# SECURITY AND QUALITY ENHANCEMENT DURING IMAGE STEGANOGRAPHY CONSIDERING VISUAL CRYPTOGRAPHY AND PSNR



**Ekta*, Ajit Singh**
Bhagat Phool Singh Mahila Vishwavidyalaya, Sonipat
*Corresponding Author- ektayadav956@gmail.com

**Abstract:**

Growing need of image processing has raised the requirement of image security and image quality enhancement. Present research is focusing on security and quality enhancement at the time of image Steganography. Visual cryptography has been considered and noise sensitivity has been observed using PSNR. In order to achieve this objective the image is preprocessed for reshaping and lossless compression mechanism is applied of graphical content. Such compression reduces the time consumption during visual cryptographic operation. Then this compressed and encrypted image is split before sending. Split image is transferred from two different routes. Then these files are merged at receiver end. Merged file is then decrypted and decompressed at receiving end. Finally, the PSNR, MSE and MAE of restored original images is evaluated to confirm the quality of image.

**Keyword:** Image processing, Steganography, Visual cryptography, Lossless compression, PSNR, MSE, MAE

**DOI Number: 10.14704/nq.2022.20.9.NQ44704** **Neuro Quantology 2022; 20(9):6041-6052**

## [1] Introduction

Steganography is a method for concealing a message or a picture of significance inside another image. Researchers have spent a lot of time thinking about steganography, the practice of secretly storing information in other files. One of steganography's greatest strengths is its ability to conceal communications [1][5]. However, although it is one of the most well-known methods, concealing the hidden information in every nth letter in a text using steganography is a risky Endeavour. The result was the development of picture Steganography, which quickly became the standard method for concealing data inside visual media. However, the message may go undetected if it is concealed in a manner that does not raise suspicion. If there is obvious noise or other indications in a picture, a steganalysis may readily decipher the concealed text. Similarly, steganography for audio and video files began to surface, allowing for the concealment of data inside a given audio or video clip. One key distinction: cryptography's overarching objective is to ensure confidential communications by transforming information into a format that others cannot decipher [2]. However, steganography is used to conceal information that would otherwise be easy to detect. Therefore, it is recommended to use both steganography and cryptography to safeguard information. Combining steganography with cryptography increases its protective power; cryptography is therefore used to augment steganography rather than replace it [3].

### 1.1 Steganography

Steganography refers to the technique of hiding information inside another message or a tangible medium. Electronic and computer environments sometimes include the hiding of one kind of data inside another. A combination of the Greek words for "covered" and "writing", steganography may be traced back to the Greek language. In 1499, Johannes Trithemius used the name "steganography" to describe his book Steganographia, which was a treatise on cryptography and steganography but was meant

to seem like a book on magic [6]. Images, articles, shopping lists, or other cover texts are often used to disguise the true nature of the secret messages [4]. There might be invisible ink between the lines of a personal letter. Some versions of steganography that don't rely on a shared secret might be thought of as a type of security by obscurity, whereas steganographic methods that rely on keys follow Kerckhoffs' principle [16].

Steganography has the benefit over purely cryptographic methods in that the hidden message is not immediately obvious. It doesn't matter how secure the encryption is, if the communications are in plain sight they will attract attention and might be used as evidence in nations where encryption is outlawed. In contrast to cryptography, which focuses only on guarding the communication's content, steganography seeks to hide both the fact that a secret message is being transmitted and the message itself. Steganography might include hiding data inside of other files. Electronic communications may use steganographic coding in the form of a document file, picture file, software, or protocol as part of digital steganography [7,17]. Media files, because to their size, are well-suited for steganographic transmission. If the sender starts with a seemingly harmless picture file, they may change the color of every 100th pixel to represent a letter of the alphabet. The shift is so slight that most people won't even notice it unless they're on the lookout for it.

### 1.2 Visual cryptography

In visual cryptography, visual data is encrypted in a manner that makes computer-based decryption unnecessary. A key concept in this method is the division of the picture into parts for the purposes of security, secrecy, and authentication. Binary pictures, which only include black and white pixels, are used in visual cryptography methods.[26] The picture is simply divided in half to do this. Stacking both shares allows one to reconstruct the original picture. Recent research has been focused on binary pictures, with few proposals for dealing with grayscale or colour images. While the fundamental model for grayscale photos does not need extensive cryptographic calculations, the size of the returned image is often not the same as the original. Most of these techniques, including the colour image processing techniques, do not give back the original picture [28]. This is because the quality of the returned picture is different from the original because of the large amount of data that is lost during the retrieval process. Steganography is an encryption method used to conceal information in plaintext. When compared to encryption, steganography's main benefit is that it just requires the sensitive data to be hidden. In addition to hiding sensitive information, steganography also aims to hide the fact that it is sending secret data.



