Protection of images by combination of vernam stream cipher, AES and LSB steganography in a video clip

Marwah Kamil Hussein[1], Haleh Amintoosi[2]
[1]Department of Computer Information Systems, University of Basrah, Basrah, Iraq
[2]Department of Computer Software, Islamic Azad University, South Thehran Branch, Iran

Article Info

Article history:

Received May 8, 2022
Revised Aug 6, 2022
Accepted Aug 28, 2022

Keywords:

AES encryption
Digital video
Image processing
Steganography
Vernum cipher

ABSTRACT

Visual communication has become more popular in recent years, and because data must be transferred safely over a restricted bandwidth, techniques of data security and preservation, such as masking and encryption, have to be included after the optimization process for the image in question. The two most common methods of data protection are encryption and steganography. Steganography is a way for covering data that is hidden in another medium without leaving any proof of the data being changed, whereas cryptography converts regular data into incomprehensible data, which is known as scrambled data. Using the least significant bit (LSB) technique, the information was scrambled with graphics. The Vernam encryption algorithm and the advanced encryption standard (AES) will have a side in the proposed method in the encryption step, and the three improvement proposals using quality standards and encryption will be compared with the Vernam encryption algorithm and the AES encryption algorithm, and the effect of the improvement ratio and the size of the encrypted data with different threshold values will be investigated.

Corresponding Author:

Marwah Kamil Hussein
Department of Computer Information Systems, University of Basrah
Basrah, Iraq
Email: marwa.hussein@uobasrah.edu.iq

1. INTRODUCTION

Advances in computer, telecommunications, and electronics have resulted in a broad perspective in the field of multimedia, which is continually developing in terms of features and technological advancements [1]. Every day, we have more and more multimedia tools and applications on the internet, in our homes, and elsewhere. For better results, our usual television (TV) broadcast crew has moved to the digital section. There are various issues associated with the rapid rise of multimedia [2], [3].

With the introduction of the compact disc and CD-ROM CDI in the 1990s, and the availability of high-memory and low-cost computers, users were able to create rich programs that served the demands of researchers and others interested in applications, games, and education [4]. Video is being employed in a wide range of purposes, not simply for entertainment. Video conferencing, medical diagnostics, and security gadgets are more valuable everyday tools, but they require improvements in means and data protection [5], [6]. Today, reliance on digital media is not limited to the fields of games or education, but has evolved into a targeted media tool that has an impact on societies. As a result, it is necessary to raise awareness of its use in a way that serves the public interest and increases society's culture and awareness, while also maintaining the confidentiality of the transmitted information. Recently, programs and apps have become reliant on the integration and integration of two or more sensory media into an educational environment in order to deliver various knowledge and experiences. Illustrations, animation, maps, and other media can also be used [7]. Many educators have emphasized the importance of using multimedia in the classroom because it facilitates the teaching and learning processes as well as the creation comprises an information database that allows the learner to freely engage and deal with the educational program, as well as access knowledge in a range of forms and formats, allowing the student to gain a variety of practical skills when using this knowledge in new educational scenarios [8], [9].

2. RESEARCH METHOD

Steganography involves embedding the important information in techniques whereby only the sender and receiver can detect the hidden data, as in following formula. Although all media are suitable for steganography, the most widely used are videos and images because they contain a large percentage of repetition, so the embedding data get less disturbed. Encryption is the process of transforming one type of information into another using mathematical equations that require the existence of specific values, which are the encryption key [10]. The goal of encryption is to change data from readable to unreadable to prevent unauthorized parties from reading or dealing with it, but the problem is that it's easy to discover that the unread image is encrypted right away. To transform the regular image (the secret message) to the encrypted image, the encryption procedure requires an encryption key, and the vernam encryption technique was utilized in this work [11]. The key, which is kept secret, is merged with the original photographs and an algorithm to carry out the encryption procedure. To restore the original images in this way, you'll need the encrypted photographs, the technique, and the encryption key [12], [13]. One-key encryption is the first, while two-key encryption is the second. Figure 1 depicts the system for security stage.

