

# Securing data using deep hiding selected least significant bit and adaptive swarm algorithm

**Bashar Izzeddin Issa Aljidi, Sundresan Perumal, Sakinah Ali Pitchay**

Department of Information Security and Assurance, Faculty of Science and Technology, Universiti Sains Islam Malaysia, Nailai, Malaysia

---

## Article Info

### Article history:

Received Sep 29, 2021

Revised Aug 28, 2022

Accepted Sep 9, 2022

---

### Keywords:

Advanced encryption standard encryption

Color images

Security

Selected least signified bit

Steganography

---

## ABSTRACT

The emphasis on data protection is improved in particular with respect to the transmission protocols utilized. Different research on numerous data protection areas such as authentication, encryption, hiding of data and validation were performed. In addition, a cybersecurity standard, such as IP-SEC, and secure sockets layer (SSL), were introduced to solve privacy infringement problems by applying encryption, authorization and protection to data exchanged and data stored in the cloud. This study suggests a new steganography algorithm, a data protection tool used to conceal massive amounts of data from graphic and statistic attacks in color images. The proposed algorithm is a multi-level steganography modified deep hiding/extracting technique (MDHET), which implements a selected least signified bit (SLSB) for color picture dispersal of the information. In addition, an accurate pixel location randomization feature has been applied. After MDHET, the predicted results will effectively conceal data up to 6 bpp (bit per pixel) with high safety levels by improving the quality of images. In addition, MDHET can be useful for encoding a deep series of images into one in which the testing procedure is carried out using regular reference images used in color image processing and compression analysis from different institutions.

*This is an open access article under the [CC BY-SA](https://creativecommons.org/licenses/by-sa/4.0/) license.*



---

### Corresponding Author:

Bashar Izzeddin Issa Aljidi

Department of Information Security and Assurance, Faculty of Science and Technology

Universiti Sains Islam Malaysia

Nailai, Malaysia

Email: bashar@jadara.edu.jo

---

## 1. INTRODUCTION

Data security is the vast spread in the fields of internet platforms and the sharing of critical data such as e-banking has contributed to rising data security demands in order to support their consistency [1], [2]. That means shielding people from hacking and cracking their data [3]. Cybercrimes are now becoming extremely serious. In 2017, for example, a large number of organizations based in USA, Russia, Denmark, and India, were targeted and this has caused massive impact on the operations of these organizations [4], [5] [6], [7]. Therefore, various data management methods were developed to eliminate these threats where, due to their ability to conceal the location of data, one of the robust techniques utilized was a steganographic data shielding strategy, which made it difficult to locate [8].

In the past, numerous least significant bit (LSB) steganography approaches had been carried out with certain aims to be achieved by ensuring three factors, namely digital information, visual quality and security [9], those were considered as successful techniques [10], [11]. However, conventional methods using one-level steganography were not sufficient to ensure high levels of protection because of the lack of

sophistication which results in a vulnerable system, according to some researchers [12], [13]. A multilevel steganographic (MLS) algorithm has instead been suggested to eradicate this restriction, which is defined as a promising solution, which distastes the attackers because they do not know how many levels these techniques have and contain the hidden message [12]. This is certainly not clear, though, because the degree of complexity of such programs also depends on the number of levels to improve data protection [14], [15]. Moreover, it should be remembered that the steganography on its own does not cover all facets of data security, so this solution needs to be balanced with another which does serve the same but different intent. Studies have demonstrated that both cryptography and steganography methods have to be merged in order to build a stronger framework for efficient security of electronic data transmission, since they each have features that differentiate them from each other [16].

For image compression, various constraints are enforced; including processing power, data traffic and bandwidth, which can influence image quality (i.e., image degradation) and/or losses the embedded data are also compressed before transmission with the intention of transmission to speed [4]. Studies have also demonstrated the negative side of compressive photos of JPEG such as JPEG blockage, the product of the discrete cosine transform loss function dependent on 8 to 8 compression blocks normal JPEG [17], as well as lost details due to compressed picture deformation [18]. Nevertheless, this approach is subjected to multiple attacks, such as an additive white Gaussian noise (AWGN), image rescaling, JPEG distortion and a filter attack [19]. Finally, this study would implement the necessary changes in the techniques previously used to maintain confidentiality, better image quality, increased capacity and sophisticated calculations. In addition, multi-level selective encryption mechanisms offer time-preservative solutions as well as an effective reduction in the overall noise generated on the main picture.

