IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Vol. 10, Issue 3, March 2021

DOI 10.17148/IJARCCE.2021.10316

A HYBRID PRIVACY PRESERVING SCHEME IN CLOUD FOR ENCRYPTED IMAGES USING CRYPTOGRAPHY AND STEGNOGRAPHY

Mr.R.Rajendran[1], K.Sheela[2], S.Simni Dhushitha[3]

Asst.Prof, Department of ECE & Krishnasamy College Of Engineering And Technology[1]

Department of ECE & Krishnasamy College Of Engineering And Technology[2,3]

Abstract: We consider a method for preventing e-Fraud in which an image is encrypted using a floating point cipher and then output is generated in image cipher text. To hide the encrypted information, the output is ‘embedded' in a host image. In principle, any cipher generator can be used for this purpose and the method has been designed to operate with images. The approach has a variety of applications and in this paper, we focus on the authentication and self-authentication of edocuments (letters and certificates, for example) that are communicated over the Internet and are thereby vulnerable to e-Fraud (e.g. modification, editing, counterfeiting etc.).

Keywords:- Watermarking, Medical Images, Stegnography

I.INTRODUCTION

In the medical world, maintaining the medical details is required to the both patients and doctor. In the hospital, medical data is widely used for number of reasons, it also helps the patient, doctor, nurses and the administrator with concurrent access the medical data with the help of these to improves the medical data and also take some decision. In the medical world most of the medical data accessed publically via the network.

Cloud computing is the emerging technology which is receiving a lot of attention from scientists for running scientific applications. The rapid transfer of health records needs some security and authentication, because the digital data can be easily duplicated and misused. Various authentication techniques have been already proposed. The former techniques convert the original data into the unreadable format, whereas later approaches use data hiding techniques. Digital Watermarking techniques play a vital role in authenticating the digital data. Digital Watermarking is the process of embedding a piece of image or data over another image to protect it from the misused. The watermark carries the data about the cover image in that it will hidden some normal content without corrupting the quality of the cover image to and it will provide good authenticity to the medical data.

In order to achieve authorized access of the ownership and secure access of data, different types of authentication techniques are being used. By combining multiple authentication techniques for accessing the data, the unauthorized users cannot have access to the data without authentication and data can be transfer to the authorized users without any loss in the data means with the original quality. The multi-level verification is embedding the watermark image into more than one image .

Cryptography is process used to encrypt plaintext into cipher text. In that Cryptography algorithm play very important roles.DNA coding will convert some binary information to DNA code thereby increase the security of the data.

In the existing system, while transferring the healthcare information from source to another location or destination there may be data loss or modification in the actual data, while transferring the medical data through the network it is easily exposed to the intruders or attacks, which the resulting will be data modification or deletion, because of which wrong data may submitted to doctor or physician which in turn results in the wrong medicine prescription or wrong treatment hence it is important to create a secure framework for transfer of these medical data.

II. RELATED WORKS

C. C. Chen et al., [1] proposes a high-capacity image-hiding scheme based on an adaptive index. Data-hiding based on vector quantization (VQ) is a technique for hiding data in the VQ index code. Data-hiding based on side match vector quantization (SMVQ) has been proposed for improving the compression rate of VQ-based data-hiding schemes. However, the hiding capacity of an SMVQ-based data-hiding scheme is very low since, at most, only one secret bit is hidden in one index code. To overcome this drawback and increase the capacity, the proposed method uses an adaptive

DOI 10.17148/IJARCCE.2021.10316

index to hide more bits in one index code. The weighted squared Euclidean distance (WSED) can also be used to increase the probability of SMVQ to get greater hiding capacity. According to the experimental results, a higher hiding capacity was obtained and a good-quality embedded image was preserved in the adaptive index SMVQ-based data-hiding scheme. The hiding capacity of the proposed scheme was approximately twice that of relevant two hiding schemes.

