Security Measures to Image Steganography and Steganalysis: An Overview

[1]Dipankar Dey and [2]Sabyasachi Samanta

[1]Global Institute of Science and Technology, Haldia, India,

Email:deydipankar2014@gmail.com

[2]Haldia Institute of Technology, Haldia, WB, INDIA

E-mail id: sabyasachi.smnt@gmail.com

Abstract

Nowadays, the security system draws an important role to protect sensitive information from theft and implement data confidentiality, data integrity, authentication, and access controls. This article focuses on different parameters used to implement a security system in digital image processing. These parameters illustrate different mathematical and statistical analysis and state thestrongest point of an algorithm. These parameters are mainly used for image encryption, image steganography, image compression and Steganalysis etc. The optimized value of different analysis protects from different types of attacks such as Brute Force Attacks, Known plaintext Attacks, Statistical Attacks, Analytic Attacks, etc. The parameters are used to algorithm better which are Histogram Analysis, Information Entropy, NPCR, UACI, Correlations of two adjacent pixels, Key sensitivity, MSE, PNSR, NCC, AD, SC, MD, LMSE, NAE, SSIM, RMSE, etc. This article illustrates the application of these different statistical parameters on 512 × 512 grayscale and color images.

Keywords: Security parameters, Chaotic Map, Sensitivity analysis, Attacks, Steganalysis

1. Introduction

In digital communication, different sensitive - confidential information has been transferred among different authorized users. But the unauthorized users frequently try to hack such confidential information. The several methods such as DOS and DDOS attacks, Statistical Attacks, Brute Force Attacks, Plain - Text Attacks etc are applied to break the securitysystem. For this reason, it is essential to implement a security system to guard against these unauthorized users and makethe essential information secure. This article focuses onlyon security systems on digital images and discusses different parameters to protect against different attacks.

Different authors had been designed different algorithms related to digital image processing. Some of the algorithms related to image encryption-decryption algorithm, image steganography algorithm, image compressions, and image signal processing, etc. In each algorithm, the authors determinethe several statistical analysis and find out the optimize values which determines the algorithm's strongest point against statistical attack. The optimize values of different statistical parameters indicate that their algorithm are secure against different attacks.

One of the main parts of digital image processing is the image encryption algorithm. Here, image encryption means to change the original images (plain text) into meaningless images(cipher text) by using secret keys, and the same or inverse keysare used to decrypt the images. The different authors propose their models where they encrypt images by the strong secret keys. They generate random numbers with respect to each pixelvalue which are used as secret keys. They used different chaosfunctions, Arnold Cat map, intertwining logistic map, Rossler

Chaotic map, etc to generate such random numbers. Here, NPCR, UACI, Correlation coefficient, Information Entropy and Histogram are used to measure the security system of the image.

The second part of the digital image processing is the image steganography. In this method, the secret information is concealed within the images. Here, information may be text message, image or any other important files which are embedded within an image. Then image pixels are scrambled by different permutation process which make the algorithm is stronger. The securities of the image are measured by different statistical parameters. Here, SSIM, PSNR, MSE etc are used to determine the security of information which is embedded within an image.

The Third parameter of the digital image processing is the image compression. In this method, the size of the original image is reducing in such way that all pixel intensities are preserved. During the decompression process the converted image back to the original size. The Wavelets method, Run length method, JPEG method, DCT method, etc are the some common algorithms are used to implement image compression.The compression ratio, PSNR, MSE etc are used to determine the effectiveness of the compression algorithm.

The Fourth part of this article is the Steganalysis. This method focuses on how to trace embedding information inside an image. To do this, the different technique has been discussed in this article. Some techniques of Steganalysis are Visual Detection, Image Quality Metrics, Similarity measure on binary images, RA Analysis etc.

There are many more applications of digital image processing out of which only four techniques are discuss in this article. This paper is designed as follow: Section 3 focus on contribution of this article, Section 4 illustrates the related papers, Section 5 discusses the Statistical and Security analysis of image encryption, Steganography, Steganalysis and Section 6 concludes of this article.