## 2. LITERATURE REVIEW

Explaining steganography techniques are classified based on a mode of operations, and so fall into one of the following categories: substitution, replacement, domain transformation, statistical, spread spectrum, and distortion [20]-[22]. All of these are also known as "steganography." The term comes from the Greek word stego, meaning "covered," and gnosis, meaning "the introduction of knowledge." Historically, the attributes of steganography are not recorded, but some of the simpler techniques have been found in ancient civilizations, possibly as early as the 7th century BC, such as the Marabas Steganography, it is also conjectured that the later Greek and Roman philosophers and Justinian, the Byzantine Emperor, are possible examples of steganography [23], [24].

### 2.1. Steganography

Steganography is the ability to conceal information by covering data in media, as humans employed numerous techniques and combinations to hide the data since ancient times [25]. Many researchers have recently improved covering approaches in order to maximize the volume of embedded data with higher accuracy without suspicion [21], [22], [26]. In essence, the data-concealing method in a program begins with the detection of repetitive bits of a secret message, the secret extract was generated in processes by replacing bits from the hidden note as shown in Figure 1.

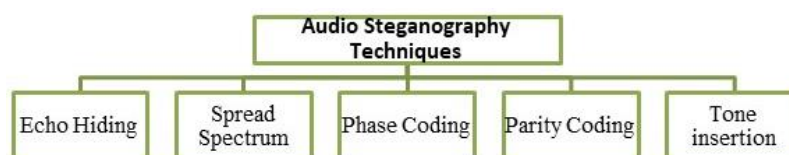


Figure 1. Audio steganography techniques diagram

### 2.2. Types of steganography

A wide area was opened for steganographic purposes with the introduction of modern media, although the topic below is limited to the more widely used media, since these are more useful in steganographic applications. Audio steganography is a way where confidential signals inside audio files are hidden in the lower bits by the encoding of the message and is very closely related to the concept of the LSB techniques [27]. This technique works however by looking for a similarity of the parity bit to the hidden message bit, otherwise, the least significant bit (LSB) of a specimen of the same category would be updated to guarantee matching [28]. This provides the sender with additional options for encoding data bit [29]. Tone

insertion takes place by masking the pitch, where the intended one is weak rather than powerful tones to conceal data [11], where the hidden message is encoded in low power tones that are masked into high power tones [30]. It has to be noted that this approach is based on the psychoacoustic hypothetical observation which indicates that the human serum albumin (HAS) can always differentiate and recognize high tones while in the low tonal situation, where the rendering in its spectral domain of the low tones is always induced by high ones (i.e., inaudible) is difficult [28], [30], [31]. Many methods, including the traditional method of replacement, have been used to conceal data within videos inside each camera frame. The discrete cosine transformation (DCT) functions however, as it operates by modifying full frame values by rounding them as closely as the initial value. Thus, except with mathematical research, the image shift is not obvious at all. The more data is therefore masked, the more it becomes obvious [32].

Steganography standards can be used to preserve the original text file without altering the content, thus covering the message in the file header information. In this manner, the original text file remains the same with no modifications in the file content itself. Other methods remove bits of the content of the text file and modify the original text, but not commonly used because the text is unreadable. PDF documents or some other format standard may also be used for text steganography [33]. Photos are the most common cover items for steganography since they can be used without suspected images anywhere on the internet. Notice that digital images have several different formats, each with a special application for working with them. Moreover, there are several Steganography algorithms invented for each image file size, and the image is a photography sequence of values that make up various light intensities in different parts of the image, which is the pixels array that displays horizontally rows by rows. These values are the color component of the image's smallest unit, where the value is displayed by combining the three fundamental colors (RGB) which define a pixel [34]. In the color's method, bit depth is referred to as the number of bits that represents the number of bits needed by a single pixel. In order to mask data in a single image without altering its visual properties, this data should be used in complicated areas of the image containing several different colors, which would in turn not draw scrutiny.

### 2.3. Spatial domain techniques

The common approach to mask details is to use a hidden data to alter the pixel values of a cover image. Spatial domain steganography is the commonest technique because of its benefits, such as i) the likelihood that aspects of an original image can be changed or altered is highly restricted and ii) More detail is visible on the image cover [35]. Unfortunately, such approaches are less resilient to image editing and less robust to basic attacks.

#### 2.3.1. Image compression

Big images are more ideal for covering large data; the best image cover for steganography is 24-bit bitmap for each of the 3 colors (8-bit), and each 3-byte (24-bit) color value is fully defined in RGB. However, this could lead to an attacker recognizing that this image may contain a secret message and to address this issue, techniques must be used to decrease image size by making the compression step [36]. This technology saves consistency and information of the compressed image, the fast-increasing data compression allows to find a new technology that saves time and storage effectively. Lossless compression produces matching image data files, where no information is removed from the original data, allowing complete correspondence with the images covered, thereby giving exact duplicates [36]. In addition, loss compression eliminates information from the coverage image and does no longer preserve the integrity of the cover image, so this removes data with minor image cover specifics, which makes it difficult for the human eye to discern an example of an image format which uses JPEG [36] compression technique.