### 1.3 Lossless compression

When data is compressed using lossless methods, the original data can be properly rebuilt from the compressed data with no loss of information. Most real-world data displays statistical redundancy, making lossless compression feasible. Lossy compression, on the other hand, only allows for a rough reconstruction of the original data, but often achieves far higher compression rates [24].

To put it simply, the pigeonhole principle means that no lossless compression technique can effectively compress every conceivable data type. This is why there is a wide variety of algorithms, each tailored to a particular flavour of input data or predicated on a unique set of assumptions about the redundant information lurking in the original, uncompressed data. Therefore, papers and code that can be read by both humans and machines have higher compression ratios than entropic binary data. There are a wide variety of uses for lossless data compression. ZIP files and the GNU compressing utility gzip both make use of this technique. It's also a common part of lossy data compression methods [23].

When maintaining the integrity of the original data is crucial, or when any changes to the data would be undesirable, lossless compression is used. The most common types are programmes that may be run directly, documentation, and source code. Lossless compression is used exclusively by file formats like PNG and GIF, whereas lossy compression is used by file formats like TIFF and MNG. Smaller lossy audio files are generally utilised on portable players and in other circumstances when storage capacity is restricted or perfect reproduction of the audio is desirable, whereas larger lossless

audio formats are typically employed for archival or production reasons [25].

### 1.4 PSNR

In engineering, the phrase "peak signal-to-noise ratio" (PSNR) refers to the comparison between the strongest possible signal and the strongest possible noise that degrades the signal's representation. PSNR is often stated as a logarithmic number using the decibel scale since many signals have a very large dynamic range[12]. Reconstruction quality for photos and videos that have been compressed lossily is often measured using peak signal-to-noise ratio (PSNR).

PSNR is defined in the same way for colour pictures with three RGB values per pixel, but the MSE is calculated differently because to the increased number of values to be compared (three times as many as in a monochrome image). Also, PSNR may be given per colour channel for colour pictures by converting the image to a different colour system as YCbCr or HSL [13].

#### Quality estimation with PSNR

In the case of lossy compression codecs, PSNR is the standard metric for gauging reconstruction quality. The original data serves as the "signal," while the mistake caused by compression serves as the "noise." PSNR is a metric used to approximate how people perceive the quality of a reconstruction while evaluating different compression codecs [15].

In lossy image and video compression, the PSNR is typically between 30 and 50 dB, with higher values being preferable, assuming a bit depth of 8 bits. Having a PSNR of 60 dB or greater is indicative of strong processing quality for 12-bit pictures. For 16-bit data, the PSNR typically ranges from 60 to 80 dB. According to industry standards, a quality loss of 20-25 dB in wireless transmission is acceptable [14]. When there is no background noise, pictures I and K are identical, and the MSE is also zero. As a result, the PSNR in this scenario is limitless.

#### Performance comparison

A greater PSNR is usually indicative of a better quality re-construction; however this is not always the case. One must use great caution when using this statistic, since its validity can only be shown by comparing results obtained from the same codec (or codec type) and material. It has been shown that PSNR is not especially useful for determining the quality of pictures and videos as seen by people when compared to other quality measures [12].

#### Variants



Incorporating features of the human visual system, such as contrast perception, PSNR-HVS is an extension of PSNR. PSNR-HVS-M is an enhancement of PSNR-HVS that takes visual masking into consideration. To better approximate human visual quality assessments, it outperformed PSNR and SSIM in a research conducted in 2007. Comparing it to DC Tune and PSNR-HVS, it was shown to be much superior [24].

### 1.5 Role of Visual Cryptography in Image Steganography

Combining steganography with visual cryptography is a great way to beef up security. With the use of Steganography, the hidden message may be concealed inside a picture. Visual Cryptography is used to divide the stenographer's picture into numerous parts before sending each part across an unencrypted network [18]. Steganography is the practice of concealing sensitive information inside a seemingly innocuous file or communication before removing it at its destination. Steganography may be used in tandem with encryption to provide an additional layer of security for secret information [23].

Biometric templates may be encrypted using visual cryptography, and the decryption process is straightforward. Biometric security, watermarking, electronic voting from a distance, bank client identification, and other sectors all benefit from the usage of visual cryptography [20]. There are four parts to this research report. Steganography has the benefit over simple cryptography in that the hidden communications go unnoticed. Visual cryptography (VC) is a relatively new kind of encryption that may be used to ensure that a hidden picture can be sent and stored safely, with the highest privacy protected. A sender sends a shared secret picture with encrypted data [19].