1.1Contribution of This Study

This article focuses on different statistical parameters of thedigital image processing. All these parameters are examined onthe 512 × 512 standard grayscale and color images.

1. This article focuses on security measure of the different statistical parameters and find out the optimum valeswhich are useful.

2. This article focus on the different techniques is used to generate the random numbers.

Table 1: NOMENCLATURE

Term	**Usage**
μ	a Threshold value i.e., $3.57 \le \mu \le 4$
$\lfloor\ \rfloor$	Floor function
$\oplus$	Bitwise xor operation
dx	Change in the value of x
dx	Change in the value of y
W	Column of the image
H	Row of the image
X_0	Initial value of the chaotic map
X_i	i-th value of the chaotic map
P_i	i-th pixel's intensity value
$C_i^{'}$	i-th pixel's modified intensity value
$C_i^{''}$	i-th pixel's modified intensity value
$H(S)$	Entropy
L	Total number of pixels

q_1, q_2, q_3, q_4	Secret keys
K_1, K_2, K_3, K_4	Secret keys
d	Decision parameter
r	Correlation coefficient
M_1 and M_2	Polynomial Matrices
M_1^{-1} and M_2^{-1}	Inverse Polynomial Matrices

1.2 Road Map of This Work

Section 2 describes the literature review of some scheme. The preliminaries of this scheme are illustrated in Section 3. The security measures is shown in Section 4. The last Section 5 describes the conclusion of this scheme.

2. **Literature Review**

Kanso et al. [1] describe a nobel chaos map based image encryption model which was suitable for medical. This model consist of several rounds and each round contains two phase : shuffling phase and masking phase. To implement the securitysystem of this model, they design pseudorandom matrix. The size of this matrix was same as image size and this matrixwas implementing the masking phase of the proposed model. According to the output of chaos map, the pixel values were scrambled. By different security analysis, they proposed that their model was secured against different cryptanalysis attacks.The different parameters which was used in the proposed model show the optimal values. These optimized values indicate that the model had strongest security system.

Jawad et al. [2] present a new color image encryption modelwhere they implement the security system using Blowfishmodel. In this model, they generate a special *F* function using this Blowfish model. The *F* function generate the four dimensional chaos map and then this chaos map, *S* box and *XOR* operation implement the proposed model. They test theiralgorithm on 512x512 different standard color images. The several statistical analysis proves that the strength of this model.

Chen et al. [3] describes an optical image encryption algorithm where they used 3-D chaos map which jointly scrambled and randomly encoding domain. Here, the domain name is gyrator domain. They use the permutation approach and designthe confusion architecture and shuffle the image. Then, they scrambled the image by using random phase encoding andthe gyrator domain. The 3-D chaos map generate the random domain. They ensure that their model was secure against different statistical attack by different cryptography analysis.

Hongjun et al. [4] describes a color image encryption modelbased on strongest chaotic map and one time key generations. They use the linear piecewise chaos functions to generate the sequence of random keys. They also use the MD5 (Message -digest algorithm) to generate the random keys to control the mouse position which ensure that the algorithm has the high level entropy. They use the perturbation function to implement the initial parameter of the key stream generation. All these features make their model strangers and they get the optimize value of NPCR and UACI. All others parameters of security analysis indicate that the strongest security system againstseveral statistical attacks.

Mukherjee et al. [5] was presenting a new image steganography process by using the mid position value. In this method, they hide the secret data inside an image. Here, Arnold transformation had been used to cover the image as a first stage. The hide the data from the MPV (mid position value) position and then scrambled image by Arnold transformation. The inverse Arnold transformation had been used to retrieve theoriginal data.

All the security analysis shows the satisfied result and they protect the sensitive data against statistical attacks.

Jeevan et al. [6] proposed an image steganography algorithmusing pseudo hexagonal image. In this method, they represent pixels of the image as a hexagonal shape. They hide the secrete data inside the hexagonal shaped pixel's image. Here, hexagonal structure used as a cover file of the secrete data. Themean square error between the cover image and original imageshows the significant result.