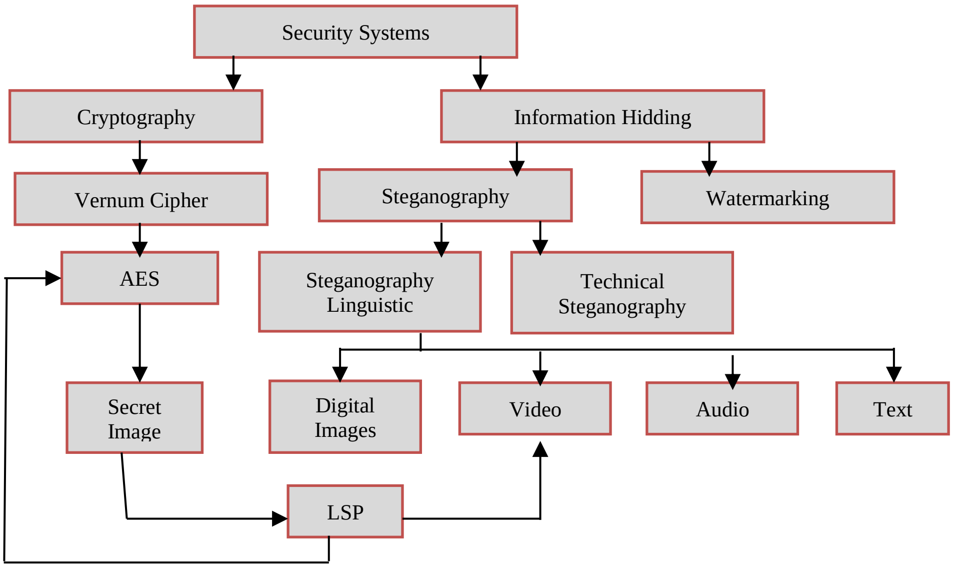


Figure 1. System for security stage

3. RELATED WORK

Uhl and Pommer [14] demonstrate how selective encryption can be used to establish a balance between security and processing needs. Wavelet image encoding, particularly wavelet packets, can be utilized for effective selective encryption. They discuss the benefits and drawbacks of each in terms of security and speed.

Research by Hussein [15], the two methods for video compression, intra and inter coded frames are utilized. Intra coded frame based on removing the spatial redundancy that found in the same frame, and inter coded frames based on removing the temporal redundancy that found between successive frames by using motion estimation algorithms. In this method (inter coded frames) two compression approaches have been proposed, The first approach is constructed from seven algorithms of motion estimation algorithms (forward motion estimation); namely, exhaustive search algorithm (ES), three step search (TSS), new three step search (NTSS), four step search (4SS), diamond search (DS), adaptive rood pattern search (ARPS) and simple and efficient search (SES).

Research by Younsi [16], learn how to use visual basic to create a package that will implement the operations used in a lossy compression strategy to compress two-dimensional images. The transform, quantization, and entropy encoding processes are the three main operations in this method. To begin, the wavelet transform is applied to two-dimensional digital pictures. Then, with no obvious loss during normal viewing, scalar quantization is used to reduce the redundancies in the images. Finally, an entropy encoder is used to compress the image in an effective manner, resulting in a significant reduction in image size. The operations are reversed to rebuild the compressed image. Research by Sanai *et al.* [17], attempts to give recipe for selecting two proposed image compression algorithm based on wavelet and multiwavelet approaches as well as to make comparison of these approaches on gray–scale image. Image compression using wavelet transform was first achieved using Daubchies 4 basis function. It is applied to each 8×8 block of the image.

Hassan and Younis [18] presented two distinct image compression and encryption techniques In the first, the image is decomposed in the spatial domain using a quad tree-based technique. In the second, a wavelet transform and a variation of the set partitioning in hierarchical trees (SPIHT) method are employed to deconstruct the image in the transform domain. In this paper, a partial encryption method takes advantage of the tree structure to reduce, if not remove, the necessity for secret-key encryption. Abdulsada [19] show how selective encryption can be used to strike a balance between security and processing requirements. For effective selective encryption, wavelet image encoding, specifically wavelet packets, can be used. In terms of security and speed, they analyze the merits and downsides of each. This is especially true when image encryption and compression are combined.

