

Video Steganography for Image and Text Using Deep Genetic Algorithm and LSB

Nouran Mohamed Selim¹, Shawkat Kamal Guirguis², and Yasser Fouad Hassan^{1,3}

(Corresponding author: Nouran Mohamed Selim)

Computer Science Department, Faculty of Science, Alexandria University¹

Alexandria, Egypt

Email: nouran.selim@alexu.edu.eg

Information Technology Department, Institute of Graduate Studies and Research, Alexandria University²

Faculty of computer science and AI, Pharos University³

(Received Jan. 30, 2021; Revised and Accepted July 5, 2021; First Online Dec. 18, 2021)

Abstract

Data security is a threat for delivering data through the internet, and it is concerned with protecting sensitive data from unauthorized access. The security threats increase with the increase of sensitive data, so security issues should be considered because hackers may use vulnerabilities over public networks to steal the information. Video steganography is considered an efficient technique and becomes an important research area for data security. This paper aims to embed images and text into a video. The proposed algorithm selects the best frames and pixels for embedding images and the best video tags to hide text. As a result, the video's size and visual quality are not altered even after embedding secret data.

Keywords: Encryption; Flash Video; Genetic Algorithm; LSB Technique; Steganography

1 Introduction

Steganography comes from the Greek words which divide into two parts, the first part is "steganos" means covered or concealed and the second part is "graphtos" means writing. Steganography is defined as hiding the existence of messages in a particular medium "cover-medium" such as audio, video, image, text communication [13]. Steganography is the art and science of secret communication which conceals the very existence of communication [16]. It is defined as the process of embedding a secret data (message, image or audio) to be hidden in a cover-medium to reproduce stego-medium that no one apart from the sender and receiver even realizes that there is a hidden message.

The basic steganography algorithm of embedding is shown in Figure 1, Steganography hides the data and the fact of communication. It ensures the anonymity of the communication parties. The amount of information trans-

mitted is greater than the secret encrypted information. It needs an additional carrier. A good steganography algorithm should be measured by embedded data as much as possible (embedding capacity), and the perceptual distortion of the cover medium after the embedding process should be minimum as possible (invisibility) [3]. Steganography is the procedure of covertly without changing its quality it inserts information inside a data source. In the major section, while concealing the information, Original data is not retained in its unique format. Steganography depends on hiding an undercover message in unsuspected different media information and is by and largely used as a part of secret correspondence between recognized gatherings [1]. In contrast to cryptography, which is the art of protecting secret data by transforming it into an unreadable format, it does not hide the data or hide the fact of communication so no need to any additional carrier. Cryptography has become a basic requirement of public electronic connectivity to secure data during transmission against the possibility of message eavesdropping and electronic fraud [7].

This paper will focus on developing one system that uses both Cryptography and Steganography for more confidentiality and security [18]. Advanced Encryption Standard (AES) algorithm is a very secure technique for cryptography, which is characterized by its flexibility and simplicity. The amount of information transmitted in the communication process depends on the amount of the encrypted information. Both transform information into a form that is incomprehensible to a third party, use the secret key to encrypt or decrypt data that becomes more secure. It is used when communicating over an untrusted medium such as the internet, where information needs to be protected from other third parties. We can apply steganography on text, image, audio or video. In this paper, we hide secret data inside the video file. We select video as cover-medium for reasons like larger spaces of the video in hiding or embedding data and can be embedded

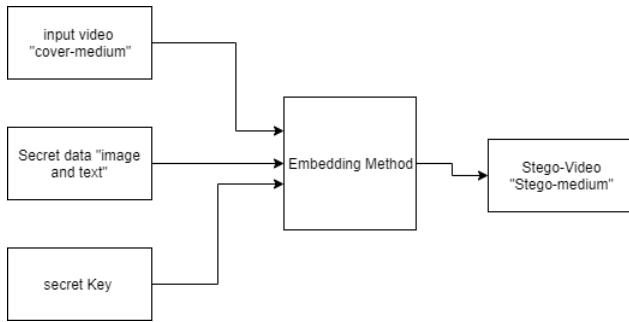


Figure 1: The basic steganography embedded algorithm

data in video/audio tags. Videos are considered as collections of images and sound files which make some of the effective methods of steganography on images and audio files also possible for applying in video files.