Kasapbasi et al. [7] illustrate a new LSB based color image steganography algorithm. In this method, they hide the secrete data by using different techniques which are AES, CRC-32 checksum, Fisher-Yates Shuffle algorithm etc. In this method, to get the better histogram analysis, they use the LSB and Chi - square analysis. Here, LSB method helps to get better payload capacity and increase security system of this algorithm.

Emad et al. [8] describes an image steganography algorithmusing the LSB (Least significant bit) and IWT (Integer wavelet transform) methods. They take IWT based cover image and the secret data was concealed inside the image by using LSB method. By the inverse IWT methods and LSB transformation, they successfully retrieve the hidden informa- tion. The several parameters such as MSE, PSNR, payload capacity, NCC etc had been compare with their algorithm. They was demanding that their algorithm was secure against statistical attacks and all statistical parameters was evaluating optimize value.

Joshi et al. [9] describes an image steganography algorithm using the sequence of 7 bits pixels. This algorithm had been implemented on the grayscale images. They hide the secret data bitwise. First bit had been hidden in randomly selected pixel 1, the 2nd bit hidden in corresponding next pixel values that is pixel+1 and so on. In this way, 7 bits of the selected pixels and 7 bits +1 for next pixels was used for hiding information inside the grayscale images. Using the reverse process, they also extract the same information. The different parameters such as MSE, PSNR etc show the significantresults.

Watters et al. [10] describes this algorithm where they embedhidden information inside a color natural image. They hide themessages into the "least significant bits" of the images. The different statistical features also show that the hidden informationis protected inside the image from the different types of attacks.

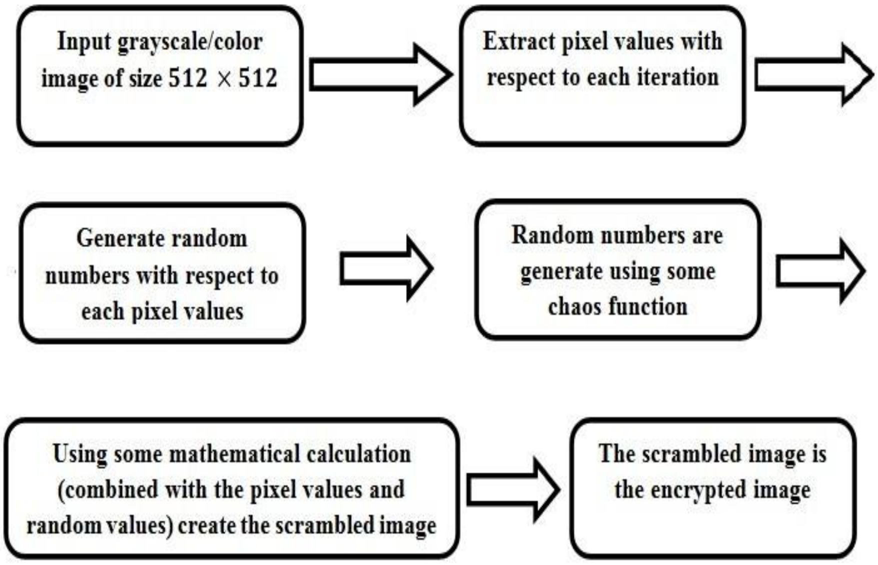
Input grayscale/color image of size 512 × 512
Extract pixel values with respect to each iteration
Generate random numbers with respect to each pixel values
Random numbers are generate using some chaos function
Using some mathematical calculation (combined with the pixel values and random values) create the scrambled image
The scrambled image is the encrypted image

