International Journal of Signal Processing, Image Processing and Pattern Recognition
Vol.9, No.8 (2016), pp.169-180
http://dx.doi.org/10.14257/ijsip.2016.9.8.15

Comparison of Hybrid Security Schemes: A Survey

Ritesh Bansal[1], Atefeh Hediayti[2], Jitisha Aggrawal[3], Bhanushree Sorlan[4] and Shailender Gupta[5]

[1,3,5]YMCAUniversity of Science &Technology,Faridabad
[2]Garmsar Islamic Azad University, Iran
[4]Jamia Millia Islamia, New Delhi
[1]ritesh.bansal@hotmail.com, [2]atefeh_hedayati68@yahoo.com,
[3]jitisha27@gmail.com, [4]sorlanbhanushree1995@gmail.com,
[5]shailender81@gmail.com

Abstract

In today's age, communication through internet has become inseparable entity of many applications. These applications often require secrecy of data to be transmitted for security reasons. Therefore, commonly used security mechanisms such as cryptography and steganography can be employedto provide security, however using these techniques standalone often poses security threats. Therefore, a hybrid approach can be used for improving security features. In this paper comparison is drawn of recently published hybrid security mechanisms on the basis of following parameters: Visual assessment, Encrypted code Analysis, Similarity Analysis, Peak Signal Noise Ratio (PSNR), Information Entropy Analysis, Embedding Capacity Analysis, Key space analysis. The schemes are implemented and comparedusing MATLAB-2015.

Keywords: *Hybrid security mechanism,stegnography,cryptography,image hiding*

1. Introduction

Information plays a vital rolein any organization. As per requirement, sometimes it needs to be exchanged securely. This means defending information from unauthorized access, use, disclosure, disruption, modification, perusal, inspection, recording or destruction. Therefore, to maintain confidentiality and integrity of data, security mechanisms are employed.

The two widely used methods for security of data in are stegnography and cryptography. Steganography is the art which hides the existence of the communication [1]. Image steganography is most widely form of encryption. Images of any format can be used for encryption. The modified image doesn't show any major changes in terms of picture quality after the steganographic process and it can be passed as a simple image without arousing any suspicion. However, if some abnormality is detected in the stego image, then the message canbe easily extracted.

Cryptography involves converting a message text into a cipher message which is unreadable and lacks any meaning [1]. Many types of cryptographic schemes are used: public-key, private key and hash functions [2]. This process ensures confidentiality and ensures that only the intended recipient have access to the data. The cipher text *i.e.*, the encrypted text is easily visible and hence attackers are easily able to deduce that some secret communication is going on. As a result, this encrypted data has to face wide range of attacks [2]. A combination of cryptography and stegnography can be used, where both covers each other's disadvantages and improve the overall security. In hybrid mechanism [9-12] both cryptography and steganography are involved during the whole process (See Figure 1). The data is first encrypted using any encryption technique and then it is embedded in a cover image using steganography [3]. The cover image carrying the encrypted data is known as the stego image.

Figure 1, shows the basic architecture of Hybrid security mechanism. Basic functionality is as follows: Message is first encrypted using secret Key, and this encrypted cipher is then embedded into the cover file using stegnography technique, resulting in creation of stego image which contains secret data embedded into it. To extract the data reverse process is also depicted in figure. First ciphered data is extracted from stego image using reverse stegnography and then this ciphered data is decrypted using secret key and decryption scheme to obtain original data.

