series of photos, resulting in video data hiding that is comparable to image data hiding.

However, there are several distinctions between video steganography and picture steganography. Because video material is dynamic, the odds of detecting concealed data are smaller than with photos. In addition to picture attacks that may be applied to individual frames of video, there are many additional video assaults such as lossy compression, altering the frame rate, switching between formats, and adding or deleting frames during video processing. Furthermore, the concealing capacity of video is substantially larger. Videos add new aspects to data concealment, such as hiding messages in motion components.

The proposed approach uses the RGB values to embed a single character. At the beginning it takes the first character of the message and divides its ASCII value into three segments, for instance if the character is “A” then its ASCII value would be “65” and after dividing the value into three segments the three numbers would be “0”,”6”, and “5” The three values then embedded in the RGB values of each pixel. Then combine these three numbers into a single pixel using its three channels (Red, Green and blue). Fig. 1. explains the method.

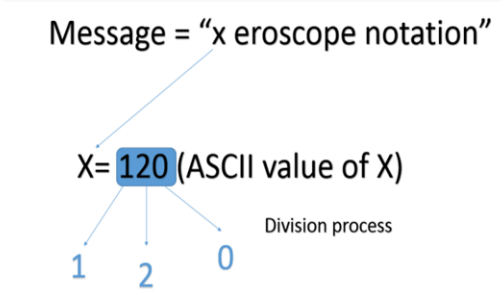

Fig. 1- Steganography Based on ASCII Code

Algorithm for the embedding process:

- Read the message to be embedded.
- Decode the characters to their corresponding ASCII values.
- Loop through the video frames.
- For each frame do the following:
    - Loop through the frame.
    - Apply division on the ASCII value to get the three numbers.
    - Embed the three values in the pixel.
    - Repeat until the end of the frame.
- Add end point.

Algorithm for the extracting process:

- Read the video.
- Loop through the video frames.
- For each frame do the following:
    - Loop through the frame.
    - Get the values of Red, Green and Blue from each pixel.
    - Extract the last digits from Red, Green and blue.
    - Combine the values to obtain the ASCII value.
    - Repeat until the end of message point reached.

The approach yields very good results, since in the worst-case scenario the difference in intensity would be only 9 points and that is entirely unnoticeable by the naked eye, however, an important point should be mentioned is that there is an exceptional case in this approach which can occur when the resulting channel value exceeds 255 (which is the highest value for any given channel in the pixel), for instance if the data to be embedded is 119 (which corresponds to the letter 'w') and the original pixel value is:

R = 19, G = 19, B = 251

And after embedding we get the following values:

R = 11, G = 11, B = 259

Notice that the Blue channel value has exceeded the one-byte value limit. We worked around this exceptional issue by skipping the problematic pixel, we established that by embedding a non-printable control character such as the SOH character (Decimal 1) provided that the same would be done when extracting.

4. Results and Discussions

The suggested method was tested on multiple videos with various sizes and various messages. The messages sizes varied from small messages to extremely huge (e.g. more than 5 million characters) and contained all printable ASCII characters. Steganography efficiency was tested with PSNR (peek signal to noise ratio) which is a common measure to test similarity between frames. In the experiments we used three MP4 videos and two large messages one is the whole works of Shakespeare with more than 5 million characters and the other is the very famous novel by Leo Tolstoy "War and peace" with more than 3 million characters. Table 1 shows the videos that have been used in the experiments.

Table 1 - Test Cases Video Information

Test Cases	Frame Rate	First Frame from Videos
Video #1	29	
Video #2	23	
Video #3	23	

5. Experimental Results

The following table explains the characteristics of the video that used to hide the text. Table 3 depicts the PSNR for video #1. While table 4 show the information of the video after stegonagraphy process.