C. F. Lee et al., [3] exploits the characteristics of image blocks to develop an adaptive data hiding scheme that is based on SMVQ prediction. Since human beings' eyes are highly sensitive to smooth images, changes in smooth cause great distortion and attract the attention of interceptors. Hence, this study proposes a data embedding scheme for embedding secret data into edge blocks and non-sufficiently smooth blocks. The experimental results show that the proposed scheme improves the quality of the stego-image and the embedding capacity. The rapid development of the Internet and multimedia techniques has caused the hiding of data in digital media to attract increasing attention. Many researchers have studied watermarking [1,7,13,17] and data embedding. Watermarking protects the copyright of multimedia products, while data embedding securely delivers invisible secret messages that are hidden in multimedia. The latter scheme is generally referred to as stegnography.

M. Bertalmio et al., [6] describes Inpainting, the technique of modifying an image in an undetectable form, is as ancient as art itself. The goals and applications of inpainting are numerous, from the restoration of damaged paintings and photographs to the removal/replacement of selected objects. In this paper, we introduce a novel algorithm for digital inpainting of still images that attempts to replicate the basic techniques used by professional restorators. After the user selects the regions to be restored, the algorithm automatically fills-in these regions with information surrounding them. The fill-in is done in such a way that isophote lines arriving at the regions' boundaries are completed inside. In contrast with previous approaches, the technique here introduced does not require the user to specify where the novel information comes from. This is automatically done (and in a fast way), thereby allowing to simultaneously fill-in numerous regions containing completely different structures and surrounding backgrounds. In addition, no limitations are imposed on the topology of the region to be inpainted. Applications of this technique include the restoration of old photographs and damaged film; removal of superimposed text like dates, subtitles, or publicity; and the removal of entire objects from the image like microphones or wires in special effects.

P. Tsai., [7] said Reversible data hiding is required and preferable in many applications such as medical diagnosis, military, law enforcement, fine art work and so on. The author proposes to use reversible data hiding applications with a vector quantisation (VQ)-compressed image. The histogram of the prediction VQ-compressed image is explored. The prediction VQ encoded image is identical to traditional VQ encoding. The index of prediction encoded VQ images is modified to embed secret data. Furthermore, the VQ images can be completely reconstructed by the recovery procedure. The experimental results show the performance of the proposed method and the efficiency of the embedding, extraction and recovery procedures. In comparison with other VQ-based schemes, the proposed method provides a higher hiding capacity and a better stego-image quality. Also, the lossless VQ image is recovered.

III.PROPOSED METHODOLOGY

In this proposed system represent how the image transfers to the user with the safe mode. It transfers the image through the network to the entire user and it contains some formats and steps also available, such as represented into the proposed system. A main concern of these formats is securing data. Using visual cryptography we have to secure the data. If the particular information transfers through the image too many users but it will be shared by the sender and they send only the part of the data which they should know. These type of security used to secure the military secretes and it is more important to avoid the leakages. Military secretes should be confidential because anyone can hack the details and they have to take against action and chance to misuse. Leaking of our security details and our draw backs is main reason for bomb blast, high jacking flight, and Ship also. It creates bad situation. In Visual cryptography we can follow some steps to avoid the retrieving of secrete details. Military attacking ways, usage of gun details and type of protection everything is going to share with our team members at the same time it should protective by the user. Army peoples are staying at the different area or place so we have to transfer the information through internet only. Some of the people will get the chance to hack and leak out the certain information. Terrorist also have chance to hack our military secretes it cause many problem and they will take action against our country. It is most useful to secure our secrete details confidentially.

Select any one of the share from the original and shares can be performing easily encrypt by the simple method using XOR method. Each share encrypts by the user and secure by the user. Select any one of the image as display image. Use that image as cover image of the encrypted share. By pausing key only decrypt the encrypted share and it shows our secrete image.

Some secrete image as shared into the users and they are going to follow and protect our country based on information. It will be highly secured by the sender. Before going to transfer the information we have to share our image. Each share of the image transfers to the different user and remaining part as hide from the other user. Each share should contain valid information and it should be valuable for the particular user.