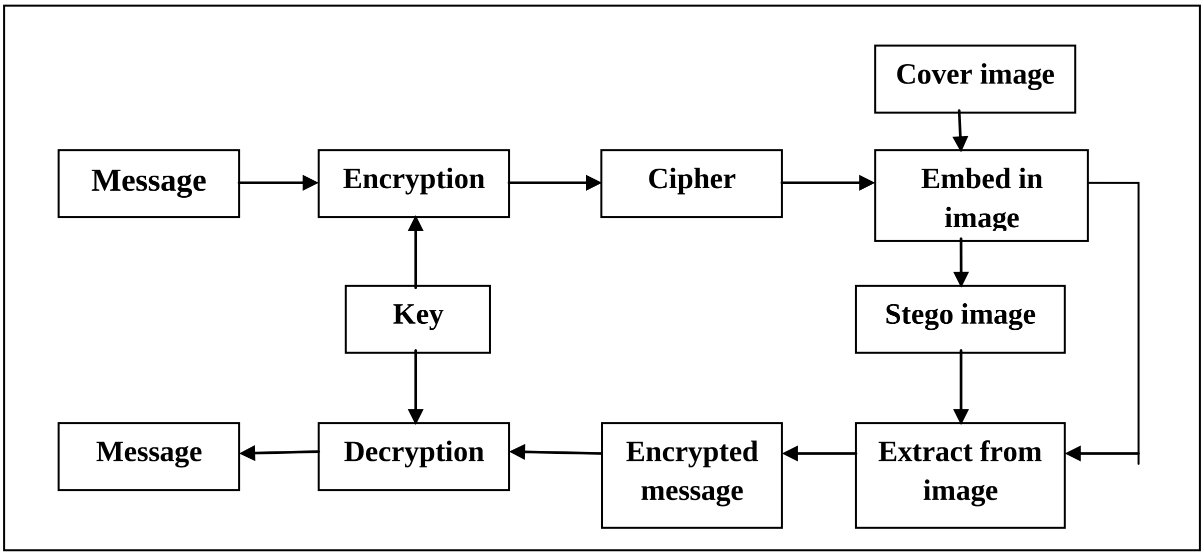

Figure 1. Hybrid Mechanism Block Diagram

The rest of the paper is as follows: Section 2, discusses the four hybrid mechanism schemes. Section 3 gives the description of the simulation parameters. The detailed results of various performance metricsare provided in Section 4 followed by a section of discussion of the best technique among the four and references.

3. Hybrid Security Schemes

The four recent hybrid schemes are taken for comparison. These are:

2.1. Divya Chaudhary*, et. al.,*

Divya Chaudhary *et. al.*, [4] scheme provides a higher level of security of data at an enhanced capacity [4]. The method consists of three steps:

- Compression: Huffmann encoding is used to encode the data. The more occurring symbols in the message are encoded with less number of bits than the symbols which occur less in the message. Less number of bits needed to be transmitted thus increasing the capacity of the message which can be sent.
- Encryption: Visual cryptography is used on the encoded message [6].The message is divided into n shares. All the shares are XORed together at the receiver end to create the message.
- Steganography: LSB steganography using status bit is used [6]. The message is encrypted either in the lighter areas or the darker areas of the image. These areas are identified by observing the MSB bits of the red, blue and green bytes of the image. For the lighter area the MSB must contain two 1 and for darker area two 0. The decimal representation of these three bits is obtained. The bit of the blue byte

at the position determined by this decimal number is checked with the message bit. If they are same then check LSB of the blue byte. If it is 1 complement it otherwise set it equal to the message bit. Also in case of darker area if decimal number is equal to 0 then LSB of the blue byte is set equal to the message bit.

At the receiver side reverse steps for the LSB steganography using status bit [6] is applied then the decryption process using the XOR operation is applied and finally the data is decompressed to obtain the message.

2.2. Md. Rashedul, *et. al.,*

Md. Rashedul, *et. al.,* [5] scheme used the combination of the AES encryption and the steganography to protect the data. This increases the PSNR and also the histogram shows changes which are negligible [5].

- AES encryption: It is a symmetric key algorithm [8]. The 128 bit key is used for the encryptionprocess. The message is divided into blocks of 16 bytes. The data is then passes through 10 rounds. The round consists of a substitution of bytes from a look-up table, shifting of rows in a certain number of steps and a mixing operation. The final round does not contain a mixing operation. This method converts the message into cipher text.
- Steganography: Same technique as used in the Divya Chaudhary, *et. al.,* [4].