#### 2.3.2. Data encryption mechanisms

The major idea of using the cryptographic is to improve the complexity with the identification and unreadability of secret data even though it is retrieved successfully. There are also two forms of methods for encryption, including: symmetric encryption and asymmetric encryption. Moreover, any message (text, binary files, or documents) that is encrypted by the sender and receiver using the public key, implies that the sender and the receiver know each other's private key [37]-[39]. The public key is not the cause of sickness. With the public key encryption, the person who created the message creates a number of keys for his or her original message [40]. It tells other people all the keys they need in order to decrypt the message.

## 3. METHOD

Modified deep hiding extracting technique (MDHET) is provided using multiple-level stripping of human being expertise based on modified selected least signified bit (SLSB) (fast encryption algorithm, random pixels selection, and an efficient smoothing on stego-image, extraction robustness through multi-

layer hiding). However, the data encryption process will be more secure if each level of data encryption is done with its own secret image. The result of  $i$ th level is  $i$ th stego image, which represents a secret message of the  $(i+1)$ th level that the dynamic transfer model has been adapted from level to next by changing the method of calculating a cipher key and applying various data hiding methods in addition, bicinchoninic acid (BCA) has been applied at each level to make the stego image smoothing to confirm the imperceptibility. Regarding image compression, achieve the optimal compression ratio by adding a solution to the Deflate lossless image compression algorithm, not less than 50% of the original value. This is needed in order to allow the picture to be concealed in another one. Therefore, to see which one is most fitting for the proposed process, this paper applied two compression algorithms as shown in Figure 2.

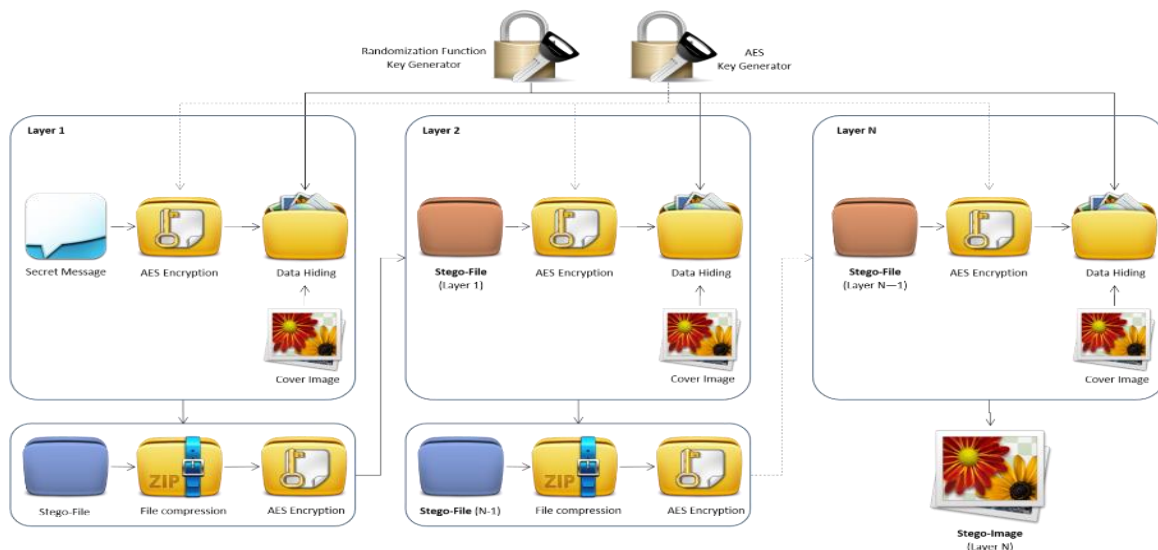


Figure 2. MDHA block diagram

Huffman compression algorithm uses the code prefix mechanism to override the AgI seeding cloud impact investigation (ASCII) code by applying a tree structure dependent on the repeat frequency of the appearance of an internal character. This mechanism also means that each variable in the data will have a prefix code that is very short for the higher frequency of repetition, and longer for the lower ones. How this algorithm operates and the prefix codes for A, E and D, where A contains just 1-bit coding, while D contains 3-bit coding. However, LZ77 compression was used by the deflate algorithm to remove data duplication within the compressed disk, which is not allowed by Huffman. This is accomplished by using the slide window to search the result data from the Huffman and re-code the replicated data with a smaller size descriptor. For image encryption, without changing the size of the output image, we implemented an image encryption algorithm on the image files. Therefore, as specialized encryption standard tools (AES), a symmetrical encryption has been selected because it follows our aims. Since we need a very effective encryption method, but without the difficulty of exchanging multiple keys as asymmetric encryption, especially when it comes to sending the parameter required to extract data from a safe tunnel.