By manipulating the values of a subset of pixels, determined by an encryption method, a hidden message may be inserted into a picture via a

process called steganography. To decode the picture, the receiver has to be familiar with the same process used to choose which pixels to choose. Using video steganography, one may conceal almost any kind of data in an electronic video file [21]. The video, or series of still images, acts as a codec to transmit secret data.

## [2] Literature review

The authors have done extensive work in the field of the hybrid approach based on Visual cryptography & Steganography to address a wide range of security concerns, including but not limited to: secure transmission of secret data; quality assurance; Contrast of image; pixel expansion; cheating; alignment issues; computational complexity; confidentiality of data; etc. Picture distortion, increased storage requirements, and increased difficulty in creating shares are just a few of the issues that might arise from increasing the number of pixels used to represent an image. Recent work in VC has focused on finding ways to limit pixel growth. The performance of a VC scheme is measured in terms of PSNR, MSE, and CC, all of which pertain to accuracy. The following literature reviews were conducted for the purposes of this study:

The purpose of the work by Kaur, S. (2022) is to provide a comprehensive overview of various methods for concealing images. These databases include IEEE Explore, Web of Science (WOS), ACM Digital Library, and Willey. In this study, we outline the fundamental ideas, performance metrics, and classifications of several picture steganographic methods. The current methods of picture steganography are extensively compared and contrasted with one another in order to determine their relative merits and shortcomings. There is an examination of the efficacy of blockchain-based steganography methods as a potential improvement over existing stego-mediums. Suggestions for further study in the field of picture steganography are provided. [1]

In a comprehensive presentation, Magdy, M. (2022) covered the spectrum of medical pictures and the potential threats to their transmission. This article provides a comprehensive overview of the current methods used to protect sensitive medical data and the many threats they face. A comprehensive analysis of current studies introduces several security methods, including cryptography, steganography, and watermarking. The purpose of this study is to provide a comprehensive overview of the many algorithms used in each method and evaluate them according to a variety of criteria, including PSNR, MSE, BER, and NC. [2]



In order to conceal information in a picture, Abood, M. H. (2017) introduced a method that uses a hash function to produce a significant approach to insert data bits in the least significant bits (LSBs) of the RGB pixels that make up the cover image. Peak signal-to-noise ratio and mean square error are used to convey the security assessments. The PSNR for the hidden picture is infinite, and the MSE is also zero. A PSNR of 63 dB and an MSE of 0.03 are achieved for the cover picture. In Histogram Analysis of Secret Images, we see that there is a significant degree of resemblance between the stego-photos and the cover images, and the same is true for the secret images and the extracted images. The MATLAB computer software was used to implement these methods [3].

The two blind LSB steganography algorithms suggested by Jiang et al. (2016) as quantum circuits are grounded on NEQR, a new kind of quantum representation. In one technique, called simple LSB, the message bits are used in place of the LSB in the pixels. The other is block LSB, which uses a group of pixels inside a single picture block to encode a message bit. Only by decoding the stego cover can the extraction circuits recover the hidden message. Experiments based on analysis and simulation show that the stealth is enough, and the trade-off between capacity and robustness may be tweaked to suit different use cases [4].

Dixit (2018) outlined the many uses and benefits of electronic banking. With the advent of new information and communication technologies, the banking industry has seen a dramatic shift in its working environment. Banks' cutting-edge innovations include ATMs, Internet and telephone banking, mobile banking, and other similar services. Every method of doing business via the Internet raises serious concerns about data privacy and security. Online banking is also susceptible to attacks that target the authentication process. The purpose of this work is to evaluate existing approaches to E-Banking security and explore several data

encryption methods based on cryptographic technology [5].

Goldreich (2019) conducted a comprehensive review of the most prominent theories, methodologies, and strategies for defining, conceptualising, and solving natural cryptographic challenges. They began by discussing the fundamental building blocks of cryptography, such as computational difficulty (in the form of one-way functions), pseudo randomness, and zero-knowledge proofs. With these resources in hand, they tackled problems like designing safe general-purpose cryptographic protocols [6] and treating fundamental cryptographic applications like encryption and signature methods.

To ensure the safety of data throughout its transformation on the internet, Alotaibiet al. (2019) advocated updating mobile device authentication methods using a mix of hash, cryptography, and steganography technologies. It was utilised for authentication purposes, allowing for safe and reliable data transmission through mobile computing. Enhanced security was provided by the proposed work thanks to the usage of a hash function to store the password. The password hash is encrypted using AES and then stored as an image for later use in authentication. Combining these security techniques allows them to guarantee authenticity, confidentiality, and integrity in their services. Our suggested strategy is a viable research route for genuine mobile security [7], as shown by the results and comparisons with other existing solutions in the field of mobile computing.