Research by Lin *et al*. [20], SPIHT and advanced encryption standard (AES) were combined to provide a partially encrypting system. Compressed SPIHT bit streams are recognized in this technique based on their value to signal quality. Then AES is used to encrypt only the important information that a user can define and choose. Parimi *et al.* [21] experimentally compare different ways to represent DCT-encoded visual data in scalable way in terms of their suitability for partial encryption.

Winder and Bibb [22] discuss the safety of sending medical photos over the internet. They propose two cryptosystems: the first is the tiny encryption method (TEA), which is a very quick algorithm by block, and the second is a stream cipher based on Vigenere's ciphering. They demonstrate the distinctions that exist between them. Khan *et al*. [23] presented a steganography algorithm for images using a neural network (NN). They used cover images and hidden secret data to extract features, which they then fed into NNs to generate outputs. The primary advantage of a NN is that it can sacrifice any non-linear functions.

Gulhane and Alvi [24] published wavelet transform steganography techniques; these algorithms offer several advantages when embedding information. A novel steganography technology for embedding sound files has also been developed by a group of researchers. They employed (LSB3) instead of (LSB1) of the cover for embedding to boost robustness, although Singh and Bhardwaj [25].Used (LSB1) in 2013 (LSB4). The algorithm used computer forensics in a new technique to improve information security. One of the best features of this method is how tough it is to implement.

4. THE PROPOSED METHOD

4.1. The sender's perspective

Encrypting and hiding the image, then moving on to the next image, and so on for all four photos (in other words, each image to which the encryption and hiding processes are applied before moving to the next image) as shown the Figure 2.

Algorithm 1: process of encryption

```
Input: Enhanced Images.
Output:Stegano Images in Video
Step1: Enter the upgraded photos to be hidden (which are represented by four colour images) and the data-hiding cover movie.
Step2: Enter the secret key, which will be used for encryption and decryption, with a value between 2 and 255.
Step3: To use in the enhanced image encoding procedure, extract the last image from the video.
Step4: Make the images that will be hidden the same size as the cover video.
Step5: Complete the rest of the image using the secret key to create the image X.
Step6: To create the image, divide the image by the secret key. Y
Step7: To create an image, combine the image with the image extracted in step 3.
Step8: For each colour image, the encoding method produces three colour images (X, Y, Z)
Step9: Repeat steps 4-7 for the remaining photos. Using the encryption key, each image from the previous stage is buried at random points throughout the video. Following are the stages that each image goes through:
```

Algorithm 2: process of hiding

```
Input: Stegano Images in Video.
Output: Original Images and Video
Step1: Generate 36 random spots (9 for each optimized image) inside the video, where random locations are generated using the secret key.
Step2: The color image X is separated into three levels: R, G, and B, and the three levels are hidden in three images within the video in the least significant bit, where each pixel represents eight bits that are hidden as follows: For all locations in each plane of the image X, 3 bits in R, 3 bits in G, 2 bits in B.
Step3: Repeat steps 2 and 3 for the photos Y and Z.
Step4: For each encoded image consisting of, operations 1 and 2 are repeated (X, Y, Z).
```