Figure 1: Block diagram of the Image Encryption

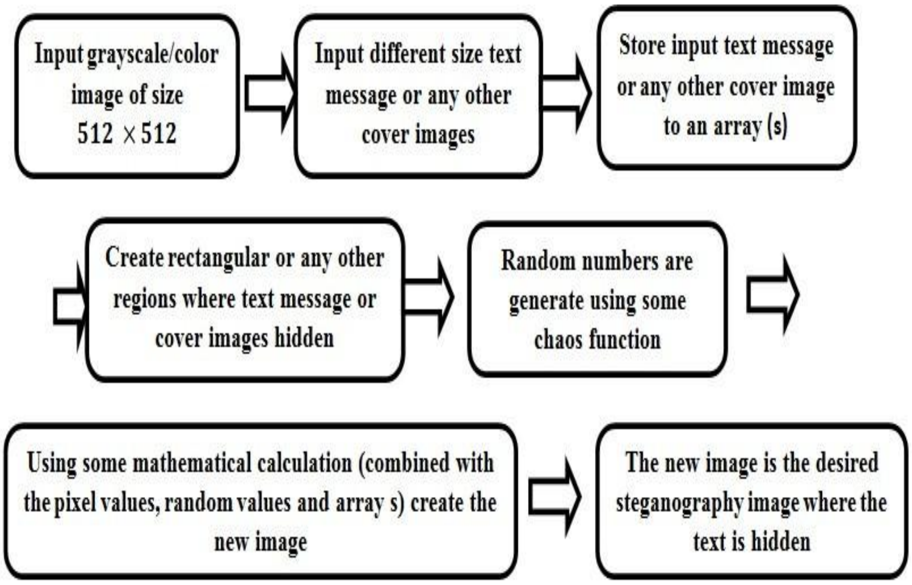
Input grayscale/color image of size 512 × 512
Input different size text message or any other cover images
Store input text message or any other cover image to an array (s)
Create rectangular or any other regions where text message or cover images hidden
Random numbers are generate using some chaos function
Using some mathematical calculation (combined with the pixel values, random values and array s) create the new image
The new image is the desired steganography image where the text is hidden

Figure 2: Block diagram of the Image Encryption

3. Background

This section focus on the different parameters that are used in this scheme. Table 1 describes the different symbols which are used in this scheme.

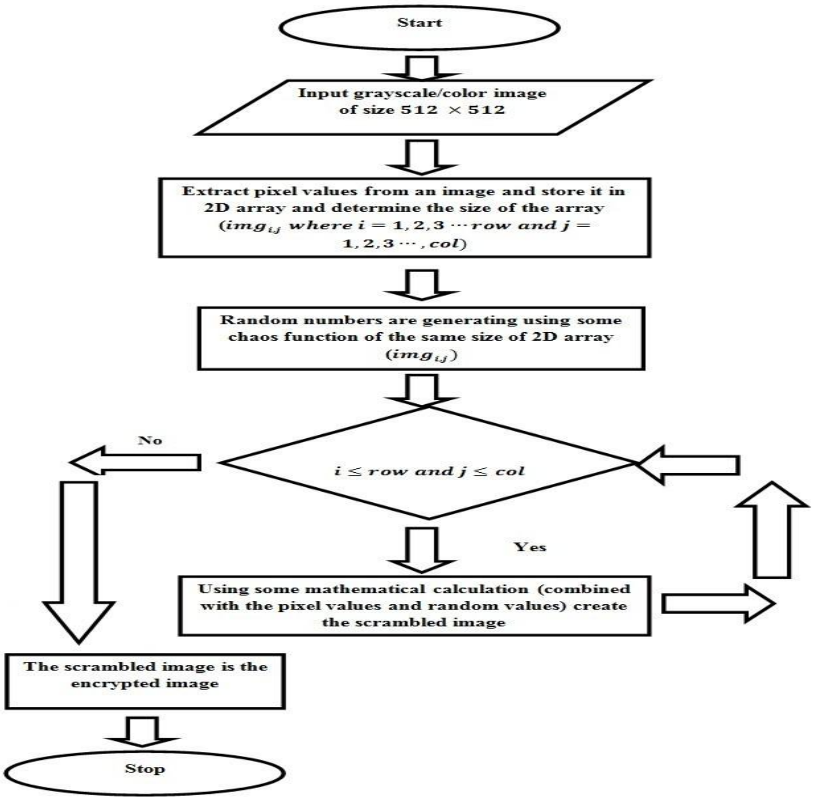
Start
Input grayscale/color image of size 512 × 512
Extract pixel values from an image and store it in 2D array and determine the size of the array ($img_{i,j}$ where $i = 1,2,3 \cdots row$ and $j = 1,2,3 \cdots, col$)
Random numbers are generating using some chaos function of the same size of 2D array ($img_{i,j}$)
$i \leq row$ and $j \leq col$
No
Yes
Using some mathematical calculation (combined with the pixel values and random values) create the scrambled image
The scrambled image is the encrypted image
Stop