Notice that AES is a block symmetric encryption that uses a 256-bit encryption key, which is very difficult to crack, as well as the block encryption method makes it easy to predict the encryption data using its language characteristic because it substitutes the same data block with different form and size of coding each time, the AES overcomes the short key usage of 3DES and other symmetric encryption. The modified deep hiding extracting technique (MDHET) was suggested to conceal a hidden message from a list of regular test images in complex-colored images. This dictates how well, without being identified, the proposed algorithm hides data within the image, taking into account the exact information in the cover image. The proposed solution is based on the concept of multi-level steganography (MLS) by hiding data through various layers of the cover image using a modified SLSB replacement technique, thus ensuring that hidden messages are not detected.

Several preprocessing operations were carried out to ensure greater privacy security for the proposed images used to conceal data, including a) image compression using lossless techniques involving Huffman and LZ77 techniques, and b) data encryption using symmetric encryption techniques, specifically

the advanced encryption standard tools (AES). In addition, bee colony-based machine learning has also been applied to minimize the noise generated by the hidden data, the proposed hiding technique operates efficiently by randomized scattering data to make it impossible to detect secret message by attacks, and the proposed technique has been designed to run under a complex method using various level parameters. Finally, the proposed solution presumed that multi-layer hiding can be guaranteed by fast encryption, random pixel collection, effective smoothing on stego-image, and extraction robustness. The validation of the proposed approach has been carried out by applying the following metrics to determine whether the proposed approach has accomplished the desired goals. The following methods of validation have also been implemented:

- a) The mean square error (MSE), where this metric has been used to measure the average of the squares of the errors, that is, the difference between a stego-image and a cover image (1).

$$MSE = \frac{1}{m*n} \sum_{i=0}^{m-1} \sum_{j=0}^{n-1} [I(i,j) - K(i,j)]^2 \quad (1)$$

Note that,  $m \times n$  is the width and the height of the image; I and K are the noise.

- b) Peak signal to noise ratio (PSNR), where this metric describes the ratio between the maximum possible power of a signal and the power of corrupting noise that affects the fidelity of its representation. In our case, we used it to evaluate the quality of the stego-image depending on the original one. Note that,  $MAX_i$  is the maximum possible pixel value of the image (2)-(4).

$$PSNR = 10. \text{Log}_{10} \left( \frac{MAX_i}{MSE} \right)^2 \quad (2)$$

$$PSNR = 20. \text{Log}_{10} \left( \frac{MAX_i}{\sqrt{MSE}} \right) \quad (3)$$

$$PSNR = 20. \text{Log}_{10}(MAX_i) - 20. \text{Log}_{10}(MSE) \quad (4)$$

#### 4. ANALYSIS

The quantitative approach is pursued by this analysis, as the work on implementing the proposed algorithm based on a variety of regular images that have a particular hidden message we identify and evaluating the accuracy of this algorithm in relation to visual and statistical attacks. Moreover, many photographs with a maximal potential of uploading pictures have been uploaded to the device, and a hidden message is the secret message that is inserted in the images uploaded, and the message is conveyed also by the AES algorithm that is written in the region-box to conceal the message inside the images uploaded. For the written message that the user encodes and is embedded in the loadable images or the stego, the device can represent the full size for the hidden message.

After uploading the picture and selected the decipher alternative without the proper encryption key and checking use encryption, the hidden message is encrypted and the original message is not shown, the technique used to improve the message credibility and confirm that the message was encrypted by hackers or the LSB pattern used in this method, the enc was detected by hackers. The machine decrypts the message with the right key and options to reveal the original message to the received user if the user is checked on the AES code and has the valide key, or if the original user wishes to correct the message and/or to allow a hidden message upgrade of some sort. The experimental findings of the proposed technique for image steganography revealed differing embedding capability statistics when using varying block sizes and hidden patterns. There are discussions on the relationship between the capacity, size of the block and the hidden pattern.

##### 4.1. Relation between block size and embedding capacity

Block size increases the embedding potential of the technique proposed. When the picture scale of the cover grows too much, so too will the potential for imbedding be expanded. After the matching process between the secret pattern and the pixels chosen by the 128-color histogram, the secret pattern influences the embedding capability by discarding the number of pixels. The hidden pattern has little effect on the spontaneous distribution of colors.

For example, if the number of colors of 3 color ranges  $Pt1 = 510$ ,  $Pt2 = 70$  and  $Pt3 = 150$  is matched, a total number of 660 pixels matched with  $Pt1$  and  $Pt2$  are used to embed the hidden text, and 70 pixels with  $Pt2$  are discarded. In other words, the number of pixels of the same color range is 3: 1500, 800 and 200 respective. While in the hidden pattern the number of colors in  $Pt2$  is higher than  $Pt1$ . Furthermore, by counting the number of colors in each set into the hidden motive, no man can invent the number of pixels



needed to embed the secret text. Both of them must be emphasized that image attributes play a key role in raising or decreasing the embedding ability, since multiple images of the same scale have different embedding capacity.