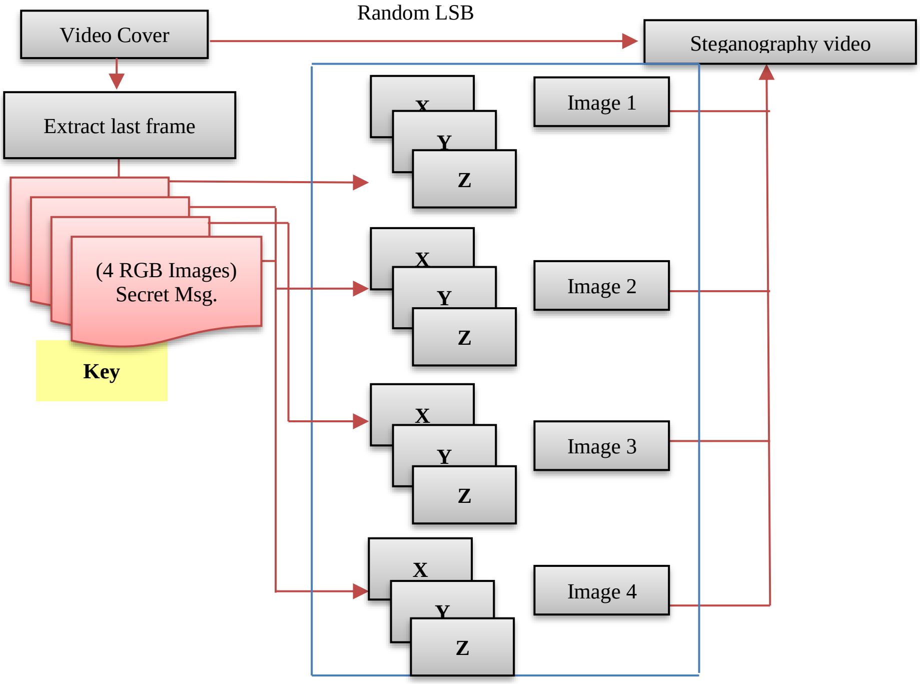


Figure 2. The general structure of the encryption and masking process

4.2. Side of the recipient

The extraction and decoding of the secret image, followed by the extraction and decoding of the following image, for each of the four photos, and so on (in other words, each image to which the two processes of extraction and decoding are applied before moving to the next image), as shown in the Figure 3.

Algorithm 3: recover images that have been hidden

```
Input:Four encoded and optimized images from the video, as well as the secret key
Output:Encrypted images.
Step1: Entering the secret key needed to decode and extract the four images from the video that are used to generate random numbers, which reflect the frame numbers in which the photos were hidden, which are 36 random locations, and the hidden and encrypted images inside the film.
Step2: Extracting the four hidden images in random positions, with RGB layers for the image x, y, and z in every three consecutive spots.
Step3: Merge all images in sequential locations to generate the colour coded image X, the next three images to generate Y, and the next three images to generate z, where each x, y, and z represents one image of the enhanced images, implying that every nine frames contains only one image of the enhanced images.
Step4: Repeat steps 3-4 to retrieve the remaining three encrypted photos from the remaining locations.
Step5: From the video, four encrypted and optimized pictures are extracted.
```

Algorithm 4: excision of code

```
Input: Encrypted images.
Output: Four Reconstructed Images and video clip.
```

```
Step1: Extracting the video's last frame for use in the encoding procedure.
Step2: Use the key of secret to multiply the image X.
Step3: Making a composite of image X and image Y to create the original image
Step4: To create the image, subtract the image extracted in step 1 from the image obtained
in step 3.
Step5: Continue using steps 2-4 for the remaining three pictures.
```