2.3. Piyush Marwaha, *et. al.,*

Piyush Marwaha, *et. al.,* [6] scheme uses DES algorithm for converting the message into cipher text and then encrypting it in the image.

- DES encryption: It operates on 8 byte message block using a 8 byte key. The 8 byte key is first expanded to generate 16 keys of 8 bytes. Then the message passes through 16 rounds takes the message bytes and key bytes and performs the functions of XOR and byte substitution. At the end of these rounds cipher text is produced.
- Steganography: The RGB values of the image are changed according to the characters in the message. Reference database is used to hide the cipher text. A certain data grid is selected from this database and one pixel is modified for every byte in the cipher.The pixel value is changed to some predefined number and then the number representing of the character is added to it.The key is also sent to the receiver.

At the receiver's end the key is used to select the grid from the database. The cipher is obtained by subtracting the pixel value from the predefined number. The original message is retrieved by following the reverse steps of the DES encryption and also reversing the way keys are applied.

2.4. Peipei Shi, *et. al.,*

Peipei Shi, *et. al.,* [7] scheme uses a modified BPCS(Bit-Plane Complexity stegnography) improving the statistical analysis. It is also aimed at improving the safety of stegnography. In the original BPCS method the image was divided into 8 bit planes.Then the complexity of every block in the bit pane is determined and the maximum complexity is found out (Cm).Now the complexity threshold is set for a plane. The plane whose complexity is larger than the set threshold is used to hide the message. In the modified BPCS different thresholds is set for the different planes. The thresholds for same bit planes may not be even the same. This process reduces the probability of detecting the message by statistical analysis.

3. Simulation Parameters

The experiments are carried out on a personal computer using MATLAB. Table 1, is about the specifications of the experimental setup and initial values and parameters.

Table 1. Specification Table

SPECIFICATIONS	
Processor	1.4GHz dual-core Intel Core i5
Memory	4GB of 1600MHz LPDDR3
Programming Language	MATLAB
Version	2015
Size Of Images	64x64,128x128, 256 x 256 , 512 x 512,1024x1024
Images Type	Color Images
Initial Parameters	Values
Huffman encoding	Number of symbols n=26 Alphabets used are 'A to Z'
Data embedded	"ABCDEFABCDEFABCD"

4. Performance Metrics

To test the efficacy of the proposed scheme the following parameters were used:

4.1. Visual Assessment

It is one of the most important test, failing this test will result in total failure of whole scheme. It checks the similarity between the stego image and the cover image to ensure the impact of stego effect that may cause a suspicion in the mind of the hacker/ attacker. It can be seen clearly(see Table 2) that no visible changes can be seen in the stego images of compared schemes.

Table 2. Comparison of Stego Images of Various Schemes

Original image	Image after applying Peipei Shi *et. al.*, method	Image after applying Piyush Marwaha *et.al.*, method	Image after applying Md. Rashedul *et.al.*, method	Image after applying Divya Chaudhary *et. al.*, method

4.2. Encrypted Code Analysis

This is a test performed on the encrypted data, obtain after encryption process. Data to be embedded should be in such a form that unauthorized parties should not be able to deduce any meaningful information out of embedded data even if they are able to extract embedded data.It was observed that encrypted code is very different from Original data as no relation/deduction can be made(see Table 3).

Table 3. Encrypted Code

CryptographyTechnique	**Original Secret**	**Encrypted Data**	**Decrypted Data**
Divya Chaudhary *et. al.*, [5]	ABCDEFAB CDEFABCD	Üaá⍰@ (Share1) >x⍰,À (Share2)	ABCDEFABCDE FABCD
Md. Rashedul *et. al.*,	ABCDEFAB CDEFABCD	÷üjðK⍰hTMØ	ABCDEFABCDE FABCD
Piyush Marwaha *et. al.*	ABCDEFAB CDEFABCD	++sC|rÃP^«⍰{A	ABCDEFABCDE FABCD