An autonomously produced audio steganography technique was proposed by Ye et al. (2019). The approach uses three neural networks: an encoder to conceal information inside a carrier, a decoder to reveal that information, and a discriminator to verify whether or not the carriers really conceal information. In order to generate an embedding, extracting, and discriminating procedure, all networks are trained at the same time. Different training parameters are used to teach the system to make predictions from two separate data sets. The suggested method can generate high-quality steganographic audio that conceals audible information, outperforming the bulk of existing methods. The supplementary trials further validate the safety and strength of our method [8].

According to Bai et al. (2018), divergence is a statistical measure of the degree to which two probability distributions are similar. They demonstrate its usefulness as an alternative to the statistical distance in security proofs for lattice-based encryption. Security proofs of primitives where the attacker must solve a search problem are especially well-suited to the Rényi divergence (e.g., forging a signature). When they have a public sample ability attribute, they demonstrate that it may be used to the case of differentiating difficulties as well (such as the semantic security of encryption systems). These methods provide simpler security proofs than those now in use, as well as security proofs for schemes with fewer parameters. The stability and safety of our method [9] have been experimentally validated.



Coverless information concealment has been created, according to a recent paper by Meng et al. (2019). However, expanding the concealing capability of coverless information hiding is difficult owing to the restricted mapping connection between hidden information and feature selection. Additionally, the steganography method that relies on object identification may only conceal sensitive data in the foreground items, which reduces the overall steganographic capability. Secret information may be translated to item categories, the link between locations, and so on since object recognition includes many objects and locations. This study proposes a novel steganography technique that combines coverless information concealing with steganography by using object identification and connection mapping. Mapping the object type, colour, and secret information in an object detection algorithm allows for coverless information hiding to take place. Also, the secure location in which to conceal communications is located using object detection. The suggested approach has the potential to increase the security and robustness of coverless information concealing [10], in addition to enhancing the steganographic capabilities of the two existing techniques.

In their 2019 paper, Jha et al. suggested using quantum physics to perform an operation on a superposition of all the potential inputs simultaneously. It's true that classical computers

have made a lot of previously impossible feats possible, but they also have limitations (optimization problems where it grows exponentially). Protocols play a crucial role in ensuring the safe movement of data. The distribution of quantum keys, for instance, uses a variety of protocols such as -BB84, SA RG04, B9 2, etc. In addition, quantum cryptography has been shown to be secure in the face of various flaws in traditional encryption. One of these flaws is the inability of the quantum system to prevent the passive copying of any kind of information without interruption [11].

According to Patel et al. (2019), quantum cryptography has emerged as a means of ensuring total security via point-to-point secure key creation. Quantum key distribution (QKD) is being studied as a potential secure method for a global communication network. Several methods and models for using QKD in encrypted communication have been created. A new paradigm for QKD was established by the uncertainty principle of quantum physics. Network-based security is one method for implementing QKD. The primary focus was on developing a high-speed, point-to-point Quantum network that would use QKD technology to ensure the security of data transfers from end to end. A variety of other methods and models that make use of QKD in a network-like form are presented in the literature. This work explores an alternative method for improving Internet security; incorporating QKD into already-established protocols. This method aims for unconditional security. Our research aims to analyse QKD in MANETs, or mobile ad hoc networks.

## [3] Problem statement

There are several researches in area of Steganography and visual cryptography. But it has been observed that there is need to improve the efficiency of model by integration of compression mechanism. Compression mechanism would reduce the time consumption and space consumption. There is need to do work on several parameters such as PSNR, MSE and MAE in order to improve the quality of image during steganography operation. Moreover there is need to enhance the security by customizing visual cryptography approach.

## [4] Proposed work

### Proposed work

In proposed work research is considering the input images (I) for visual cryptography. Research is applying image pre-processing to reshape the input image (I). Now, in this work, compression mechanism has been applied that is Huffman compression on that image to reduce the image size. After that, research is considering key image (KI) for data encryption. By using KI over I, research is performing the image encryption and get the encrypted image (EI). Finally, splitter mechanism over encrypted image to split image in two parts (EI1, EI2) is applied. These images would be sending from sender via two different routes. Now, merging, decryption and decompression is performing their role on receiver end. And finally, we get the MSE, PSNR of images to evaluation the quality of images. See fig. 2 below.

### Process flow of work

In this process flow of work, research is considered images and applies preprocessing. In sender module, preprocessed image is considered for processing. On that image compression mechanism is applied then encrypts that file. See fig. 1 below.