DOI 10.17148/IJARCCE.2021.10316

Each and every share is encrypted by the sender with different keys. Keys should be protected by both sender and receiver. Each and every user contains separate key to encrypt their part of the share. After encrypted that share should be embedded with the display image. It will be useful to change the unknown person attention so it will be very useful to protect the data. These methods represented as the segmentation. Each and every share before going transfer into the user we have to embed by the display image. This is the best way to encrypt the image and change the unauthorized person attention. It can be used to secure military secretes and also their equipment structure and gun models also we can store.Transfer the encrypted share to the user and each and every user contains one share. Shares are differed by the user and it should be secured by separate key to decrypt their shares. Each part of the share contains different information. Extract the encrypted image from the display image. Before going to decrypt the image user should extract their encrypted part from the display image. Users receiving their encrypted shares and each share contains different key. Using the keys they decrypt only their part of the share. They will get the detail from the encrypted image by performing decryption operation. Finally using the key they will receive their secrete information. It defines the best way of encrypting and decrypting the image from the user.

The theme of architecture is containing information should be secure from the third party. It contains secrete information may belongs to particular person, user, personal details, country secrete information, weapon design, space plans, etc... All the information must be secure from the third party. Maintain our secrete information highly confidential. Secrete information may track from the third person and they have chance to miss behave that details. In this architecture represent the security of the military image. We can choose any of the image to secure and transfer to the different place. Image should be secured before transfer to the user and it contains some key before transfer. It uses the encryption algorithm to secure the image. Key should be secure highly from the sender and receiver. Key should be greater than 512 to 1024 because the dimension of the image as 512 X 512.

Input image contains any file format jpeg, gif, bmp, png. After selecting the input image it converted as jpeg. Shared image, encoded, cover, decrypted image everything as converted as jpeg image. It highly secures the image and reduce the size of the image. It highly secures the image. Each share should produce certain information to the user

Sharing of Image:

Every image before going to transfer to the user it must be secured by the user. Image was selected by the sender and it contains valid information. They select as map or any other gun circuit and all should be mandatory to protect from the unauthorized person before transfer to the particular group members. Select any one of the image before going to process. Image as splited into different parts and transfer to the different user. Each part contains different information. All the important information we have to share to all the users by pausing text or image. It should be mandatory to know what type of action going to perform and also should know only their part of the work. Sender selects the image and it contains some information so it should be mandatory to secure. Before going to transfer the image sender should share the image. Each sharing part contains valid information and all the shares transfer to the users.

Sharing is the best way to perform all the operation and it takes less time to encrypt also. Visual cryptography main concept is sharing only and it contains all the information shared by the sender. Sharing part also we have to secure by the sender. Shared part contains length and width of image should be 256 of 256, 512 of 512, because it can be easily splited by the user and it separated by 4 images. Each contains less size of the image. So we can easily encrypt by the user and it takes less computational time. Each part of the shared image contains valid information and it cannot predict by the third party.

Encrypting Shared Image:

Encryption option is going to perform by the sender. We are going to transfer encrypted share into the different user. Each user receiving encrypted shares only and it contain information cannot be get without pausing keys. Encryption operation is very important and it contain information should be secured. It contains key should be confidential. Key can be used by both sender and receiver only; at the same time key will be differ by shares. All the shares do not have same keys. Surely it will be differ by shares. This is the best way to hide all the information within the group members. So If any one of the caught by terrorist our information will not be leaked out. Shares are encrypted by the separate keys and it is going to use the symmetric algorithm. It encodes the original image share by the symmetric operation. Encryption can be performed by the Advanced Encryption Standard (AES) algorithms. It contains different ways to encrypt. We can use which is suitable to encrypt our share and easy to use. Every encrypted image we are going to transfer to the different user with containing information.

Embedded into Display Image:

After performing the encrypted operation each share needs to send to the user but if any one saw the will think it contain highly confidential image. So, we have to embedded that every encrypted image into one display image. It looks like a common image but it enclosed by the confidential data.