4.3. Peak Signal Noise Ratio (PSNR)

Peak signal-to-noise ratio, often abbreviated PSNR, is a term for the ratio between the maximum possible power of a signal and the power of corrupting noise that affects the fidelity of its representation. The original plain image is considered as a signal and the Stego image is considered as a noise. PSNR is calculated as,

$$PSNR = 20 \times log_{10}(\frac{255}{\sqrt{MSE}})db$$

where MSE is,

$$MSE = \frac{1}{MN}\sum_{i=1}^{M}\sum_{j=1}^{N}(|I(i,j) - K(i,j)|)^2$$

where I(i, j) is the pixel value of the original plain image and K(i, j) is the pixel value of the encrypted image at location (i, j).This test is used to measure the quality of the stego image. Stego image is treated as noise in this test. It is clear (see Table 4) that peak signal to noise ratio of all the schemes are comparable to the each other. Divya Chaudhary, *et. al.*, [4] showing the best PSNR result among all.

Table 4. Comparison of PSNR of Proposed Scheme with Other Implemented Schemes

	Divya Chaudhary, *et. al.*, [4]	Md. Rashedul, *et. al.*, [5]	Piyush Marwaha, *et. al.*, [6]	Peipei Shi, *et. al.*, [7]
64	77.26470304	73.84047624	73.22777967	73.22778745
128	83.58493519	80.73257791	80.73257791	78.91838745
256	95.04621555	89.92738194	87.4495371	81.5033
512	98.01645325	94.99224212	93.66318857	84.73208745
1024	101.3471027	100.0977153	100.5552902	97.21644145

4.4. Similarity Analysis

It is used to measure the resemblance between input i.e. cover image and output *i.e.,* stego image. Below are the two tests which are performed in this section

4.4.1.Correlation Coefficient: This Correlation analysis is done to find relationships of current variable to its neighboring variable. Image pixels are treated as variable here. It is a measure of linear association between two variables. Range of the correlation coefficient is -1 to +1. A correlation coefficient of +1 indicates that two variables are perfectly related in a positive linear sense while a correlation coefficient of -1 indicates that two variables are perfectly related in a negative linear sense, and a correlation coefficient of 0 indicates that there is no linear relationship between the two variables. Correlation value of ‘0’ is a desirable effect.

$$r\alpha\beta = \frac{cov(\alpha,\beta)}{\sqrt{D(\alpha)}\sqrt{D(\beta)}}$$

$$E(\alpha) = \frac{1}{N}\sum_{i=1}^{N}\alpha_i$$

$$E(\alpha) = \frac{1}{N}\sum_{i=1}^{N}(\alpha i - E(\alpha)^2)$$

$$cov(\alpha,\beta) = \frac{1}{N}\sum_{i=1}^{N}(\alpha i - E(\alpha))(\beta i - E(\beta)))$$

Correlation analysis is done to check relationship among the pixels in stego image and original cover image. If image’s structure is not disturbed, then it should have high correlation. It is evident (see Figure 2) that correlation among pixels in stego and cover image is near its ideal value of 1 for Piyush Marwaha, *et. al.*, [6] and Peipei Shi, *et. al.*, [7] technique, thereby depicting that both are almost identical in structure.