Larger space for embedding and having small unnoticeable distortions make video steganography a reliable method in hiding data [12]. Also, we select Flash video format (FLV) because it has smaller file size compared to all the other formats. FLV is very simple. It starts with the headers then metadata tag (data that describes the FLV), then interleaved audio and video tags (actual data). This paper will use two methods to embed image and text in cover video. One of these methods is the least significant bit (LSB) in the pixel/video tags value of the video. It works by replacing the least significant bit of some randomly selected pixels or tags in the cover image with value of new secret data. Another method is embedded secret data with Genetic Algorithm (GA) by calculating the highest fitness function which depends on the lowest difference between pixel of cover image and secret data. Artificial Intelligence (AI) including machine learning, Genetic Algorithm, heuristic optimization is one sub branch of computer science, which can be used to steganography technology and can achieve high visual quality, robustness, low cost, optimal and adaptive solutions. Recently, AI technology is rarely used in video steganography, though applied to various kinds of image steganography, including Genetic Algorithms. Due to the generality of image steganography and pre-embedding video steganography, the AI technology applied to image steganography has great reference value for pre-embedding video steganography [20].

The Rest of the paper is organized as follows: Section 2 discusses related work of steganography. Section 3 presents the proposed work. Section 4 gives results of the work and Section 5 concludes the papers.

2 Related Works

Sahu and Mitra [17] described an algorithm to hide the message in the frames of the video. The algorithm suggested selecting a random video frames then using a pixel swapping algorithm for blue channel of the frames. The secret message is encrypted using AES technique then

embedded it into video frames with Least Significant Bit (LSB) technique. Authors conclude that using only LSB technique for data hiding is not a secure method therefore, they was used the random frames selection algorithm and pixel swapping algorithm to improve the security of the method.

Eltahir *et al.* [5] described an algorithm to hide secret data in video by splitting the digital video file into separate frames. They suggested algorithm [9] is based on LSB technique but using a 3-3-2 approach. The 3-3-2 approach uses least significant bits of RGB (Red Green- Blue) level but it takes 3 bits of the red and green and only 2 bits from Blue color to form one byte. They only take 2 bits from blue color because they depend on HVS (Human Vision System) that is more sensitive to blue color. The algorithm produces image look visually like the original one.

Ibrahim *et al.* [8] described an algorithm to conceal data in video frames. They selected video frames and splitted them into three bands (red, green and blue), then applied discrete cosine transform (DCT) and ZigZag scan to convert image from two-dimensional array form to one-dimensional array and after that they sort it from low to high frequency who converted the secret image to binary form then the secret data is embedded using LSB in high frequencies to get little distortion places.

Sudeepa *et al.* [19] proposed an algorithm to hide secret information in cover video based on randomization, Steganography, Symmetric encryption and parallelization. They designed an algorithm which selects random frames and split secret data into parts then apply encryption and embedding technique for each part in parallel which it takes less computational time.

Manisha and Sharmila [11] described an algorithm for hiding secret image within one frame of AVI video. They did a two level of encryption process that uses only two bit positions in a particular video frame to accommodate bits of a secret image and it is placing in four different quadrants. The Size of secret image must be compatible with size of the video frame. They proposed to use a hashing function to hash the bits of the secret image onto the video frame.

Limkar *et al.* [10] proposed an algorithm to hide secret information behind audio and video files. Dividing secret data and video/audio file into frames then embedding secret data in frames and dividing resulting frames into bits and encrypted them using Rivest -Shamir-Adleman RSA/Data Encryption Standard DES/Triple Data Encryption Standard 3DES algorithm. The algorithms try to increase the level of security by encrypted video/audio file after embedded secret information.