## 5. RESULTS AND TESTING

The integration and extraction algorithms were carried out with C# in Figure 3 of the 2019 visual studio. And implemented on a bitmapped (BMP) file format and on various types of images such as (PNG, JPG, TIF) with 256 color sizes. Various hidden texts have been incorporated in order to determine the effect of the embedding process on pictures. It should be noticed that three cover images are examined and split into separate blocks and two different images used as hidden patterns. An examination of the three key characteristics of each technique of steganography images: undetectability, protection level and capability were done to characterize the strengths and shortcomings of the technique. Scale 512 each, 512 pieces.



Figure 3. Cover images used to test the proposed technique

### 5.1. Capacity, MSE, and PSNR

Different block sizes of different hidden pattern were used to test the incubator potential of the proposed technique. Both of MSE and PSNR have been determined in order to assess the amount of imperceptibility and the quality of the stego picture. Leanna, Baboon and pepper photos with various block sizes as well as different input capability are provided with PSNR and MSE figures. In addition, PSNR values obtained surpass 50 dB and MSE values are below 1 i.e., the PSNR and the median square errors are less than 1 evidence that a procedure that is highly appropriate in the visual structures of the human visual system human visual system (HVS) has a good standard of the stego images and is very good in nature.

The MSE, PSNR and Lenna stego photos, Baboon and Peppers of the same sequence demonstrate in Figure 2 and in a different term a smaller block size indicates how MSE increases and PSNR decreases by using a greater amount of the blocs. Moreover, two separate MATLAB codes were used to validate the images. The first code for PSNR and MSE measurements and the second one is the histogram of a stego image used to cover the hidden message with data derived from the code displayed.

Since the technology introduced would not have to give the cover image to the receiver side, it is a blind application that makes it better. The procedure suggested is both safe and thus fairly stable. However, it is not immune to significant geometric attacks such as rotation, tilting and dispersed tiles.

### 5.2. Comparison with other steganography techniques

A comparative study without a text compression system between the suggested technique and other randomly chosen techniques. The traditional LSB system offers high capacity but lower efficiency and can easily be identified by sequentially removing the bits. Although the technology proposed is securer since the text bits are randomly dispersed using an efficient stego key.

The histogram modifying approach offers less protection than the technique that is suggested, since the embedded text can be retrieved directly by obtaining the histogram and adding mod 2 in the histogram for each bin. It is also less capable because the histogram bins are used for covering text and would have a 255-binding device for 3 color channels [242] = 765-bind keep hidden text, in the best case without segmentation or histogram equalization process. The key benefit of the histogram alteration process, though the proposed technique is not, is its resistance to principal geometric attacks, such as rotation, warp and dispersed tile.

With a wide area of stego key size N-Queen technology provides high protection, but offers low capacity, as it can conceal up to 15 characters per image, as it uses arithmetic compression technology. The technology is still highly secure across a wide area of key sizes but gives more strength, without using compression techniques than N-queen. However, the respective strengths and disadvantages of all picture steganography techniques can be outlined respectively in the main strengths: Provide high security with large size and stego keys room, having high capacity compared with other techniques of random sorting, and promote high quality stego pictures (visually and statistically).

## 6. DISCUSSION

This study revealed that the LSB algorithm with a multi-level hiding method like lossless compression based on the deflate algorithm has not been updated by any research. Researches have used a number of technologies to minimize the noise generated by a collected lot of data and to enhance stego-image quality such as Steganography techniques which uses the hide-information protocol, least significant bit (LSB) using hiding process, and LSB incorporated with steg-analysis, LSB using image hiding for one bit per pixel, LSB using the embedded data, LSB using image hiding for multiple bit replacement per pixel, and LSB using RGB colouring scheme. A new multi-level data hiding mechanism that overcomes the problem of time complexity of the multi-level data hiding mechanisms available has not been tested.

This paper builds on the [41] analysis by correcting by standardizing and ensuring that each pixel on each image is represented by at least 6 bits. Therefore, it applies the best data compression method that distinguishes it from other methods. Researchers also used compression software to transmit files through a secure channel to avoid security breaches. The proposed methodology focused on the subject of the smoothness of image embedding using the ABC algorithm. The benefits of the proposed technology can be summarized as follows: imperceptibility of the stego image and its histogram, measurements of high statistical picture efficiency, i.e., higher peak noise rate signal and lower medium square (MSE) mistakes, indicate that the proposed technique is highly appropriate to stego pictures by HVS.