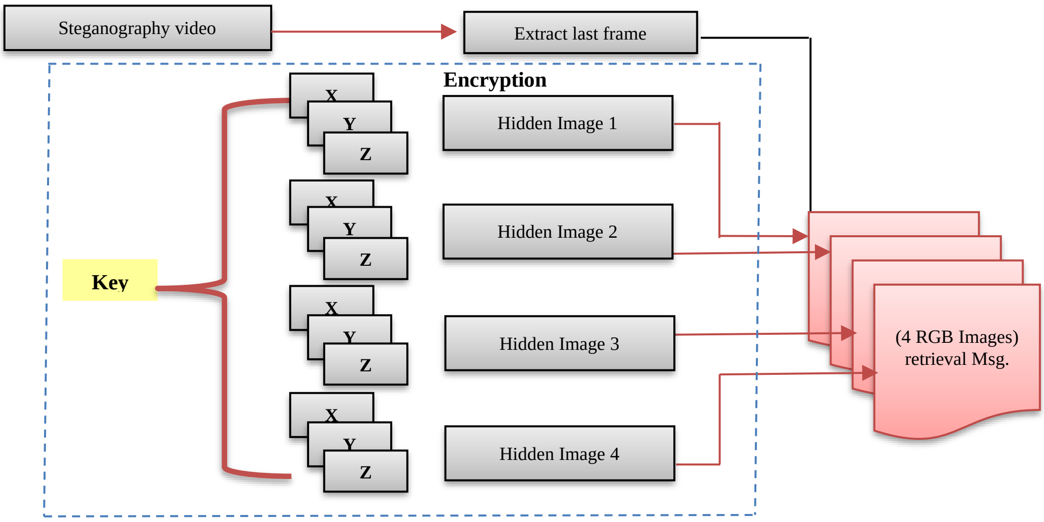
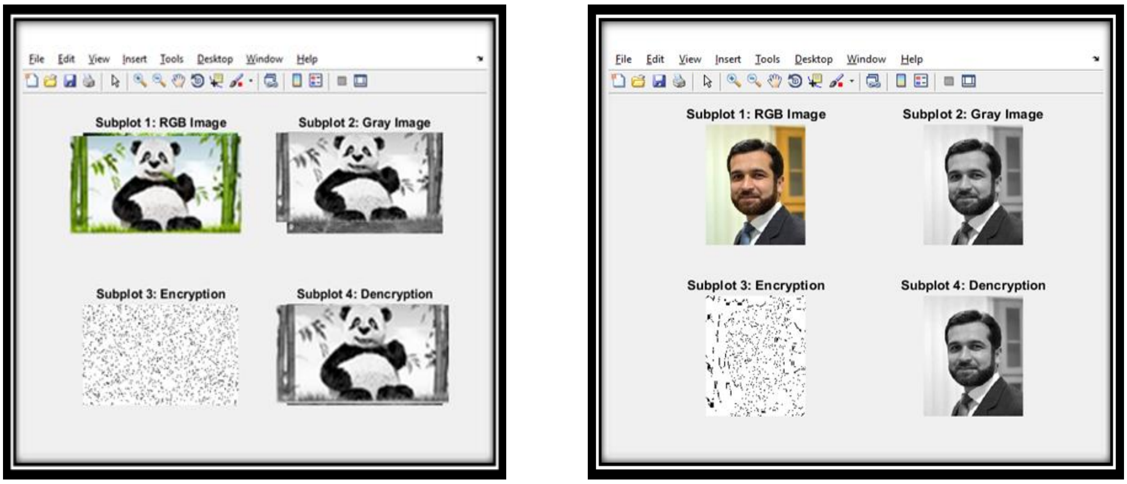


Figure 3. General structure of decoding and masking

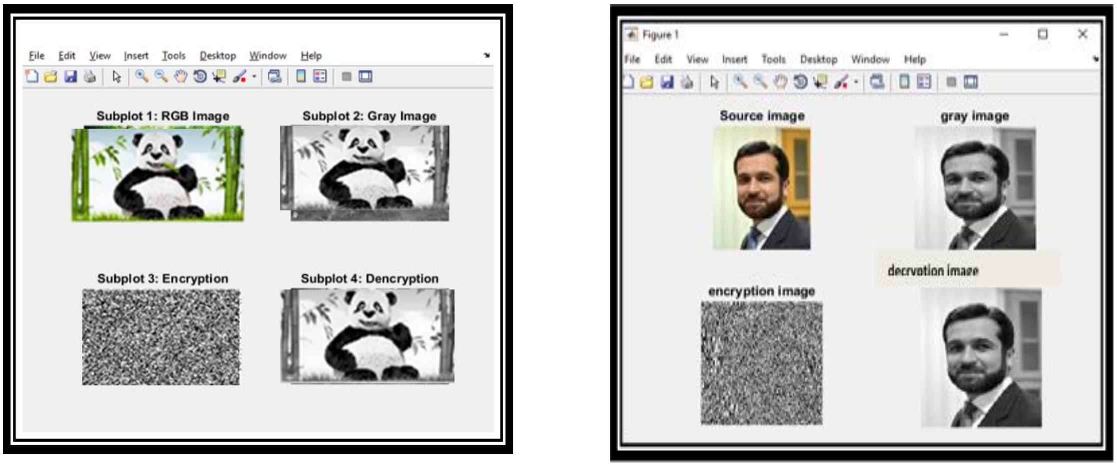
5. RESULTS AND DISCUSSION

The second proposed approach, is security stage: encryption and steganography. Where each image is encrypted using an image extracted from the video, which is the carrier of confidential data and results, where the protection process goes through two stages: the stage of encryption using the development of the encryption algorithm Vernam and merging it with the algorithm AES, in three gray images from the encryption process, and then enters another encryption stage, which is a method AES that makes it more difficult to decode and get the resulting we. The image results are displayed in the MATLAB window as shown in Figures 4 and 5 for (a) and (b) shows encoded with Vernam cipher, proposed method after optimizing them with a daptive and PCA filters.