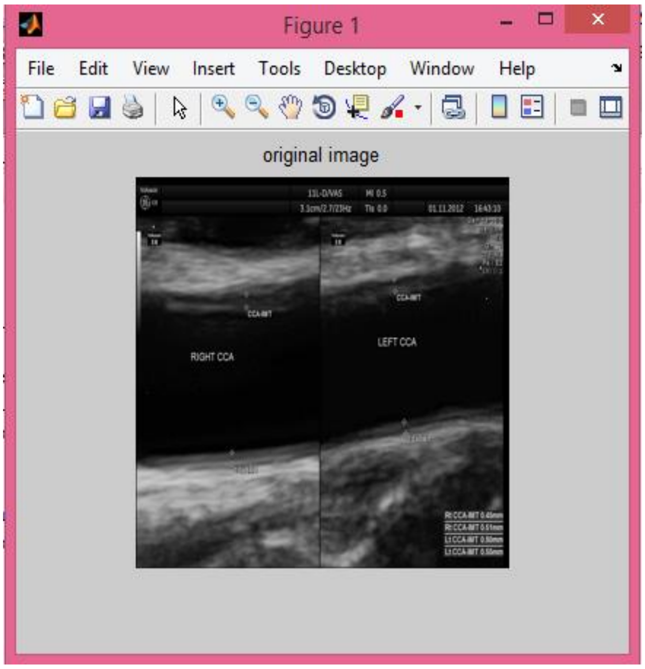
Shares contain image as encrypted by symmetric algorithm after that it is going to embed by the display image and all the image is going to combined into the display image. Display image is common for all the shares. Here we are going to embed the display image in the least significant bit of the image. It will be extract easily and also hide the details by the sender. Here all the user receives the display image only in that image there are going to extract secrete information. Display image covers the encoded secrete image and it protects our secrete image highly.

Decrypting the Display Image:

User receives the separate encrypted share and it overlapped by the display image. It contain secrete image and it will be useful to the receiver. Sender transfer the secrete message to the entire user and it contains separate key. Image is decrypted by symmetric algorithm and it pass by the private key. Private Key is very confidential and it is used to decrypting the image. Extract the encrypted image from the display image.In that secrete image is extracted from the cover image. That extracted part shows as the encrypted image. Pausing key we will get the secrete information. Finally, user gets the information.

IV.RESULTS AND DISCUSSIONS

Our project is functioning effectively as getting the requirements. We are encrypt the image successfully and also embed and extract the secrete image from the cover image. After performing the each and every process the image moved to the containing folder. Steganography process is performed based on the LSB. Reversible function of steganography is also performing well. We have tested all the modules as individuality and integrated form. It extracts our encrypted image from the cover image. Encrypted image as covered into the original image as new concept and it highly secure our secrete image from third party. It is used to identify the LSB from the image and hide into it. Finally extraction performs from the cover image and it easily came out from the cover. This classification is based on a reference image derived from the image itself, a prediction of it. It highly performs the security of image after extracting by pausing the key only the image is decrypting. Decryption is going to perform after the steganography operation.



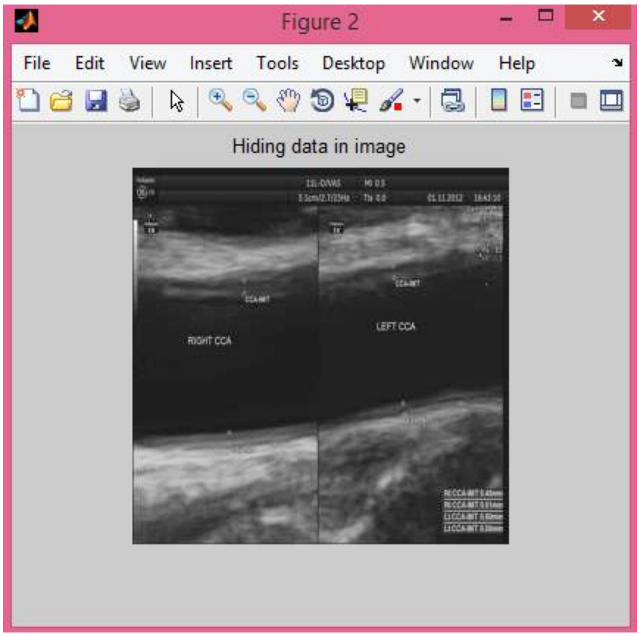
IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