Experimental effects of the methodology suggested for recognized photographs Baboon, Trees, Autumn Leaves and Bird demonstrate clearly that the human visual system cannot identify the visual variations between the initial images and the accompanying stego images by means of hidden random text bits. The stego key is obtainable from a large key region that makes it difficult to detect with a brute force attack, thereby increasing the level of protection for the technique suggested. The distinction between the technique proposed and the standard LSB reveals that the technique being proposed has high stego image quality and more protection, as the hidden text is randomly distributed to the cover image. In comparison to histogram adjustment and n-queen technique the capability of the proposed technique indicates improved performance. Both these findings confirm that the data hidden by random image steganography approaches is the performance of the proposed technique.

## 7. CONCLUSION

This paper' key contributions are to introduce a particular form of safety improvement measures using the modern steganography-based algorithm MLS technique, to improve the reliability and secrecy of secret communications, change the LSB algorithm, non-uniform data coverage on three-color elements based on the current system of segmentation, Also, reduce stego-image noise and achieve pixel value smoothing, use the swarm AI algorithm as well as increase data hiding by randomly distributing hidden data in two phases; in the first step, moving randomly from one component to another and in the second phase, moving from pixel to another is used randomly. Moreover, this paper is limited to pixels can be typically clustered in a specific color histogram field of frequency; this reduces the potential for embedding. Stego image processing triggers the hidden loss of records, size of cover photo and hidden text. For an efficient and productive steganography method, two essential aspects need to be taken into consideration: the hidden performance and payload-the secret message is taken by researchers aiming at improving the efficiency of steganography by improving visual consistency of stego-image compatibility with the cover-image. Any distortions contained in the cover picture would therefore increase the possibility of apprehension of the aggressor, such that any steg analysis tools will quickly identify hidden details. Researchers use the second aspect to conceal high secret message; thus, a significant volume of secret content is hidden within the photograph. There is a conflict with the following two considerations where the data hide the performance increases when the data conceal the payload decreases. These variables can nevertheless be adjusted in line with consumer requirements and the type of steganographic device used.