(a) (b)

Figure 4. Represent images (a), (b) encoded with Vernam cipher after optimizing them with adaptive and PCA filters



(a) (b)

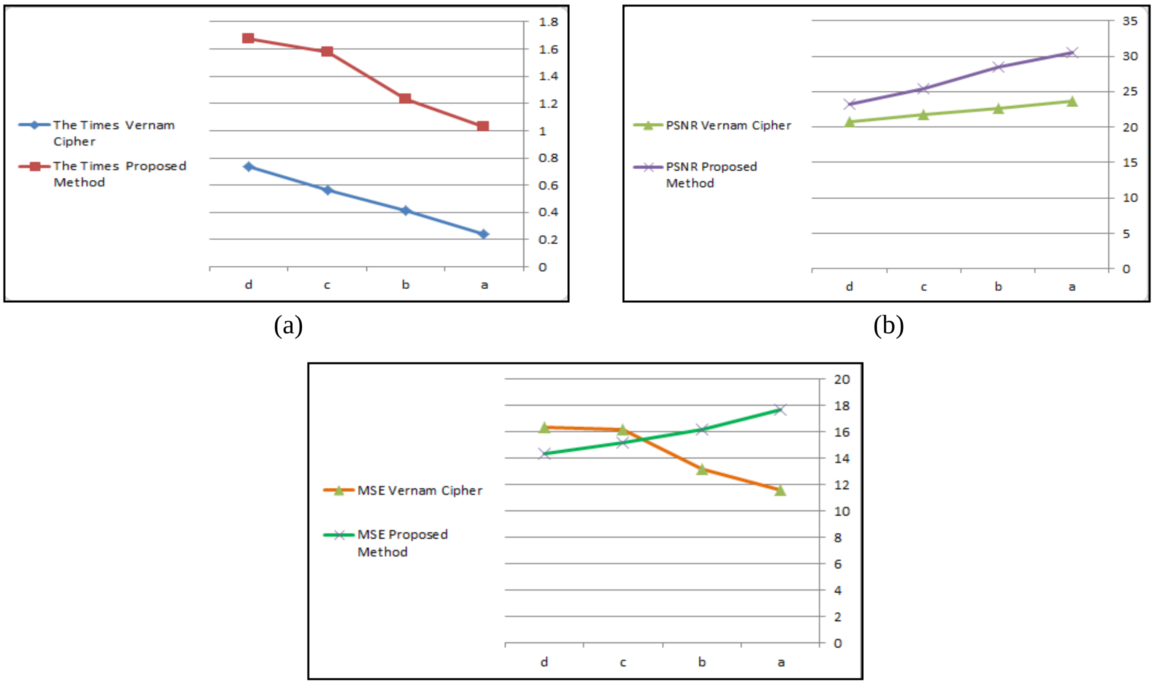
Figure 5. Represent image (a), (b) encoded with Vernam and AES cipher (proposed method) after optimizing them with adaptive and PCA filters

The second proposed method is based on hiding the optimized and encrypted images in the frames of a video clip, which has over 2,000 frames. Only 72 frames were chosen for data hiding and to complete the work of the second proposed method, as shown in Figure 6. Where this data is hidden in random segments inside the video using the LSB method and algorithm, depending on a secret key shared between the sender and recipient, and then the same secret key is used in the video encryption process, which was it also serves as a disguise for the four photos that have been encrypted. As shown in Table 1 and Figures 7(a)-(c) show the different times, PSNR and MSE between Vernam cipher only and proposed method. the amount of time for Vernam's method and the proposed method is somewhat slow, but the clarity of the image in the proposed method is better than Vernam's method, as well as the error rate.