Dasgupta *et al.* [4] proposed architecture for hiding information in video frames using 3-3-2 LSB for embedding technique and a genetic algorithm is used as an optimization technique. The optimizer is trying to optimize the stego-frame using the objective function then take the optimized value and goes through the Anti-steganalysis test module. Genetic algorithm is trying to optimize hiding

process in video.

Khodaeia *et al.* [9] proposed a new adaptive steganographic technique to hide secret data within a gray-scale cover image by dividing the cover image into several non-overlapped blocks with two consecutive pixels and then producing the number of secret bits that could embed into two consecutive pixels. They embedded the secret bits into the cover image by modifying the LSBs of two consecutive pixels.

3 Proposed Steganography Method

In this section, the proposed steganography algorithm will try to embed image and text inside the cover video without a third party suspected in.

3.1 Hiding Data Algorithm in Video

This algorithm will discuss how to hide image and text message in video using deep genetic algorithm and Least Significant Bit LSB method. Figure 2 shows the proposed embedding algorithm for hiding image and text in the video. This video called a "cover video" because it is selected to cover or hide all secret data "image and text". The cover video was splitted into frames. In the proposed method, we are using Genetic Algorithm because it is one of the best search techniques that are used to find an optimal or near-optimal solution to the complicated problems [4]. The sender will apply a genetic algorithm to the frames to get the highest fitness function which is calculated by the highest difference between video frames. The reason behind selecting the highest difference between frames is to be less noise sensitive when embedding the secret data and this is described in Equation (1).

$$fitness[x] = max[frame[i] - frame[i + 1]]. \quad (1)$$

Applying noise mutation to the frames (that sender is selected from previous step) to get the best frame that is calculated by the lowest affected frame after noise mutation. The sender takes the selected frames with high fitness function ($hF1, hF2, \dots, hFn$) to embed parts of the secret image in them. Taking into consideration, the numbers of frames selected are equal to the number of image parts, to put each part of the image in different frame. Also, we must consider the minimum number of the secret image to be divided is four parts and the maximum number is the count of frames that change scene inside the video.

3.1.1 Input Secret Image

This is a secret image that we are trying to hide from a third party. At first, the secret image are splitted into parts ($p1, p2, p3, \dots, pN$) then applying Advanced Encryption standard AES technique for each part of image

bytes to be more secured, this AES step for adding a new layer for security data [14] before embedding data into the video so that secret image will be changed to encrypted byte parts ($Ep1, Ep2, Ep3, \dots, EpN$). After the Encryption process is completed for all parts of secret image, it can embed each part of the image in the frames video using deep genetic algorithm approach. Deep genetic algorithm helps the proposed method for searching to select the best pixel to replace its value with the value of the secret image based on high fitness function. Fitness function is measured with the lowest difference value between image pixel of the cover image and image pixel of stego-image after applying mutation with image part value as shown in Equation (2).

$$fitness[x] = min[stegoimage[x] - coverframe[x]]. \quad (2)$$

Also, it helps for searching to select the best frame for each part of the image with respect to the highest fitness function after applying mutation on each selected frames with each part of the secret image as shown in Equation (3).

$$fitness[x] = min(coverframe[i], imagepart[j]). \quad (3)$$

The difference between the two images is saving in Pixel Index Table (pit file) and encrypted pit file with Rivest, Shamir and Adelman RSA algorithm [15] to add a level of security. We selected a genetic algorithm (GA) approach for embedding images in the video for many reasons like keeping visual video quality and more dynamically embedding to be hard for detecting with a hacker. After GA embedded successfully we recombine stego-frames together to reproduce video with secret image "stego-video".

3.1.2 Input Secret Text

This is a secret text that trying to hide from a hacker. This text is converted to bytes then encrypted using the AES technique. After the encryption process is completed, it can be embedded in the encrypted byte in stego-video (that generated from the previous step) with many methods like using Least significant bit LSB in FLV tags [16] or using the genetic algorithm to find the best pixel with high fitness. After the embedding step is completed, it will produce the final Stego-Video with encrypted images and text and can easily send the video on the public network to the receiver without a hacker suspected in.