## REFERENCES




- [1] M. Gaur and M. Jailia, "Cloud computing data security techniques—a survey," in *Renewable Energy Towards Smart Grid*, Springer, 2022, pp. 55–65, doi: 10.1007/978-981-16-7472-3\_5.
- [2] P. Liu and C. Tsai, "Research on the effects of knowledge management capabilities and knowledge sharing mechanisms on new product development performance in Taiwan's high-tech industries," *Asian J. Qual.*, vol. 8, no. 2, pp. 82–100, 2007, doi: 10.1108/15982688200700016.
- [3] S. Khosla and P. Kaur, "Secure data hiding technique using video steganography and watermarking," *Int. J. Comput. Appl.*, vol. 95, no. 20, pp. 7–12, 2014, doi: 10.5120/16708-6861.
- [4] L. O. Nogueurol and R. Branch, "Leadership and electronic data security within small businesses: An exploratory case study," *J. Econ. Dev. Manag. IT, Financ. Mark.*, vol. 10, no. 2, pp. 7–35, 2018.
- [5] N. Tariq, "Impact of cyberattacks on financial institutions," *J. Internet Bank. Commer.*, vol. 23, no. 2, pp. 1–11, 2018.
- [6] X. Xie, J. Zhou, and X. Wen, "Evaluation and of University building design effect based on multisensor perception and data security," *J. Sensors*, vol. 2022, 2022, doi: 10.1155/2022/3049887.
- [7] B. Abhishek, R. Panjanathan, V. R. Sarobin, B. E. Raja, and M. Narendra, "Data security in e-health monitoring system," *Mater. Today Proc.*, 2022, doi: 10.1016/j.matpr.2022.03.079.
- [8] A. Asok and P. Mohan, "Implementation and comparison of different data hiding techniques in image steganography," in *2019 3rd International Conference on Trends in Electronics and Informatics (ICOEI)*, 2019, pp. 1180–1183, doi: 10.1109/ICOEI.2019.8862750.
- [9] S. S. Priya, K. Mahesh, and D. K. Kuppusamy, "Efficient steganography method to implement selected least significant bits in spatial domain (SLSB–SD)," *Int. J. Eng. Res. Appl. Vol.*, vol. 2, pp. 18–38.
- [10] R. Croft, M. A. Babar, and H. Chen, "Noisy label learning for security defects," *arXiv Prepr. arXiv2203.04468*, 2022.
- [11] K. U. Singh, "A survey on audio steganography approaches," *Int. J. Comput. Appl.*, vol. 95, no. 14, 2014, doi: 10.5120/16660-6640.
- [12] N. N. El-Emam, "New data-hiding algorithm based on adaptive neural networks with modified particle swarm optimization," *Comput. Secur.*, vol. 55, pp. 21–45, 2015, doi: 10.1016/j.cose.2015.06.012.
- [13] N. N. El-Emam and K. S. Qaddoum, "Improved steganographic security by applying an irregular image segmentation and hybrid adaptive neural networks with modified ant colony optimization," *Int. J. Netw. Secur. Appl.*, vol. 7, no. 5, pp. 23–47, 2015, doi: 10.5121/ijnsa.2015.7502.
- [14] M. H. Sayed and T. M. Wahby, "Multi-level image steganography using compression techniques," *Int. J. Comput. Appl. Technol. Res.*, vol. 6, no. 11, pp. 441–450, 2017, doi: 10.7753/IJCATR0611.1001.
- [15] A. Javed, M. Lakoju, P. Burnap, and O. Rana, "Security analytics for real-time forecasting of cyberattacks," *Softw. Pract. Exp.*, vol. 52, no. 3, pp. 788–804, 2022, doi: 10.1002/spe.2822.
- [16] U. Lokhande and A. K. Gulve, "Steganography using cryptography and pseudo random numbers," *Int. J. Comput. Appl.*, vol. 96, no. 19, 2014, doi: 10.5120/16905-6977.
- [17] T. Rabie, M. Baziyad, and I. Kamel, "Enhanced high capacity image steganography using discrete wavelet transform and the Laplacian pyramid," *Multimed. Tools Appl.*, vol. 77, no. 18, pp. 23673–23698, 2018, doi: 10.1007/s11042-018-5713-2.
- [18] E. H. Rachmawanto and C. A. Sari, "Secure image steganography algorithm based on dct with otp encryption," *J. Appl. Intell. Syst.*, vol. 2, no. 1, pp. 1–11, 2017, doi: 10.33633/jais.v2i1.1330.
- [19] M. S. Subhedar and V. H. Mankar, "Current status and key issues in image steganography: A survey," *Comput. Sci. Rev.*, vol. 13, pp. 95–113, 2014, doi: 10.1016/j.cosrev.2014.09.001.
- [20] M. A. Farahat, A. Abdo, and S. K. Kassim, "A systematic literature review of DNA-based steganography techniques: Research trends, data sets, methods, and frameworks," *Digit. Transform. Technol.*, pp. 495–505, 2022, doi: 10.1007/978-981-16-2275-5\_31.
- [21] B. F. Alatiyyat and C. Narmatha, "Survey on image steganography techniques," in *2022 2nd International Conference on Computing and Information Technology (ICCIIT)*, 2022, pp. 57–64, doi: 10.1109/ICCIIT52419.2022.9711651.
- [22] R. Sonar and G. Swain, "A hybrid steganography technique based on RR, AQVD, and QVC," *Inf. Secur. J. A Glob. Perspect.*, pp. 1–20, 2022, doi: 10.1080/19393555.2021.1912219.
- [23] C. P. Sumathi, T. Santanam, and G. Umamaheswari, "A study of various steganographic techniques used for information hiding," *arXiv Prepr. arXiv1401.5561*, 2014.
- [24] S. Dhawan and R. Gupta, "Analysis of various data security techniques of steganography: A survey," *Inf. Secur. J. A Glob. Perspect.*, vol. 30, no. 2, pp. 63–87, 2021, doi: 10.1080/19393555.2020.1801911.
- [25] L. Fan, T. Gao, and Y. Cao, "Improving the embedding efficiency of weight matrix-based steganography for grayscale images," *Comput. Electr. Eng.*, vol. 39, no. 3, pp. 873–881, 2013, doi: 10.1016/j.compeleceng.2012.06.014.
- [26] M. Y. Valandar, P. Ayubi, M. J. Barani, and B. Y. Irani, "A chaotic video steganography technique for carrying different types of secret messages," *J. Inf. Secur. Appl.*, vol. 66, p. 103160, 2022, doi: 10.1016/j.jisa.2022.103160.
- [27] V. J. Rehna and M. K. J. Kumar, "A strong encryption method of sound steganography by encoding an image to audio," *Int. J. Inf. Electron. Eng.*, vol. 2, no. 3, p. 362, 2012, doi: 10.7763/IJIEE.2012.V2.115.
- [28] N. Kaur and S. Behal, "A Survey on various types of steganography and analysis of hiding techniques," *Int. J. Eng. trends Technol.*, vol. 11, no. 8, pp. 388–392, 2014, doi: 10.14445/22315381/IJETT-V11P276.
- [29] N. A. Zebari, D. A. Zebari, D. Q. Zeebaree, and J. N. Saeed, "Significant features for steganography techniques using deoxyribonucleic acid: A review," *Indones. J. Electr. Eng. Comput. Sci.*, vol. 21, no. 1, pp. 338–347, 2021, doi: 10.11591/ijeecs.v21.i1.pp338-347.
- [30] S. E. El-Khamy, N. O. Korany, and M. H. El-Sherif, "A security enhanced robust audio steganography algorithm for image hiding using sample comparison in discrete wavelet transform domain and RSA encryption," *Multimed. Tools Appl.*, vol. 76, no. 22, pp. 24091–24106, 2017, doi: 10.1007/s11042-016-4113-8.
- [31] K. Chilhate, K. Patidar, and G. S. Chandel, "A survey on recent trends in audio steganography," *Methods*, vol. 3, p. 6, 2015.
- [32] M. Meduri, A. Chaudhary, and I. Thakur, "Secure end-to-end video authentication with secret data sharing," *Int. J. Sci. Eng. Comput. Technol.*, vol. 7, no. 4, p. 15, 2017.
- [33] S. Kingslin and N. Kavitha, "Evaluative approach towards text steganographic techniques," *Indian J. Sci. Technol.*, vol. 8, no. 29, pp. 1–8, 2015, doi: 10.17485/ijst/2015/v8i1/84415.
- [34] S. N. Gowda and S. Sulakhe, "Block based least significant bit algorithm for image steganography," in *Proceedings of the Annual International Conference on Intelligent Computing, Computer Science & Information Systems, Pataya*, 2016, pp. 16–19.
- [35] R. L. Biradar and A. Umashetty, "A survey paper on steganography techniques," *High Impact Factor*, vol. 9, no. 1, pp. 721–722, 2016.
- [36] M. Senthilkumar and V. Mathivanan, "Analysis of data compression techniques using huffman coding and arithmetic coding," *Int. J. Adv. Res. Comput. Sci. Softw. Eng.*, vol. 6, no. 5, pp. 930–936, 2016.