Figure 6. Frames of video clips

Table 1. Times and PSNR for the second proposed method for images (a,b)

Images	Image size	The times		PSNR (db)		MSE	
		Vernam cipher	Proposed method	Vernam cipher	Proposed method	Vernam cipher	Proposed method
a	797 MB	0.242	1.031	23.721	30.521	11.622	17.688
b	517 MB	0.411	1.233	22.670	28.470	13.211	16.221



(a) (b)

(c)

Figure 7. Represent the different (a) times, (b) PSNR and (c) MSE between Vernam cipher only and proposed method

6. CONCLUSION

Due to the necessity to safeguard information communicated over the internet from being violated by unauthorized parties, many security solutions have emerged to address data leakage issues. Encryption is one of these options, but once the data is decoded, it will be easy to breach, thus a method to boost the strength of protection has been presented. Steganography's goal is to hide data by communicating between two parties in an unobtrusive manner to a third party. It's a strategy or technique for blocking and hiding data within a digital medium till it's hidden that there's a secret connection or information exchange that only he knows about.

The third party can see that there is a connection between two parties (two persons or two parties) when security (encryption or cryptography) information is used, but he cannot interpret the information because it is encrypted. The third person in the instance of Steganography is unaware that something is hidden or that there is a link between the two. On the other hand, after acquiring information that had been encrypted and hidden by the relevant authority, it was required to propose a method to improve the clarity of this information due to the loss and distortion it is subjected to after decoding and re-displaying it after concealment. We employed a strategy of improvement based on quality criteria to improve the information's clarity and retain it as much as feasible.

REFERENCES

[1] D. Raychaudhuri and N. B. Mandayam, “Frontiers of wireless and mobile communications,” *Proceedings of the IEEE*, vol. 100, no. 4, pp. 824–840, 2012.

[2] K. R. Raghunandan, A. Ganesh, S. Surendra, and K. Bhavya, “Key Generation Using Generalized Pell’s Equation in Public Key Cryptography Based on the Prime Fake Modulus Principle to Image Encryption and Its Security Analysis,” *Cybernetics and Information Technologies*, vol. 20, no. 3, pp. 10–2478, 2020.

[3] J. S. Lim, Y. C. Hwang, S. Kim, and F. A. Biocca, "How social media engagement leads to sports channel loyalty: Mediating roles of social presence and channel commitment," *Computers in Human Behavior*, vol. 46, May 2015, doi: 10.1016/j.chb.2015.01.013.

[4] H. Cheng and X. Li, "Partial encryption of compressed images and videos," *IEEE Transactions on signal processing*, vol. 48, no. 8, pp. 2439–2451, 2000.

[5] M. K. Hussien, K. R. Hassan, H. M. Al-Mashhadi "The quality of image encryption techniques by reasoned logic," *TELKOMNIKA (Telecommunication Computing Electronics and Control)*, no. 6, pp. 2992-2998, 2020.

[6] A. A. Alhijaj and M. K. Hussein, "Stereo Images Encryption by OSA & RSA Algorithms," in *Journal of Physics: Conference Series*, 2019, vol. 1279, no. 1, p. 12045.

[7] L. De Sousa, B. Richter, and C. Nel, "The effect of multimedia use on the teaching and learning of Social Sciences at tertiary level: A case study," *Yesterday and Today*, no. 17, pp. 1–22, 2017.

[8] A. Sadik, "Digital storytelling: a meaningful technology-integrated approach for engaged student learning," *Educational Technology Research and Development*, vol. 56, no. 4, pp. 487–506, 2008, doi: 10.1007/s11423-008-9091-8.

[9] S. Abdul-Wahed, M. K. Hussein, and H. A. Ahmed, "Compression of image using multi-wavelet techniques," International Journal of Nonlinear Analysis and Applications, vol. 13, no. 1, pp. 1519–1535, 2022.

[10] H. A.-K. Younis and Z. A. Abbood, "Steganography System to Hide a Sound File in a Color Image," *JOURNAL OF THI-QAR SCIENCE*, vol. 3, no. 3, 2012.

[11] A. S. Jubair, A. J. Mahna, and H. I. Wahhab, "Scale Invariant Feature Transform Based Method for Objects Matching," in *2019 International Russian Automation Conference (RusAutoCon)*, 2019, pp. 1–5.