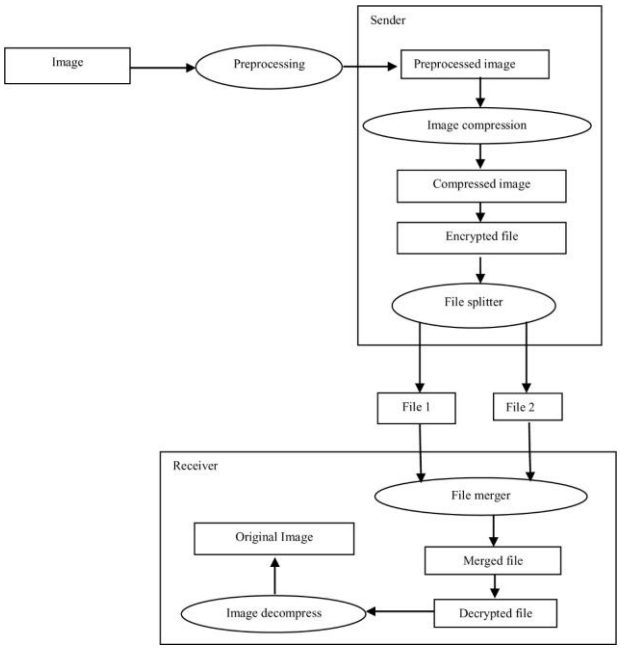



**Fig 1** Overall process of visual cryptography

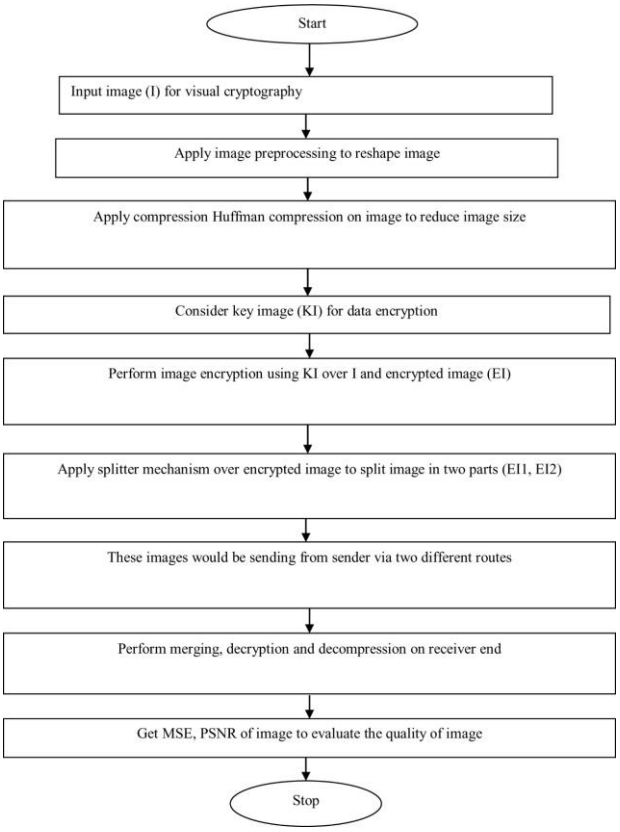



**Fig 2 process flow of proposed work**

**Algorithm**

**Step 1:** Considered input image (I)

**Step 2:** Apply Image Pre-processing for Reshaping that image

**Step 3:** Apply Huffman Coding Compression for reduction of Size of that image

**3.1 Algorithm: Constructing Huffman Coding**

*Huffman (C)*

*n*□*|C|*

Q←C

**For** i←1 **to** n-1

**do** allocate a new node z

left[z]← x ← Extract-Min (Q)

right[z]← y ← Extract-Min (Q)

f[z] ← f[x] + f[y]

insert (Q,z)

Return Extract-Min (Q)

**Step 4:** Considered key Image (KI) for Encryption of Data

**Step 5:** Perform image encryption using KI over I and encrypted image (EI)

**Step 6:** Apply Splitter mechanism over encryption image in to parts (EI1, EI2)



**Step 7:** Send that image via two different routes

**Step 8:** Perform merging, decryption and decompression on receiver end

**Step 9:** To get MSE, PSNR of image to evaluate the quality of image

**9.1 MSE**

An image's Mean Squared Error (MSE) value indicates its overall consistency with respect to pixel variation. When the MSE score is high, it indicates that the difference between the unaltered and treated versions of a picture is large.

$$MSE = \frac{\sum_1^n [x-y]^2}{M*N}$$

**9.2 PSNR**

A peak signal-to-noise ratio (PSNR) is defined as the ratio between the greatest possible signal strength and the maximum possible noise strength that degrades the quality of an image's representation. An picture's PSNR may be estimated by contrasting it with a theoretically perfect, noise-free version of the same image.