3.2 Extracting Data Algorithm from Video

This algorithm explains how the secret image and text message will be extract from stego-video. This is an opposite technique for embedding process.

Input: stego-Video, Encryption key, Pixel Index Table (pit) file.

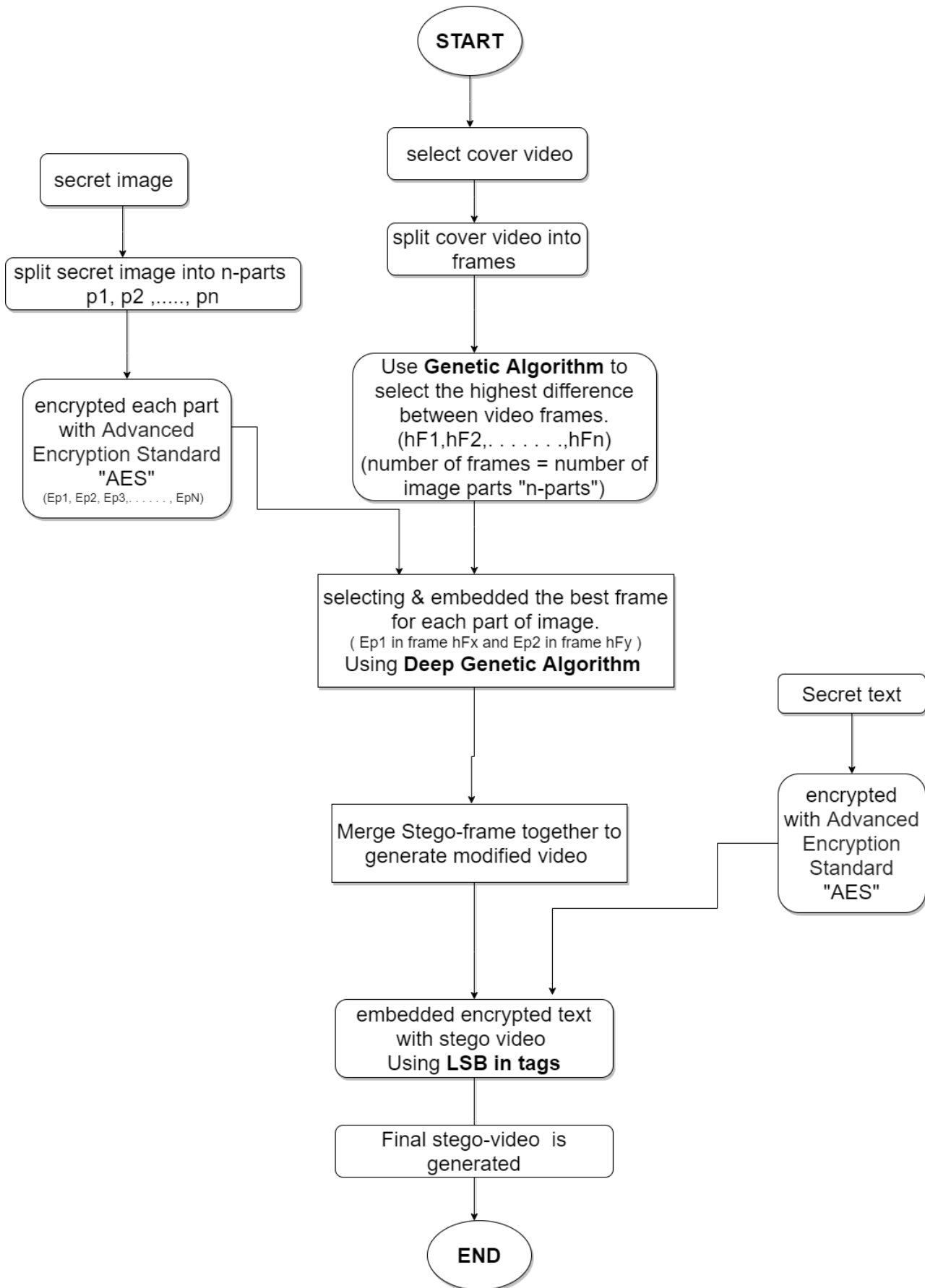


Figure 2: The proposed steganography embedding algorithm

Output: Secret Information.