Figure 3: Block diagram of the Image Encryption

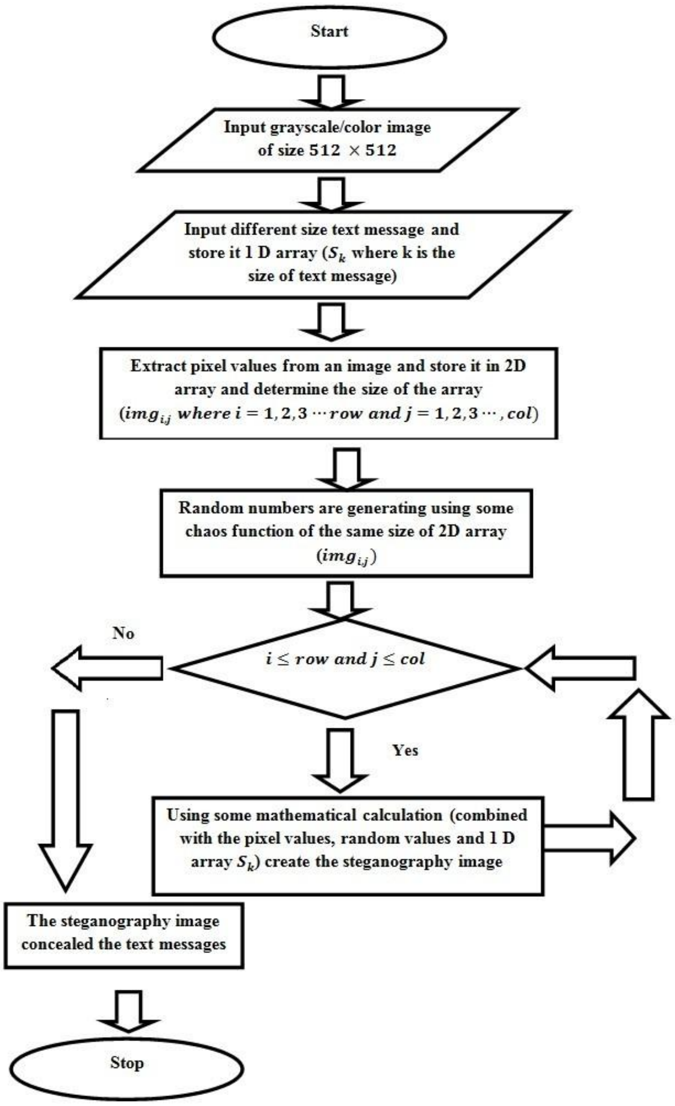
Start
Input grayscale/color image of size 512×512
Input different size text message and store it 1 D array (S_k where k is the size of text message)
Extract pixel values from an image and store it in 2D array and determine the size of the array ($img_{i,j}$ $where\ i = 1,2,3 \cdots row\ and\ j = 1,2,3 \cdots, col$)
Random numbers are generating using some chaos function of the same size of 2D array ($img_{i,j}$)
No
$i \leq row\ and\ j \leq col$
Yes
Using some mathematical calculation (combined with the pixel values, random values and 1 D array S_k) create the steganography image
The steganography image concealed the text messages
Stop

Figure 4: Block diagram of the Image Steganography

4. Statistical and Security analysis

The statistical and security analysis is the powerful feature of the image encryption algorithm and image steganography algorithm. These parameters are used to examine an algorithm which is more powerful against several statistical attacks. In Image encryption algorithm, these parameters help to design the confusion-diffusion architecture of the scheme. In image steganography algorithm, these parameters are used to determines the quality of the cover image. Here, this article illustrates different parameters which are essential to design an image encryption algorithm and image steganography algorithm.