Table 2- Video Information

Size	Number of Frames Needed	Average PSNR
461 MB	25	35.3122

Table 3- PSNR for Test Video 1

Frame NO.	PSNR value
1	35.1014
2	35.1213
3	35.1168
4	35.1188
5	35.1276
6	35.1132
7	35.1120
8	35.1106
9	35.1095

10	35.1095
11	35.0992
12	35.1258

Table 4-Video Information After Steganography Process

Width	Height	Frame rate	Duration	Original size	Payload length
640	360	29	23 S	1.7 MB	5,583,449 characters

Table 5- Methods Comparisons

Technique	Methods	Embedding techniques	Advantages	Drawbacks
Temporal Domain	Low bit encoding (least significant bit)	LSB of each audio sample is replaced with data sample	Easy and simple data hiding in target signal	Easy to extract and to destroy
	Echo hiding	Cover data by introducing echo signal in target signal	Resilient to lossy data compression algorithms	Low Capacity and security
Transform Domain	Phase spectrum	Modulate the phase of the cover signal	Robust against signal processing manipulation and data retrieval needs the original	Low capacity
	Magnitude spectrum	Use frequency bands to hide data	Longer message to hide and less likely to be affected by errors during transmission	Low robustness to simple audio manipulations

6. Conclusion

The steganography approach was implemented in this project was originally proposed for images. In this project an extension to the original approach was proposed and implemented to include video files. Testing data showed

excellent results when it comes to payload size and PSNR, with payload size exceeded 5 million characters and average PSNR of (34.942) which is quite decent and unnoticeable by the human eye. However, the only downside for this approach that we could notice was the resulting video size which can be mitigated by using lossless compression.

References

[1] A. Jose and K. Subramaniam, "DNA based SHA512-ECC cryptography and CM-CSA based steganography for data security," Mater. Today Proc., no. xxxx, 2020, doi: 10.1016/j.matpr.2020.09.790.

[2] Shivani, V. K. Yadav, and S. Batham, "A Novel Approach of Bulk Data Hiding using Text Steganography," Procedia Comput. Sci., vol. 57, pp. 1401–1410, 2015, doi: 10.1016/j.procs.2015.07.457.

[3] A. I. Al-Hussein, M. S. Alfaras, and T. A. Kadhim, "Text hiding in an image using least significant bit and ant colony optimization," Mater. Today Proc., no. xxxx, 2021, doi: 10.1016/j.matpr.2021.06.413.

[4] Q. Liu, A. H. Sung, B. Ribeiro, M. Wei, Z. Chen, and J. Xu, "Image complexity and feature mining for steganalysis of least significant bit matching steganography," Inf. Sci. (Ny)., vol. 178, no. 1, pp. 21–36, 2008, doi: 10.1016/j.ins.2007.08.007.

[5] R. Amirtharajan and J. B. Balaguru Rayappan, "An intelligent chaotic embedding approach to enhance stego-image quality," Inf. Sci. (Ny)., vol. 193, pp. 115–124, Jun. 2012, doi: 10.1016/j.ins.2012.01.010.

[6] K. Meng, F. Miao, Y. Xiong, and C. C. Chang, "A reversible extended secret image sharing scheme based on Chinese remainder theorem," Signal Process. Image Commun., vol. 95, Jul. 2021, doi: 10.1016/j.image.2021.116221.

[7] X. Wu and C. N. Yang, "Partial reversible AMBTC-based secret image sharing with steganography," Digit. Signal Process. A Rev. J., vol. 93, pp. 22–33, 2019, doi: 10.1016/j.dsp.2019.06.016.

[8] K. Joshi, "A New Approach of Text Steganography Using ASCII Values." [Online]. Available: www.ijert.org , doi: 10.17577/IJERTV7IS050273.

[9] M. Hashemzadeh, "Hiding information in videos using motion clues of feature points," Comput. Electr. Eng., vol. 68, pp. 14–25, May 2018, doi: 10.1016/j.compeleceng.2018.03.046.

[10] K. Deshpande and N. Kamble, International Journal of Computer Science and Mobile Computing "Application of Data Hiding in Audio-Video Using Advance Algorithm," 2016. [Online]. Available: www.ijcsmc.com , doi: 10.47760/ijcsmc.

[11] A. Febryan, T. W. Purboyo, and R. E. Saputra, "Steganography Methods on Text, Audio, Image and Video: A Survey," 2017. [Online]. Available: http://www.ripublication.com , doi:10.37622/000000.