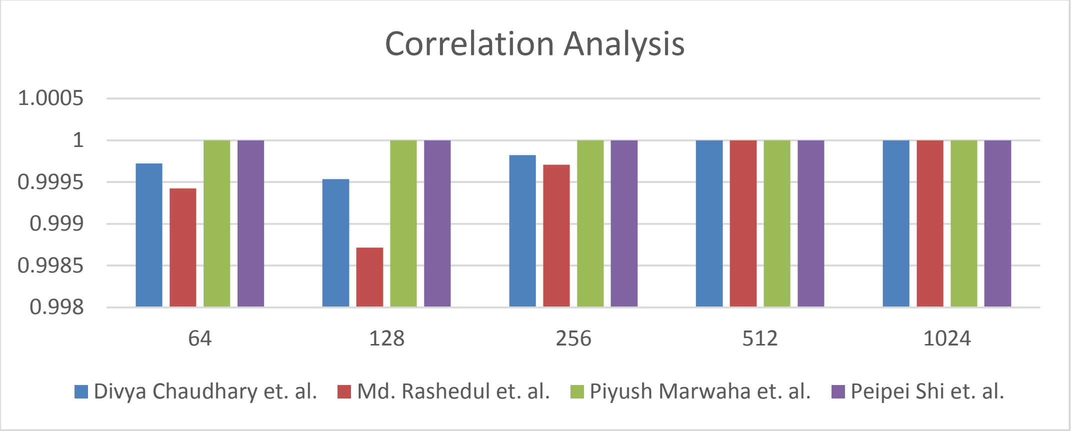

Figure 2. Comparison of Correlation Coefficients

4.4.2.Universal Image Quality Index (UIQI): In an image, pixels value available at different positions shows different effect on Human Visual System (HVS). If some distortion or changes is introduced in the image, such distortion in image is calculated as a combination of three factors loss of correlation, contrast distortion and luminance distortion.

Luminance distortion,

$$L(A,B) = \frac{2\ \mu_A \mu_B}{{\mu_A}^2 + {\mu_B}^2}$$

Contrast distortion,

$$C(A,B) = \frac{2\sigma_A \sigma_B}{{\sigma_A}^2 + {\sigma_B}^2}$$

Loss of correlation,

$$S(A,B) = \frac{2\sigma_{AB}}{\sigma_A + \sigma_B}$$

$$UIQI(A,B) = L(A,B) * C(A,B) * S(A,B)$$

Where A is cover image, μ_A and σ_A are mean and standard deviation, respectively of A. B is stego image, μ_B and σ_B is mean and standard deviation, respectively of B. σ_{AB} is covariance between A and B.Universal Image Quality Index (UIQI), which is a measure of image quality in terms of contrast, luminance and loss factor, provides very good results for proposed technique. It is clear(see Figure 3) that UIQI for the Piyush Marwaha, *et. al.*, [6] and Peipei Shi, *et. al.*, [7]scheme, is very close to the ideal value of 1.

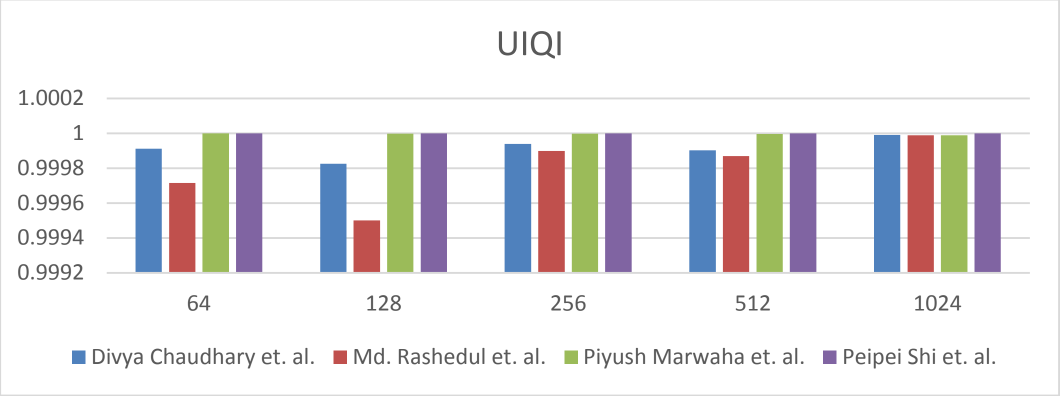

Figure 3. Comparison of UIQI

4.5. Information Entropy Analysis

Information entropy is a measure of randomness in encrypted output. Below is the mathematical formula used to calculate entropy.

$$H(S) = \sum_{i=0}^{n-1} P(S_i) log_2 \frac{1}{P(S_i)}$$

where Si represents the pixel values, P(Si) is the probability of the symbol Si and n is the total number of pixels, it’s value is 256 for gray scale images. Suppose that, the source emits 28 symbols with the same probability, *i.e.*, S = (S0, S1, S2, ..., S255) after evaluating above equation, entropy obtained is H(S) = 8. In this case Entropy of stego image should be as close to original as it can, reason being, probability of occurrence of pixels in stego image should be equal to the original’s one. They should be identical ideally.It is clear(see Figure 4) that entropy for all the schemes is very close to entropy values of original image thereby depicting that stego image of proposed scheme shows minimum change in pixels’ probability.