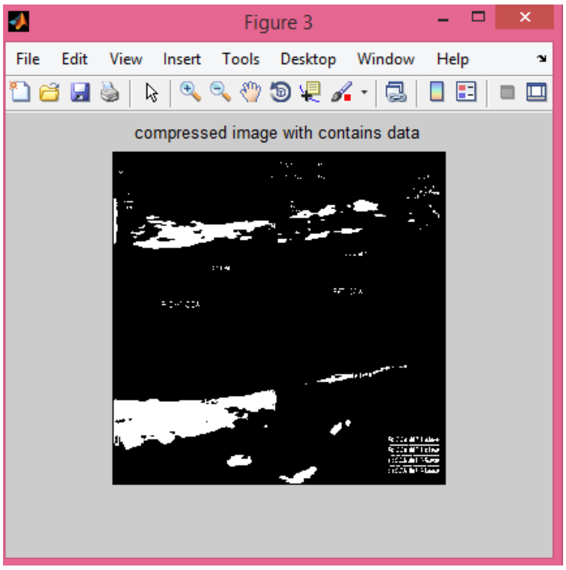
International Journal of Advanced Research in Computer and Communication Engineering

Vol. 10, Issue 3, March 2021

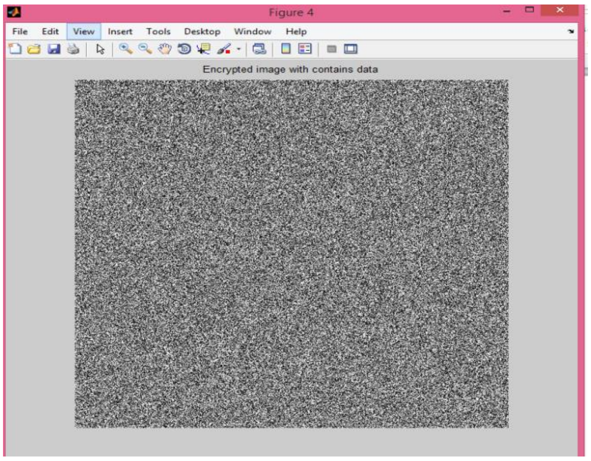
DOI 10.17148/IJARCCE.2021.10316



Hiding data in image



compressed image with contains data



Encrypted image with contains data

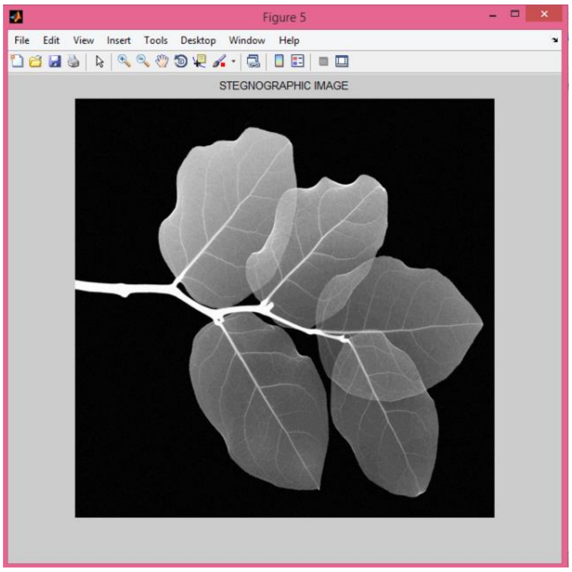


Figure 5
File Edit View Insert Tools Desktop Window Help
STEGNOGRAPHIC IMAGE

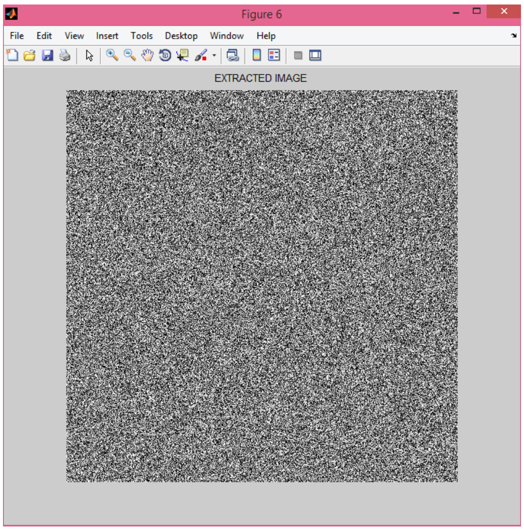


Figure 6
File Edit View Insert Tools Desktop Window Help
EXTRACTED IMAGE

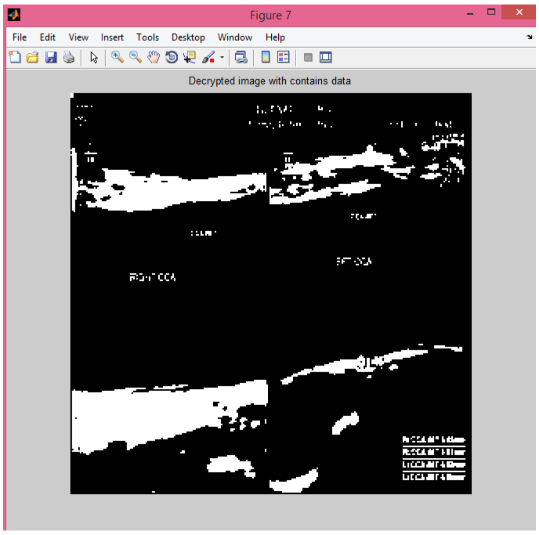
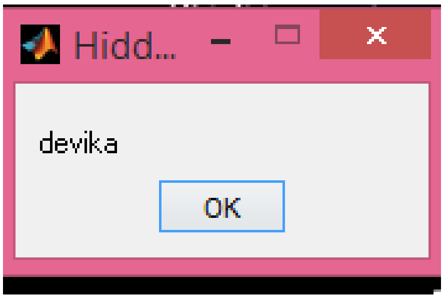
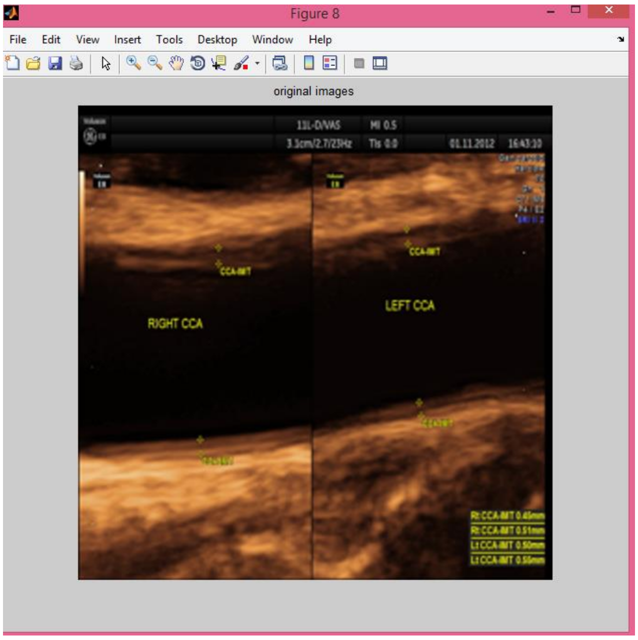


Figure 7
File Edit View Insert Tools Desktop Window Help
Decrypted image with contains data



devika



V.CONCLUSION

Embedded techniques in visual cryptography is highly secured the military secretes and it protects our weapon designs and country security details. When we transfer the secrete details from one place to another place is highly protects. It passes the data easily through the network. It protects from the secrete hackers, other country people. We can easily maintain our military secretes and increase our military power then other countries. It increases the security power. In this project we are going to perform reversible of steganography and it extracts the encrypted image from the cover image and the extracted image is used to decrypt by the user. By pausing keys used to decrypt the image and getting the secrete image. Future work is providing the better pixel production for the decrypted image and increases the resolution. Providing and raising the qualities of the image after decrypting the secrete image. It is one of the upcoming challenges.