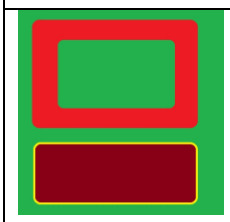
$$PSNR = 10 * \log_{10} \frac{R^2}{MSE}$$

According to a comprehensive analysis of several Visual Cryptography and steganography techniques, their comparative study, preliminary work, and various applicable fields, there are still some issues with the secret data communication, including pixel expansion, quality of shares, reconstructed image, and cheating, all of which lead to a low Peak signal to noise ratio (PSNR), high mean square error (MSE), and high mean absolute error (MAE). This approach effectively protects the confidentiality of the communicated secret by imbuing it with appropriate security levels.

## [5] Result and discussion

During simulation operation image of "lena" has been considered for visual cryptography. Original image has 512x512 dimensions that is processed by wrapper image in order to get steganograph image. Table is presenting the extension, dimension, size of image, space consume by image on disk, PSNR and MSE.

**Table 1 Feature of original, wrapper, steganograph, compressed image, and split image**

| Image | Ext | Size | Size of image | Space on disk | PSNR | SNR | MSE |
|---|---|---|---|---|---|---|---|
|  Original image | .jpg | 512x512 | 39.1 KB | 40.0 KB | 21.7890 | 14.3125 | 430.5576 |
|  Wrapper image | .jpg | 512x512 | 18.3 KB | 20.0 KB | 21.4484 | 14.5772 | 462.5529 |
|  Image after steganography | .jpg | 512x512 | 65.9 KB | 68.0 KB | 21.7891 | 16.2488 | 424.7472 |
|  Image after compression | .jpg | 512x512 | 48.7 KB | 52.0 KB | 22.5613 | 16.4137 | 340.9989 |
|  Part 1 Image after splitting operation | .jpg | 512x512 | 15.0 KB | 16.0 KB | 20.4319 | -3.1778 | 600.2613 |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
|  Part 1 Image after splitting operation | .jpg | 512x512 | 7.11 KB | 8.00 KB | 20.1622 | -16.8547 | 641.3405 |
|  Image after merging | .jpg | 512x512 | 34.3 KB | 36.0 KB | 21.9318 | 16.5394 | 421.6190 |

**Simulation of file size comparison**

File size of different images has been considered on random bases and comparison of file size in case of original, steganographic image and compressed steganographic image has been shown in following figure 3.

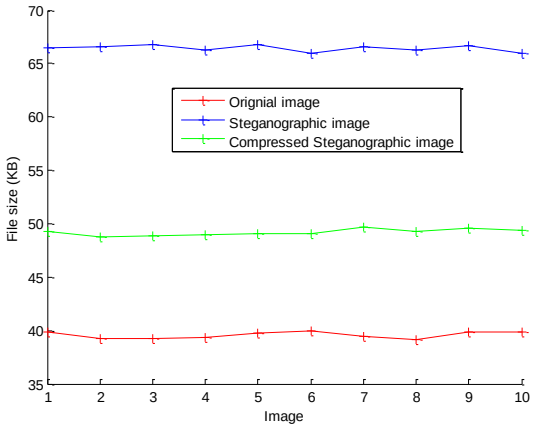



Fig 3 Comparison of File size

**Simulation of disk space comparison**

Disk space consumption of different images has been considered on random bases and comparison of disk space consumption in case of original, steganographic image and compressed steganographic image has been shown in following figure 4.

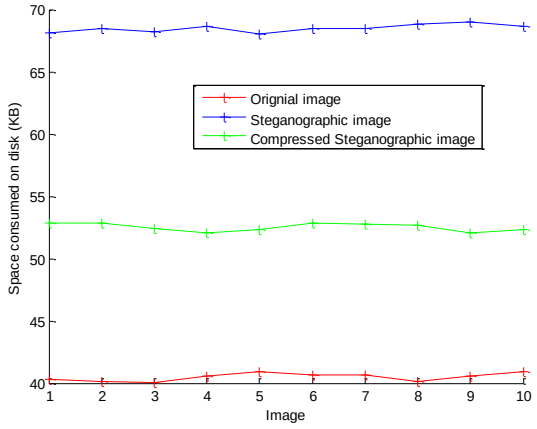



**Fig 4 Comparison of space consumed on disk**

**[6] Conclusion**

Instead of relying only on Visual Cryptography or Steganography, a hybrid technique based on the two may be more successful in terms of information security, pixel expansion, quality of reconstructed picture, and noise-like structure of image over network. There is need to consider existing research in area of Steganography, visual cryptography and compression mechanism. Prior studies in the fields of Steganography, Visual Cryptography, and Compression Mechanism are taken into account. After that, we thought about the factors that affect dependability, scalability, and security and how those factors limited prior mechanisms. The goal of this unique technique is to improve picture quality and security by combining steganography, encryption, and compression mechanisms. There should be focus on the limitation of previous mechanism and consider the influencing factor that are affecting reliability, scalability and security. There is need

of integration of steganogrpahy, cryptography and compression mechanism in order to develop novel approach for security and quality enhancement of image. The generated hybrid solution is evaluated from the point of view of the security offered during data transmission in order to resolve concerns with pixel expansion, sharing quality, reconstructed data quality, and so on. Performance, security, and dependability of hybrid techniques have been assessed and compared to those of state-of-the-art approaches.