Step 1: Taking Stego-video and extract secret data from the least significant bit of FLV tags and decrypted with the AES technique. From this step, the receiver has the actual message from the sender.

Step 2: Splitting stego-video into frames and selecting frames with the highest difference that sender embedded secret image parts in them.

Step 3: Decrypted pit file then use it to extract encrypted image parts from each frame.

Step 4: Decrypted image parts with AES technique.

Step 5: merge image parts to get the actual image. From this step, the receiver has the actual image from the sender.

4 Experimental Results

The experimental results discussed in this section to show and verify the performance of our proposed steganography method. We are selecting a random Flash video (.FLV extension) as cover video because FLV video can easily remove data tags [12] or add new data at the end of tags without any corruption for original video or hidden secret data at the Metadata [2] and we are using this tags for embedding secret text and for these reasons we have chosen the embedded method is Least significant bit LSB in FLV tags [16] so Adding this encrypted byte to tags is to preserve the quality of the video.

The proposed method was implemented using eclipse java version (4.12.0) and MATLAB release R2011a on Lenovo with Intel Core i7 CPU @ 2.70 GHz 2.90 GHz processors and 8 GB memory running on Microsoft Windows 10 to get the stego-video. It was found that the cover and stego-video/frames visually seemed identical. We measure the quality of the video frame by using two parameters, the first one is Mean Square Error (MSE) and the second is Peak Signal-to-Noise Ratio (PSNR) described in Equations 4 and 5. The following equations have defined these parameters:

$$MSE = \frac{1}{mn} \sum_{r=0}^{m-1} \sum_{c=0}^{n-1} [I(r, c) - K(r, c)]^2 \quad (4)$$

$$PSNR = 10. \log_{10} \frac{MAX_I^2}{MSE} \quad (5)$$

where $I(r,c)$ is the original image and $K(r,c)$ is the stego-image, m and n is the number of rows and columns in the input images respectively. MAX_I is the maximum possible pixel value of the image. It is desirable to have low values of Mean Square Error (MSE) and high values of Peak Signal to Noise Ratio (PSNR) which gives indicator for good quality of the image and more similar to the cover image. Table 1 shows the values of PSNR and MSE of the proposed method and display histogram for the cover

frame and stego-frame where the cover frame is Lena and its size is 265*265 and Figure 3 shows the secret image which is Alexandria university logo and its size is 110*143. As you can see from the result below, the histogram of the cover image and histogram of the stego-image seem approximately identical.



Figure 3: The secret image

Table 1: The PSNR, MSE and histogram Results of our proposed method











Cover image	Histogram	Secret image	Cover image after steganography	histogram	PSNR	MSE
		Top part 			42.326	3.806
		Bottom part 			44.878	2.1145

Table 2 shows the results of PSNR and MSE values for some images on the proposed method compared with Steganography Technique using the Genetic Algorithm method in [6]. They are used an advanced search algorithm such as GA to generate a key of sequence of blocks that minimizes the fitness function in which it is defined as the MSE between the original hidden text/image and the covered image. At first, initialize the population of size by rearranging the order of the blocks of the secret message using uniform random number generator. Each gene in a chromosome contains index of image pixel then using a genetic algorithm to find the optimal distribution of secret message blocks in cover. For each chromosome, the best position of each block (gene) is determined by converting each block of cover image to vector then compare all pixels of this vector with one pixel of blocks of secret message then choose minimum different and then hide the secret message/image within cover to generate the stego-image. After that, Encrypt the fit chromosome obtained from GA by adapting the BITXOR function to increase security.