4.1 Security Measures

Here, SSIM, MSE, PSNR, RMSE etc. are the essential parameters which are used to determine the quality of the image with respect to image steganography algorithm. These parameters illustrate that how to derive high quality images. The different parameters are described below:

(a) The Structural Similarity Index is the conceptual parameters that determine the image quality with respect to data compression or image steganography. To determine the SSIM parameters, the method requires two images:

one is input image and other is steganography / compressed images which can be found from image compression or image steganography. The SSIM value is determined by the parameter *r*. The equation of the SSIM 4.1 value can bewritten as:

$$r = \frac{\Sigma(C_i - \bar{C})(S_i - \bar{S})}{\sqrt{\Sigma(C_i - \bar{C})^2}\sqrt{\Sigma(S_i - \bar{S})^2}}$$ ……………….…..(4.1)

where C_i, S_i are the original and steganography images, and ¯C, S¯ are the mean value of the images respectively. The approximate value of SSIM can be found as 1 if there are no noise between two images.

(b) The full form of the PSNR is the"Peak Signal to Noise Ratio". This ratio is used to measure the quality of the images between the cover images and the steganography images. This parameters determines the accuracy between the coverimage and the steganography image. The full form of the MSE is the "Mean Square Error". The MSE value can be found when there is comparison between the cover image and the steganography / compressed images. The MSE represents "Cumulative Square Error" between the cover image and the steganography / com- pressed images. The minimum value of the MSE indicatesthat the lower error between images. The equation of the MSE 4.3 can be defined as:

$$PSNR = \frac{10\log_{10}\left(255^2\right)}{MSE} db$$

………………..(4.2)

© The full form of the MSE is the"Mean Square Error". The MSE value can be found when there are comparisons between the cover image and the steganography / compressed images. The MSE represents"Cumulative Square Error" between the cover image and the steganography / com- pressed images. The minimum value of the MSE indicatesthat the lower error between images. The equation of the MSE 4.3 can be defined as:

$$MSE = \frac{1}{M \times N}\sum_{i=1}^{M}\sum_{j=1}^{N}[C_{ij} - S_{ij}]^2$$

………………..(4.3)

(d) Here, C_{ij} is the cover image and S_{ij} is the steganographyimages. The full form of RMSE is the "Root Mean Square Error". RMSE is the error between the cover images and the steganography images. It is the average squared difference among the pixels in the cover image and the steganography image. It evaluate the volume of alteration per pixel between the cover image and the steganography image. When the MSE and RMSE close to 0, it can be consider that there are no difference between these two image, that is , the cover image and the steganography images. Hence, the both images are same. The equation of the RMSE 4.4 can be defined as:

$$RMSE = \sqrt{MSE}$$ ……………….(4.4)

(e) The AD or average difference between the cover image and the steganography image is defined as the sum of the difference between each pixel. The AD 4.5 value can be defined as:

$$AD = \frac{1}{M \times N}\sum_{i=1}^{M}\sum_{j=1}^{N}(C_{ij} - S_{ij})$$

…………..(4.5)

where M, N are the number of pixels of the cover image (Ci j) and the steganography image (S i ,j). The 0 value for MSE refers perfect similarity and a AD > 1 indicates less similarity and will give optimize value as the AD between intensities of pixels increases as well.

(f) The MD or maximum difference 4.6 between the neighbourhood pixels can be defined as:

$$MD = max(C_{ij} - S_{ij})$$

…………….(4.6)

where i = 1,2,3,…….. M and j = 1,2,3……..N. This parameter also determines the maximum error present between the cover image (Ci j) and the steganography image (S I, j). So, the minimum value of MD indicates that both the cover image and the steganography image are almost same.