## [7] Scope of research

In Last few years, a lot of good research work has been dedicated towards Visual Cryptography. Although a lot of advancement have been achieved but still there are various significant disadvantages like Space Complexity etc. with it which restricts it to apply in real life applications. To overcome these kind of problems, one research direction could be to analyse & improve many existing schemes for a particular of application. One may try to apply via schemes in real-life which may not be affected by its drawbacks.

One of the main problems is pixel expansion. There are lot of schemes developed to resolve it but they in turn makes it inefficient for real life applications. So, to achieve good pixel expansion quality of reconstructed image, improving PSNR, MSE etc Space complexity and time complexity etc while managing the trade -off between them can be a very good research scope.

The choice of hybrid technique based on visual cryptography and steganography may be demonstrated more effective than the solo ones. This Research approach can be beneficial in terms of providing better security to information to be communicated with less pixel expansion, good quality of shares which will not looks like a noise like structure on network, good quality of reconstructed image which in turns improve the quality factors like Peak signal to Noise Ratio (PSNR), mean square error (MSE), mean absolute error (MAE) which is the main focus in recent times in field of VC and steganography etc. while providing the maximum of security to data during communication. The suggested study work may be applied to a file which can consist of text, picture, audio, video, which will bring the better security and quality to the information transmission.

## Reference

1. Kaur, S., Singh, S., Kaur, M. et al. A Systematic Review of Computational Image Steganography Approaches. Arch Computat Methods Eng (2022). https://doi.org/10.1007/s11831-022-09749-0
2. Magdy, M., Hosny, K.M., Ghali, N.I. et al. Security of medical images for telemedicine: a systematic review. Multimed Tools Appl (2022). https://doi.org/10.1007/s11042-022-11956-7
3. Chhikara, S., & Kumar, R. (2021). Image steganalysis with entropy hybridized with chaotic grasshopper optimizer. Multimedia Tools and Applications, 80(21), 31865-31885. doi.org/10.1007/s11042-021-11118-1
4. Abood, M. H. (2017, March). An efficient image cryptography using hash-LSB steganography with RC4 and pixel shuffling encryption algorithms. In *2017 Annual Conference on New Trends in Information & Communications Technology Applications (NTICT)* (pp. 86-90). IEEE.
5. Jiang, N., Zhao, N., & Wang, L. (2016). LSB based quantum image steganography algorithm. *International Journal of Theoretical Physics*, *55*(1), 107-123.
6. Dixit, U. (2018). Cryptography–Security in E-Banking. *IOSR Journal of Business and Management*, *2*, 33-37.
7. Goldreich, O. (2019). On the foundations of cryptography. In *Providing Sound Foundations for Cryptography: On the Work of Shafi Goldwasser and Silvio Micali* (pp. 411-496).
8. Alotaibi, M., Al-hendi, D., Alroithy, B., Al Ghamdi, M., &Gutub, A. (2019). Secure Mobile Computing Authentication Utilizing Hash, Cryptography and Steganography Combination. *Journal of Information Security and Cybercrimes Research (JISCR)*, *2*(1).
9. Ye, D., Jiang, S., & Huang, J. (2019). Heard More Than Heard: An Audio Steganography Method Based on GAN. *arXiv preprint arXiv:1907.04986*.
10. Bai, S., Lepoint, T., Roux-Langlois, A., Sakzad, A., Stehlé, D., &Steinfeld, R. (2018). Improved security proofs in lattice-based cryptography: using the Rényi divergence

rather than the statistical distance. *Journal of Cryptology*, *31*(2), 610-640.