[12] M. K. Hussein, A. J. Jalil, and A. Alhijaj, "Face Recognition Using The Basic Components Analysis Algorithm," *IOP Conference Series: Materials Science and Engineering, 2nd International Scientific Conference of Al-Ayen University (ISCAU-2020)*, Thi-Qar, Iraq, 15-16 July 2020, vol. 928, pp. 1-10, doi: 10.1088/1757-899X/928/3/032010

[13] A. A. Yassin, A. M. Rashid, A. J. Yassin, and H. Alasadi, "A novel image encryption scheme based on DCT transform and DNA sequence," *Indonesian Journal of Electrical Engineering and Computer Science*, vol. 21, no. 3, pp. 1455–1464, 2021.

[14] A. Uhl and A. Pommer, *Image and video encryption: from digital rights management to secured personal communication*, vol. 15. Springer Science & Business Media, 2004.

[15] M. K. Hussein, "Encryption of stereo images after estimated the motion using spatially dependent algorithms," *International Journal of Computer Science and Mobile Computing*, vol. 5, no. 12, pp. 150–159, 2016.

[16] R. Younsi, "Investigating Randomised Sphere Covers in Supervised Learning." University of East Anglia, 2011.

[17] F. M. Sanai *et al.*, "Clinical and economic burden of nonalcoholic steatohepatitis in Saudi Arabia, United Arab Emirates and Kuwait," *Hepatology international*, vol. 15, no. 4, pp. 912–921, 2021.

[18] N. S. Hassan and H. A. Younis, "Approach for partial encryption of compressed images," *Journal of Babylon University Application Science*, vol. 21, no. 3, pp. 1–10, 2013.

[19] A. I. Abdulsada, "An suggested Algorithm For partial Encryption of Compressed Images," *Journal of University of Thi-Qar Vol*, vol. 9, no. 4, 2014.

[20] T.-L. Lin *et al.*, "An efficient image processing methodology based on fuzzy decision for dental shade matching," *Journal of Intelligent & Fuzzy Systems*, vol. 36, no. 2, pp. 1133–1142, 2019.

[21] S. Parimi, A. SaiKrishna, N. R. Kumar, and N. R. Raajan, "An imperceptible watermarking technique for copyright content using discrete cosine transformation," in *2015 International Conference on Circuits, Power and Computing Technologies [ICCPCT-2015]*, 2015, pp. 1–5.

[22] J. Winder and R. Bibb, "Medical rapid prototyping technologies: state of the art and current limitations for application in oral and maxillofacial surgery," *Journal of oral and maxillofacial surgery*, vol. 63, no. 7, pp. 1006–1015, 2005.

[23] I. Khan, B. Verma, V. K. Chaudhari, and I. Khan, "Neural network based steganography algorithm for still images," in *INTERACT-2010*, 2010, pp. 46–51.

[24] A. A. Gulhane and A. S. Alvi, "Noise reduction of an image by using function approximation techniques," *International Journal of Soft Computing and Engineering (IJSCE)*, vol. 2, no. 1, pp. 60–62, 2012.

[25] N. Singh, and J. Bhardwaj, "Comparative Analysis Among Steganographic LSB Variants" *First International Conference on Information Technology, Communications and Computing (ICITCC 2017)*, 2017, doi: 10.5281/zenodo.1134255.

BIOGRAPHIES OF AUTHORS

Marwah Kamil Hussein is a lecturer in computer information systems since (2013), University of Basra in Iraq. Her current research interests included information security, Video and image processing. She is a PhD student's at the Islamic Abad University of Iran and holds the status of Assistant Professor from the University of Basra, State of Iraq. She can be contacted at email: marwa.hussein@uobasrah.edu.iq.

Haleh Amintoosi is an associate professor at the Department of Computer Engineering and the head of E-Learning Center at Ferdowsi University of Mashhad, Iran. She is also a visiting senior lecturer at the School of Computer Science and Engineering, UNSW, Australia (since 2014), and a member of FUM CERT lab. She is obtained her B.Sc and M.Sc in computer engineering from Ferdowsi University of Mashhad, Iran, in 2000, and 2003, respectively. She obtained her Ph.D. from the University of New South Wales, Australia in 2014. Her main research interest focuses on computer networks and cybersecurity. In particular, she is interested in research at the intersection of networking and security. Her research areas include: security protocols, soft security, trust, and privacy in crowdsourcing and crowdsensing systems, wireless sensor network security, security issues in internet of things (IoT), security issues in smart grid. She can be contacted at email: amintoosi@um.ac.ir.