But in our proposed method, At first we select the best frames using GA depending on high difference between frames and the secret image is divide it into a different numbers of parts according to its size. the secret image encrypted using AES technique and then each pixel of frame describe as chromosomes contain its position and the RGB values. we are applying cross over and mutations to get the highest fitness which is depending on the lowest difference between the video frame and the secret image

Table 2: The PSNR and MSE Results

Cover Image	Secret image	Split Secret image	Proposed Method				Steganography Method in [Essa, Abdullah, and Al-Dabbagh 2018]	
			MSE		PSNR		MSE	PSNR
			0.2160	0.3093	54.786	53.4336	2.6083	44.0012
			0.4026		52.081			
			0.4293	0.5877	51.802	50.602	2.1778	44.7847
			0.7461		49.402			
			0.0128	0.01945	67.058	65.511	0.0412	62.0193
			0.0261		63.964			

so can be easily replace secret data in the selected pixel. we trying to select the best image parts that is fit in the best frame in the best pixels/positions.

It was concluded that the proposed method gave better values [lower values of MSE and higher values of PSNR] than the steganography method in [6] where the size of the secret image is 32*32 and size of the cover image is 384*384. Finally, these results were shown no changes observed between the original video and stego-video, also the size of stego-video will remain unchanged.

5 Conclusion and Future Work

The proposed steganography algorithm, which is seeking for data hiding technique, can be applied to a video to hide secret text messages and secret images inside the tags and frames of the video. The proposed algorithm gave good results because it used many levels of deep genetic algorithm. Using genetic algorithm for selecting the best frames and the best pixels to embed images with small visual distortions also using least significant bit method for hiding secret text in video tags. We conclude that the size of the video and the quality of the secret image remain the same before and after embedding. In the future, we will apply video steganography to hide a secret video using deep genetic algorithms.

References

- [1] P. C. Bebe, K. Rajamani, P. Srideviponmalar and C. T. Samyuktha, "Secured implementation of steganography in multicloud," *Materials Today: Proceedings*, 2020. (<https://doi.org/10.1016/j.matpr.2020.12.900>)
- [2] J. P. Cruz, N. J. Libatique, and G. Tangonan, "Steganography and data hiding in flash video (FLV)," in *IEEE Region 10 Conference*, Nov. 2012. DOI:10.1109/TENCON.2012.6412279.
- [3] S. M. Darwish, S. K. Guirguis, and W. A. Alatafy, "An enhanced steganographic system for data hiding in true color images," in *The Second International Conference on Informatics Engineering & Information Science (ICIEIS'13)*, pp. 75–83, 2013.
- [4] K. Dasgupta, J. K. Mondal, and P. Dutta, "Optimized video steganography using genetic algorithm (GA)," in *Procedia Technology 10 International Conference on Computational Intelligence: Modeling, Techniques and Applications (CIMTA'13)*, pp. 131–137, 2013.
- [5] M. E. Eltahir, B. B. Zaidan, L. M. Kiah, and A. A. Zaidan, "High rate video streaming steganography," in *International Conference on Information Management and Engineering*, 2009. DOI: 10.1109/ICFCC.2009.44.
- [6] R. J. Essa, N. A. Z. Abdullah, and R. D. AL-Dabbagh, "Steganography technique using genetic algorithm," *Iraqi Journal of Science*, vol. 59, no. 3A, pp. 1312–1325, 2018.
- [7] M. M. H. Gaber, Y. F. Hassan, and K. M. Mohamed, "Cryptography with cellular automata," *International Journal of Computational and Applied Mathematics*, vol. 4, no. 1, pp. 11–18, 2009.
- [8] A. E. Ibrahim, M. A. Elshahed, and T. I. Elarif, "Video steganography using least significant bit in frequency domain," *International Journal of Intelligent Computing and Information Science*, vol. 16, no. 1, pp. 89–98, 2016.
- [9] M. Khodaei, B. S. Bigham, and K. Faez, "Adaptive data hiding, using pixel-value-differencing and lsb substitution," *Cybernetics and Systems*, vol. 47, no. 8, pp. 617–628, 2016.
- [10] S. Limkar, A. Nemade, A. Badgular, and R. Kate, "Improved data hiding technique based on audio and video steganography," *Smart Computing and Informatics*, vol. 78, pp. 581–588, 2018.
- [11] S. Manisha and T. S. Sharmila, "A two-level secure data hiding algorithm for video steganography," *Multidimensional Systems and Signal Processing*, vol. 30, no. 2, pp. 529–542, 2018.
- [12] A. J. Mozo, M. E. Obien, C. J. Rigor, D. F. Rayel, K. Chua, and G. Tangonan, "Video steganography using flash video (FLV)," in *International Instrumentation and Measurement Technology Conference*, May 2009. DOI: 10.1109/IMTC.2009.5168563.
- [13] A. Pandey and J. Chopra, "Comparison of various steganography techniques using LSB and 2LSB: A