[12] S. Sharma, A. Gupta, M. C. Trivedi, and V. K. Yadav, "Analysis of different text steganography techniques: A survey," in Proceedings - 2016 2nd International Conference on Computational Intelligence and Communication Technology, CICT 2016, Aug. 2016, pp. 130–133, doi: 10.1109/CICT.2016.34.

[13] S. L. Chikouche, and N.Chikouche. "An improved approach for lsb-based image steganography using AES algorithm." 2017 5th International Conference on Electrical Engineering-Boumerdes (ICEE-B). IEEE, 2017, doi: 10.1109/ICEE-B.2017.8192077.

[14] A. Chatterjee, S. K. Ghosal, and R. Sarkar, "LSB based steganography with OCR: an intelligent amalgamation," Multimed. Tools Appl., vol. 79, no. 17–18, pp. 11747–11765, May 2020, doi: 10.1007/s11042-019-08472-6.

[15] A. M. Aaref, "Video Steganography Using LSB Substitution and Sobel Edge Detection," Diyala J. Eng. Sci., vol. 11, no. 2, pp. 67–73, 2018, doi: 10.26367/DJES/VOL.11/NO.2/9.

[16] Y. Khan, A. Algarni, A. Fayomi, and A. M. Almarashi, "Disbursal of Text Steganography in the Space of Double-Secure Algorithm," Math. Probl. Eng., vol. 2021, 2021, doi: 10.1155/2021/7336474.

[17] B. Osman, A. Yasin, and M. Nizam Omar, "An Analysis of Alphabet-based Techniques in Text Steganography."

[18] S. R. Yaghobi and H. Sajedi, "Text steganography in webometrics," Int. J. Inf. Technol., vol. 13, no. 2, pp. 621–635, Apr. 2021, doi: 10.1007/s41870-020-00572-z.

[19] H. J. Shiu, B. S. Lin, B. S. Lin, P. Y. Huang, C. H. Huang, and C. L. Lei, "Data hiding on social media communications using text steganography," in Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics), 2018, vol. 10694 LNCS, pp. 217–224, doi: 10.1007/978-3-319-76687-4_15.

[20] D. Nashat and L. Mamdouh, "An efficient steganographic technique for hiding data," J. Egypt. Math. Soc., vol. 27, no. 1, Dec. 2019, doi: 10.1186/s42787-019-0061-6.

[21] A. Mishra , P.Johri , A . Mishra. "Audio steganography using ASCII code and GA." 2017 International Conference on Infocom Technologies and Unmanned Systems (Trends and Future Directions) (ICTUS). IEEE, 2017,doi :10.1109/ICTUS.2017.8286088.

[22] R.Bala Krishnan1, Prasanth Kumar Thandra , M.Sai Baba "An overview of text steganography." 2017 Fourth International Conference on Signal Processing, Communication and Networking (ICSCN). IEEE, 2017,doi :109/ICSCN.2017.8085643 .

[23] M. Mulya, O. Arsalan, L. Alhaura, R. Wijaya, S. Ramadhan, and C. Yeremia, "Text Steganography on Digital Video Using Discrete Wavelet Transform and Cryptographic Advanced Encryption Standard Algorithm" Advances in Intelligent Systems Research, volume 172, Sriwijaya International Conference on Information Technology and Its Applications (SICONIAN 2019), doi :10.2991/aisr.k.200424.021.

[24] M. A. Majeed, R. Sulaiman, Z. Shukur, and M. K. Hasan, "A review on text steganography techniques," Mathematics, vol. 9, no. 21. MDPI, Nov. 01, 2021, doi: 10.3390/math9212829.

[25] Z. Jasim, M. J. Altalqani, and Z. J. Jaber, "Improving The Security Of Steganography In Video Using Genetic Algorithm Arabic Plagiarism detection system View project Improving The Security Of Steganography In Video Using Genetic Algorithm," 2021. [Online]. Available: https://www.researchgate.net/publication/357889185,doi : 10.17762/turcomat.v12i10.5265.