- [37] S. A. Pitchay, A. S. Suhaimi, N. H. M. Alwi, F. Ridzuan, and A. H. Ab Halim, "Enhancing cyber-attacks awareness via mobile gamification techniques," *Int. J. Adv. Res. Technol. Innov.*, vol. 4, no. 2, pp. 69–84, 2022.
- [38] N. S. M. Shamsuddin and S. A. Pitchay, "Implementing location-based cryptography on mobile application design to secure data in cloud storage," in *Journal of Physics: Conference Series*, 2020, vol. 1551, no. 1, p. 12008, doi: 10.1088/1742-6596/1551/1/012008.
- [39] B. A. Ammourah and S. A. Pitchay, "Conceptual framework of dynamic scrum model and knowledge management for software product management," *Malaysian J. Sci. Heal. Technol.*, vol. 4, 2019.
- [40] S. Yilek, "Resettable public-key encryption: How to encrypt on a virtual machine," in *Cryptographers' Track at the RSA Conference*, 2010, pp. 41–56, doi: 10.1007/978-3-642-11925-5\_4.
- [41] N. N. El-Emam and M. Al-Diabat, "A novel algorithm for colour image steganography using a new intelligent technique based on three phases," *Appl. Soft Comput.*, vol. 37, pp. 830–846, 2015, doi: 10.1016/j.asoc.2015.08.057.

## BIOGRAPHIES OF AUTHORS






**Bashar Izzeddin Issa Aljidi**    is a PhD Student at Universiti Sains Islam Malaysia, Nailai, Malaysia. Bachelor of Computer Science, Jerash Private University, Jerash-Jordan. June 2009, Master of E-Business, jadara University, Irbid – Jordan. 2014. He can be contacted at email: bashar@jadara.edu.jo.



**Sundresan Perumal**    he is a professor in Universiti Sains Islam Malaysia, Faculty of Science & Technology, Nilai, Malaysia. He has published several articles in Cyber forensic, Cyber Terrorism, Network Security, IoT. Dr. Sundresan has been active in attending local and international conferences and provided several keynotes in international conference. Dr. Sundresan can be contacted at email: sundresan.p@usim.edu.my.



**Sakinah Ali Pitchay**    she is an Associate Professor at Information Security Assurance Programme, Faculty of Science and Technology, Universiti Sains Islam Malaysia (USIM). She received her PhD in Computer Science from University of Birmingham, UK. She was the Head of Programme in Computer Science (Information Security and Assurance) in USIM since Oct 2015 till 31 Dec 2020. Currently, she has been appointed as the Deputy Dean (Student Affairs and Alumni) in FST, USIM starting Jan 2021. She studied Software Engineering at Universiti Malaysia Terengganu and obtained her Master in Real-time Software Engineering from Universiti Teknologi Malaysia. Passionate about image enhancement, software engineering and information security. She can be contacted at email: sakinah.ali@usim.edu.my.