(g) The quality of image also determines using one of the essential parameter which is Normalized Absolute Error or NAE. The equation of the NAE 4.7 can be defined as:

$$NAE = \frac{\sum_{i=1}^{M}\sum_{j=1}^{N}\left(|C_{ij} - S_{ij}|\right)}{\sum_{i=1}^{M}\sum_{j=1}^{N}\left(C_{ij}\right)}$$

……………..(4.7)

This parameters determines the difference between the cover image (Ci j) and the steganography image (S i j). It is also indicates that the numerical variance between two images. The result of NAE are defined within (0; 1). If the value of NAE is 0, it indicate that image is high quality and if the value is 1, indicates that the quality of the image is poor.

(h) The full form of the NCC is the ”Normalized Cross Cor- relation” between the cover image and the steganography image. This parameters makes the per pixel comparison between two images. The equation of the NCC 4.8 can be defined as:

$$SC = \frac{\sum_{i=1}^{M}\sum_{j=1}^{N}\left(C_{ij}\right)^2}{\sum_{i=1}^{M}\sum_{j=1}^{N}\left(S_{ij}\right)^2}$$

…………………(4.8)

(i) The NCC determines the degree of similarity between the cover image ($C_{i\ j}$) and the steganography image ($S_{i\ j}$). The main point of the NCC with respect to the ordinary cross correlation is that it is less sensitive to linear changes in theamplitude of illumination between two different images.

The NCC value ranges between (–1, 1).

(j) The full form of SC is the ”Structural Content”. The SC value determines the quality of the image. The maximum value of SC indicates that the image is poor quality and minimum value of SC indicates that the image has high quality. The equation of the SC 4.9 can be written as

$$SC = \frac{\sum_{i=1}^{M} \sum_{j=1}^{N} \left(C_{ij}\right)^2}{\sum_{i=1}^{M} \sum_{j=1}^{N} \left(S_{ij}\right)^2} \quad \text{.........(4.9)}$$

Here C_{ij} and S_{ij} are the cover image and the steganographyimage respectively.

4.2 Information Entropy, Key Sensitivity, NPCR, UACI and Correlation Coefficient

The security system of an image encryption algorithm is determines by several parameters. These parameters are used to illustrate to make a scheme better against statistical attacks. The different parameters of the statistical analysis are describe below:

(a) Information entropy (IE) is one of the essential feature of the statistical analysis. The IE describes the amount of information contained within the image. The IE also evaluate the degree of disorder between the meaningful image and the cipher image. If the value of the information entropy is nearest to the value of 8, then the images have the high disorder between plain image and the cipher image. Using the value 8, this tool determines the 28 gray level values. Mr. Shannon in 1949 had been invented the information entropy concept where he had defined some mathematical rule of the IE 4.10 which is

$$H(S) = \sum_{i=0}^{2^L-1} P(S_i) \log_2 \frac{1}{P(S_i)}, \quad \text{...(4.10)}$$

where P(S i) is the source image’s probability, S i is the summation of the pixels, L is the gray level of the image and H(S) defines the information entropy.

(b) Key sensitivity one of the main features of the image encryption. In cryptography, an algorithm should be sensitive to its secret keys. Since an attacker always tries to find the small clues by using different technique and if he/she finds some clues, then he/she break the security system of the scheme. If the keys are generated randomly, then it is impossible to crack the security of the scheme and the attacker unable to recover the meaningful information from the encryption scheme.

Where× W H (here, H is row and W is column) defines the size of the image, the maximum intensities of the pixel indicate by L and C_1, C_2 are two encrypted images. After encryption, the intensities between the plain image and the cipher images are huge changes which refer the disparities properties of the plain image and the cipher image.