review,” *International Journal of Scientific Research Engineering & Technology (IJSRET'17)*, vol. 6, no. 5, pp. 522–525, 2017.

- [14] A. Pandey and J. Chopra, “Steganography using aes and LSB techniques,” *International Journal of Scientific Research Engineering & Technology (IJSRET'17)*, vol. 6, no. 6, pp. 61–73, 2017.
- [15] P. Patil, P. Narayankar, D. G. Narayan, and S. M. Meena, “A comprehensive evaluation of cryptographic algorithms: DES, 3DES, AES, RSA and blowfish,” in *Procedia Computer Science 78 International Conference on Information Security & Privacy (ICISP'15)*, pp. 617–624, Dec. 2016.
- [16] M. M. Sadek, A. S. Khalifa, and M. G. M. Mostafa, “Video steganography: A comprehensive review,” in *Multimedia Tools and Applications*, vol. 74, pp. 7063–7094, 2014.
- [17] U. Sahu and S. Mitra, “A secure data hiding technique using video steganography,” *International Journal of Computer Science & Communication Networks*, vol. 5, no. 5, pp. 348–357.
- [18] D. K. Sarmah and N. Bajpai, “Proposed system for data hiding using cryptography and steganography,” *International Journal of Computer Applications*, vol. 8, no. 9, pp. 7–10, 2010.
- [19] K. B. Sudeepa, K. Raju, H. S. R. Kumar, and G. Aithal, “A new approach for video steganography based on randomization and parallelization,” in *Procedia Computer Science 78 International Conference on Information Security & Privacy (ICISP'15)*, pp. 483–490, 2016.
- [20] Y. Wang, H. Zhao, S. Liu, Y. Liu, S. Liu, “Video steganography: A review,” *Neurocomputing*, vol. 335, pp. 238–250, 2019.

Biography

Nouran Mohamed Selim was born in 14 th May, 1993, Alexandria, Egypt. She obtained the B.Sc. degree in Computer Science, Faculty of Science, Alexandria University, 2015 with Grade: “Excellent with the degree of honor”. Currently, she is Teaching Assistant of Faculty of Education, department of Mathematics, Alexandria University, Egypt. Her research interests include computer and information security.

Shawkat Kamal Guirguis was born in 25 th February, 1958, Alexandria, Egypt. He obtained the B.Sc. and M.Sc. Degrees in Computer Science & Automatic Control, Faculty of Engineering, Alexandria University, 1981 and 1984 respectively, with Grade: “Distinction with the degree of honor”. In 1988 he obtained a Ph.D. in Electronics & Communication, Cairo University, Co-Supervised by Imperial College of Science & Technology, University of London, U.K. Currently he is Professor of Computer Science and Informatics, department of Information Technology, Institute of Graduate Studies & Research (IGSR), Alexandria University, Egypt. His current research interests include network and information security, wireless sensor networks, data mining and cloud computing.

Yasser Fouad Hassan was born in 20 th May, 1974, Alexandria, Egypt. He obtained the B.Sc. degree in Computer Science, Faculty of Science, Alexandria University, 1996. In 2003 he obtained a Ph.D. degree in Computer Engineering, Tooin University of Yokohama, Japan. Currently, he is Professor of Computer Science, Faculty of computer science and AI, Pharos University, Egypt. His current research interests include Artificial Intelligence, Soft Computing, Machine Learning, Neural Networks, Cellular automata.