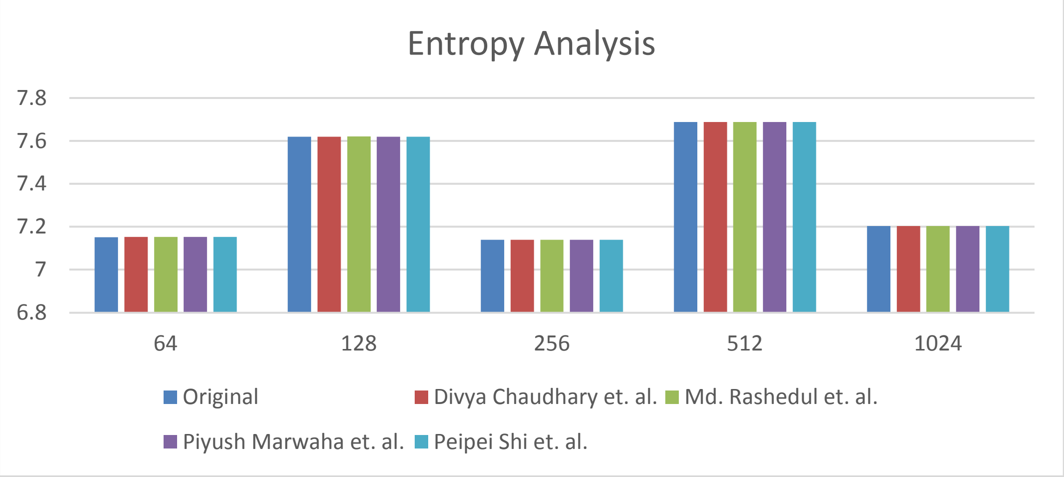

Figure 4. Comparison of Entropy

4.5. Embedding Capacity Analysis

Embedding capacity can be defined as the ratio of number of bits that can be embedded to the total number of bits. This analysis is basically used to test whether a technique is capable to embed a large amount of data or not. It can be seen clearly(see Figure 5) that expected embedding capacity of Peipei Shi, *et. al.*, [7]scheme is higher then its compared counterparts. Embedding capacity is calculated for proposed scheme on the basis of presence of potential complex blocks present in the testing images according to the proposed complexity measure and considering them for swapping with data blocks. Embedding capacity can be further increased by decreasing the threshold values if required