REFERENCES

1. C. C. Chen and C. C. Chang(2010) ‘High Capacity SMVQ-Based Hiding Scheme Using Adaptive Index’ Signal Processing, vol. 90, no. 7, pp. 2141-2149.

2. C. C. Chang, W. L. Tai and C. C. Lin, ‘A Reversible Data Hiding Scheme Based on Side Match Vector Quantization,’ IEEE Transactions on Circuits and Systems for Video Technology, vol. 16, no. 10, pp. 1301-1308, 2006.

3. C. F. Lee, H. L. Chen and S. H. Lai(2010) ‘An Adaptive Data Hiding Scheme with High Embedding Capacity and Visual Image Quality Based on SMVQ Prediction through Classification Codebooks’ Image and Vision Computing, vol. 28, no. 8, pp. 1293-1302.

4. C. Qin, S. Wang and X. Zhang(2012) ‘Simultaneous Inpainting for Image Structure and Texture Using Anisotropic Heat Transfer Model’ Multimedia Tools and Applications, vol. 56, no. 3, pp. 469-483.

5. L. S. Chen and J. C. Lin(2010) ‘Steganography Scheme Based on Side Match Vector Quantization’ Optical Engineering, vol. 49, no. 3, pp. 0370081–0370087.

6. M. Bertalmio, G. Sapiro, V. Caselles and C. Ballester(2000) ‘Image Inpainting’ Proceedings of 27th International Conference on Computer Graphics and Interactive Techniques, New Orleans, Louisiana, USA, pp. 417-424.

7. P. Tsai(2009) ‘Histogram-Based Reversible Data Hiding for Vector Quantisation-Compressed Images’ IET Image Processing, vol. 3, no. 2, pp. 100 114.

8. S. C. Shie and J. H. Jiang(2012) ‘Reversible and High-Payload Image Steganographic Scheme Based on Side-Match Vector Quantization’ Signal Processing, vol. 92, no. 9, pp. 2332–2338.

DOI 10.17148/IJARCCE.2021.10316

9. W. J. Wang, C. T. Huang and S. J. Wang(2011) ‘VQ Applications in Steganographic Data Hiding Upon Multimedia Images’ IEEE Systems Journal, vol. 5, no. 4, pp. 528-537.
10. Zhiwei Yu, Clark Thomborson, Chaokun Wang, Jianmin Wang, and RuiLi,“A Cloud-Based Watermarking Method for Health Data Security.”
11. MohammadrezaNajaftorkaman, Nazanin Sadat Kazazi"A Method to Encrypt Information with DNA-Based Cryptography "
12. ArcangeloCastiglione ,RaffaelePizzolante , Alfredo De Santis , Bruno Carpentieri,Aniello Castiglione, Francesco Palmieri." Cloud-based adaptive compression and secure management services for 3D healthcare data".
13. JiantingGuo, PeijiaZheng, Jiwu Huang " Secure watermarking scheme against watermark attacks in the bencryptedvdomain ".
14. Puja Agrawal, Dr. A. A. Khurshid " Novel Invisible Watermarking for Various Images using HWT- GA-PSO based Hybrid Optimization ".
15. Bell, T., Witten, I.H., Cleary, J.G.: Modeling for Text Compression. ACM Computing Surveys 21(4), 557–592 (1989)
16. Cover, T.M., Thomas, J.A.: Elements of Information Theory. John Wiley & Sons, New York (1991)