11. Meng, R., Zhou, Z., Cui, Q., Sun, X., & Yuan, C. (2019). A Novel Steganography Scheme Combining Coverless Information Hiding and Steganography. *Joural of Information Hiding and Privarcy Protection*, *1*(1), 43-48.
12. Jha, M. S., Maity, S. K., Nirmal, M. K., & Krishna, J. (2019). A Survey on Quantum Cryptography and Quantum Key Distribution Protocols.
13. Patel, N. A., & Patel, H. B. (2019). Analysis of Network Performance Using Aspect of Quantum Cryptography. *International Journal of Computer and Information Engineering*, *13*(9), 504-507.
14. Junlan Bai et al., "A high payload steganographic algorithm based on edge detection" in ELSEVIER, 2017, pp. 42-51, D.O.I https://doi.org/10.1016/j.displa.2016.12.004.
15. Her Chang Chao et al., "Generating Random Grid-based visual secret sharing with multi-level encoding" in ELSEVIER, Vol. 57, 2017, pp. 60- 67, DOI: http://dx.doi.org/10.1016/j.image.2017.05.005
16. Prof. Priyanka Bubna, Anshula Panchabudhe, Pallavi Choudhari, "Review on Implementation of Visual Cryptography and Steganography for secure authentication" in International Journal of Engineering and Technology (IRJET) Vol. 4, Issue: 2, 2017, pp. 510- 513, ISSN: 2395-0056, Available: https://www.irjet.net/archives/V4/i2/IRJET-V4I296.pdf .
17. J. Ida Christy and V. Seenivasagam, "Feed Forward Networks In Colour Extended Visual Cryptography To Generate Meaningful Shares", in International Journal of Security and Its Applications, Vol. 9, Issue: 1, pp. 165-178, 2015, DOI: http://10.14257/ijsia.2015.9.1.18
18. Souvik Roy, P. Venkateswaran, "Online Payment Using Steganography and Visual Cryptography" in IEEE Conference on Electrical, Electronics and Computer Science, 2014, DOI: http://10.1109/SCEECS.2014.6804449
19. Jonathan Weir et al., "Visual Cryptography and its Applications," © 2012, ISBN:978-87-403-0126-7, Available: https://books.google.com/books/.../Visual_Cryptography_and_Its_Applications.html
20. Xuehu Yan et al., "Halftone visual cryptography with minimum auxiliary black pixels and uniform image quality," in Conference on Digital Signal Processing, vol. 38, D.O.I https://doi.org/10.1016/j.dsp.2014.12.002, 2015, pp. 53–65.
21. Sana Siva et al., "Secure E- marketing Using Steganography & Emergence of Cryptography" in International journal of computer science & mobile computing (ijcsmc), Vol. 4, Issue: 1, 2015, pp. 532-538, ISSN: 2320–088X, Available: http://www.ijcsmc.com/docs/papers/January2015/V4I1201504.pdf
22. Priyanka More et al., " Online Payment System using Steganography and Visual Cryptography" in International Journal of Computer Engineering In Research Trends, Vol. 3, Issue: 4, 2016, pp. 157-161, ISSN: 2349-7084, Available: http://www.ijcert.org/issue_des.php?id=30 .
23. Bhoite Bhupali Vikas et al., "Online Secure Payment System Using Visual Cryptography and Steganography" in International Journal of Novel Research in Computer Science and Software Engineering, Vol. 3, Issue: 1, 2016, pp. 88-92, Available: http://www.noveltyjournals.com/download.php?file=Online%20Secure%20Payment%20System-547.pdf&act=book.
24. Mahsuna Abdul Sathar et al., "Secured E-Payment System Using Image Steganography and Visual Cryptography" in International Journal of Computer Trends and Technology (IJCTT), 2015, pp. 189-191, ISSN: 2231-2803, DOI: http://10.14445/22312803/IJCTT-V28P137
25. Swati Akolkar et al., "Secure Payment System using Steganography and Visual Cryptography" in International Journal of Computing and Technology, Vol. 3, Issue: 1, 2016, pp. 58-61, ISSN : 2348 – 6090, Available: https://www.ijcat.org/IJCAT-2016/3-1/Secure-Payment-System-using-Steganography-and-Visual-Cryptography.pdf .

26. Bhagyashri P. Kandalkar et al., "A Review Paper on Development of Visual Cryptography Technique for Authentication Using Facial Images" in International Journal of Science and Research (IJSR), Vol. 8, Issue :1, 2013, pp. 8-12, ISSN: 2319-7064, Available: https://www.ijsr.net/archive/v5i1/NOV152524.pdf .
27. T. Ambritha et al., "Visual Cryptography Scheme for Colored Image using XOR with Random Key Generation" in International Journal Of Engineering And Computer Science, Vol. 5, Issue: 4, 2016 , pp. 16281-16287, ISSN: 2319-7242, DOI: http://10.18535/Ijecs/v5i4.45
28. Sneha M. Shelke et al., "Prevention of Phishing Threats using Visual Cryptography and One Time Password (OTP)" in International Journal of Science and Research (IJSR), 2016, pp. 65-69, ISSN: 2319-7064, Available: https://www.ijsr.net/archive/v5i2/NOV153187.pdf .