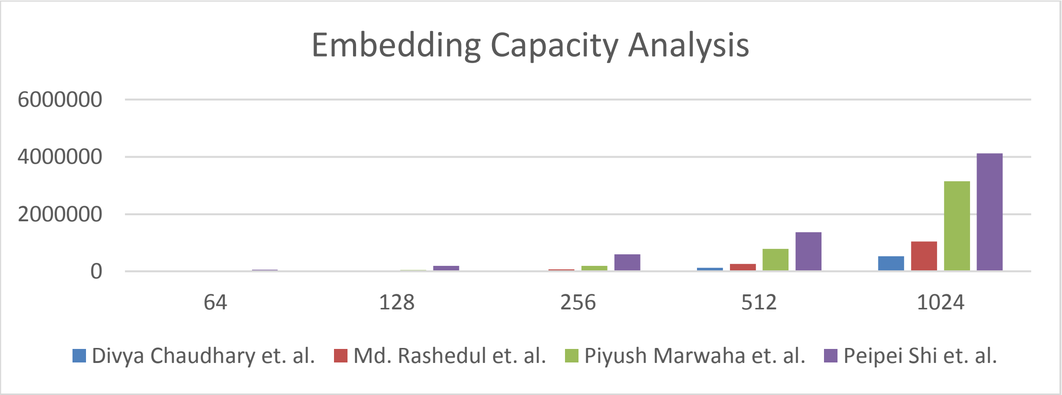

Figure 5. Comparison of Embedding Capacity

4.6. Key Space Analysis

Encryption should be very sensitive for a slight change in the value of key, as this will create a huge change in the encrypted output. Using a large key space ensures resistance of technique towards brute force attacks *i.e.*, breaking of algorithm by trial and error method to get the key by using automated software to generate a large number of consecutive guesses. Larger the key space, lower the possibility of this attack. So, for a scheme to be successful, key size should be large to get a large key space. A good encryption scheme should have a large key space as it is directly related with brute force attack.It can be seen clearly(see Table5) that Divya Chaudhary, *et. al.*, [4] scheme has variable key space depending upon the length of data, thereby showing that scheme can clearly resist brute force attacks.

Table 5. Key Space Analysis

Techniques	Divya Chaudhary, *et. al.*, [4]	Md. Rashedul, *et. al.*, [6]	Piyush Marwaha, *et. al.*, [5]	Peipei Shi, *et. al.*, [7]
Key size	Same as data length(say l)	128 bits	64 bits	No key
Key space	2^l	2^{128}	2^{64}	-

4.7. Time Complexity

It can be seen(see Figure6) that among the schemes compared, Piyush Marwaha, *et. al.*, [5] shows the best time complexity.

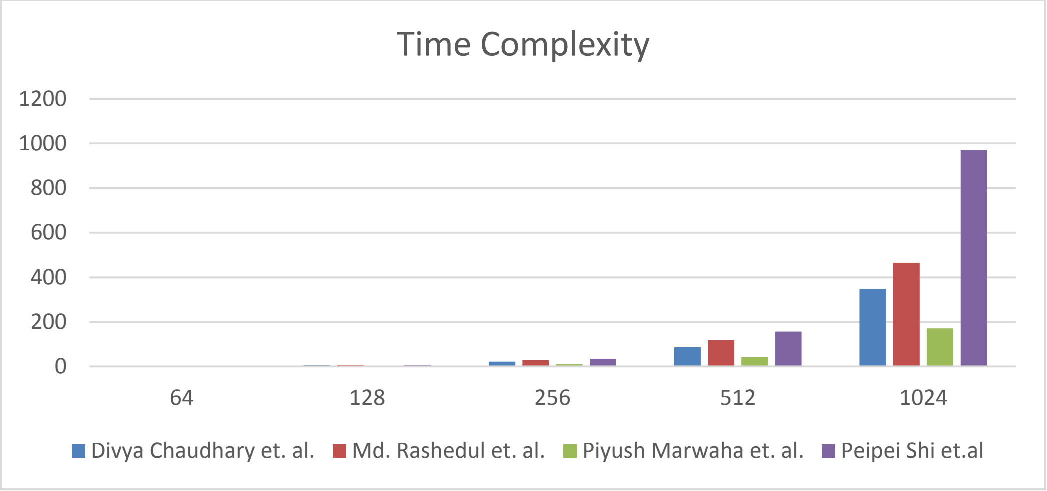

Figure 6. Comparison of Time complexity

5. Conclusion

The four Hybrid security schemes namely Divya chaudhary, *et. al.*, [4], Piyush Marwaha, *et. al.*, [6], Md. Rashedul, *et. al.*, [5] and Peipei Shi, *et. al.*, [7] have been compared on various parameters like Visual assessment, Encrypted code Analysis, Similarity Analysis, Peak Signal Noise Ratio (PSNR), Information Entropy Analysis, Embedding Capacity Analysis, Key space analysis. The overall result is analyzed(see Table 6).

Table 6. Overall Comparison

Parameters	**Divya Chaudhary, *et. al.*, [4]**	**Md. Rashedul, *et. al.*, [5]**	**Piyush Marwaha, *et. al.*, [6]**	**Peipei Shi, *et. al.*, [7]**
Encrypted Code	Unreadable and compressed	Unreadable	Unreadable	Unreadable
Key Space	Large and varying	Small and fixed	Small and fixed	No key space as there is no key
Correlation Coefficient	Higher	High	Highest	Highest
UIQI	Higher	High	Highest	Highest
PSNR	Highest	Higher	Lowest	Low
Embedding Capacity	Lowest	Low	High	Highest
Entropy	Comparable to original	Comparable to original	Comparable to original	Comparable to original

From table it’s clear that Divya Chaudhary, *et. al.,* provided the best overall results. It has the varying key space, correlation analysis shows that value of correlation is nearly equal to the ideal value of 1. Universal Image Quality Index analysis shows that when data is embedded into stego image, minimum changein terms of contrast, luminance and loss factor is experienced as value of UIQI comes out to be nealy equal to ideal value of 1. In terms of Image quality , it has the highest PSNR value calculated among among all compared schemes. The entropy of stage image calculated is comparable to that of original image depicting minimum change in frequency of pixel values.

References

[1] R. Nivedhitha and Dr. T. Meyyappa, “Image Security Using Steganography And Cryptographic Techniques”, International Journal of Engineering Trends and Technology, vol. 3, no. 3, **(2012)**, ISSN: 2231-5381.

[2] H. Rout and B. K. Mishra, “Pros and Cons of Cryptography, Steganography and Perturbation techniques”, IOSR Journal of Electronics and Communication Engineering (IOSR-JECE), pp. 76-81. ISSN: 2278-8735.

[3] D. Chaudhary, S. Gupta and S. Deswal, “Origin of Hybrid Security Mechanisms and Ways of Improvement”, International Journal of Big Data Security Intelligence, vol. 2, no. 2, **(2015)**, pp. 1-18. ISSN: 2205-8524.

[4] S. Gupta, K. D. Chaudhary, “ A NOVEL HYBRID SECURITY MECHANISM FOR DATA COMMUNICATION NETWORKS “, published in forth coming articles of International Journal of Information Privacy, Security and Integrity, **(2016)**.

[5] Md. R. Islam, A. Siddiqa, Md. P. Uddin, A. K. Mandal and Md. D. Hossain, “An Efficient Filtering Based Approach Improving LSB Image Steganography using Status Bit along with AES Cryptography”, Third IEEE International Conference on Informatics, Electronics and Vision, **(2014)**, pp. 1-6.

[6] P. Marwaha and P. Marwaha, “Visual Cryptographic Steganography in Images”, in proceedings of Second International conference on Computing, Communication and Networking Technologies, **(2010)**, pp. 1-6.

[7] P. Shi and Z. Li, “An improved BPCS Steganography based on Dynamic Threshold”, 2010 International Conference on Multimedia Information Networking and Security, pp. 388-391.

[8] W. Bender, D. Gruhl, N. Morimoto and A. Lu, “Techniques for data hiding”, IBM Systems Journal, vol. 35, no. 3-4, **(1996)**.

[9] B. Saha and S. Sharma, “Steganographic Techniques of Data Hiding using Digital Images”, in Defence Science Journal, vol. 62, no. 1, **(2012)** January, pp. 11-18.

[10] S. Goel, A. Rana and M. Kaur, “A Review of Comparison Techniques of Image Steganography”, IOSR Journal of Electrical and Electronics Engineering (IOSR-JEEE) e-ISSN: 2278-1676, p-ISSN: 2320-3331, vol. 6, no. 1, **(2013)** May-June, pp. 41-48.

[11] M. Taye and H. Shawky, “A Proposed Assessment Metrics for Image Steganography”, International Journal on Cryptography and Information Security (IJCIS), vol. 4, no. 1, **(2014)** March, pp. 1-11.

[12] S. Dhall, B. Bhushan and S. Gupta, “An In-depth Analysis of Various Steganography Techniques”, in International Journal of Security and Its Applications, vol. 9, no. 8, **(2015)**, pp. 67-94.