Another important feature of the statistical tool is the cor- relation coefficient (CC). Here, CC are used to determinesthe strongest relationship between the neighborhood pix- els of the plain image and the cipher image. The plain image has the higher pixel relationship that means its CC value is maximum. But, in the cipher image, this strongestrelationship between the neighborhood pixels is not pre- serve. At that time, the value of the CC is minimum. The proposed value of CC ranges between (-1,1). An image encryption algorithm determine correlation values in three ways that is the ”x-direction (horizontal) correlation, the y-direction (vertical) correlation and the z-direction (diag-onal) correlation”. The following equation 4.13 determines

4.3. Steganalysis

There are different Steganography algorithms using which some sensitive information has been embedded inside an image. Depending on this concept, images can be divided into two parts: 1) cover-object and 2) stego-object. The cover object is the object that does not contain any secret information whereas the stego object contains the secret information inside an image. In this context, Steganalysis is a set of techniques that try to find such hidden information inside an image. The different Steganalysis techniques have been described as follows:

(a) Visual Detection [10]: It is possible when the embedding secret information inside an image is visible to the eye and it is easily recognized able to the difference between the cover image and the stego image. This technique is also called known carrier attack. However, it will not be possible to detect the difference between stego image and self noise image.

(b) Image Quality Metrics [11]: Steganalysis is based on various Image Quality Metrics. The different predictions from these metrics, it is determined the embedding of secret information inside an image.

(c) Similarity measure on binary images [12]: In this method, the similarity is measured between two binary images. The different statistical feature examines the lower order bit plane for the presence of embedding hidden information. It is possible that alter the pixel intensity using a steganography algorithm. The similarity measure on binary image checks the intensity of the neighbourhood pixel and then determines that whether any hidden information is present on the image or not.

(d) Histogram Difference: Histogram of the cover image and stego image shows some significant differences between the two images that help to trace embedding information present inside an image. In the steganography process, the least significant bits of the cover image may be changed, and also the pixel values of the cover image maybe change during embedding secret information inside an image. For this reason, if the histogram of both the cover image and stego image is examined, it shows some significant differences between the two.

(e) Bit plane analysis: This technique can trace the presence of embedding information inside a cover image. This technique focuses on the correlation coefficient value between the cover image and the stage image. Since the structural properties of the pixel of the cover image may be changed due to embedding information inside an image, the correlation coefficient values refer to that result.

(f) RA Analysis: This technique describes that the hidden in- formation is randomly scattered throughout the stego image. For this reason, relationships between the LSB plane and the cover images pixels are low. From this weak relationship, it can be determined that there is some embeddinginformation inside a cover image.

5. Conclusion

This paper dictates an extensive review of different algorithms. This article focuses on different statistical analysis of image encryption and image steganography. This article also focuses on Steganalysis concept and "Visual Detection", "Bit plane analysis", etc are some techniques of Steganalysis. The strongest security analysis state that an algorithm is secureagainst different types of attacks was as Steganalysis states how to trace hidden information inside an image.

References

[1] A. Kanso,M. Ghebleh, “An efficient and robust image encryption scheme for medical applications”, Commun Nonlinear Sci Numer Simulat, Vol. 24, pp. 98-116, 2015.

[2] L. M. Jawad, G. Sulong, “Chaotic map-embedded Blowfish algorithm for security enhancement of colour image encryption”, Nonlinear Dynamics, Vol. 81, pp. 2079-2093, 2015.

[3] J. X. Chen, Z. L. Zhu, C. Fu and H. Yu, “Optical image encryption scheme using 3-D chaotic map based joint image scrambling and random encoding in gyrator domains”, Optics Communications, Vol. 341, pp. 263-270, 2015.

[4] L. Hongjun and W. Xingyuan, “Color image encryption based on one-time keys and robust chaotic maps”, Computers and Mathematics with Applications, Vol. 59, pp. 3320-3327, 2010.

[5] S. Mukherjee, S. Roy and G. Sanyal, “Image Steganography Using Mid Position Value Technique”, International Conference on Computational Intelligence and Data Science, Vol. 132, pp. 461-468, 2018.

[6] K. M. Jeevan and S. Krishnakumar, “An Image Steganography Method Us- ing Pseudo Hexagonal Image”, International Journal of Pure and Applied Mathematics, Vol. 118, pp. 2729-2735, 2018.

[7] M. C. Kasapbasi and W. Elmasry, “ New LSB-based colour image steganography method to enhance the efficiency in payload capacity, se- curity and integrity check”, pp. 43-68, 2018.

[8] E. Emad, A. Safey, A. Refaat, Z. Osama, E. Sayed and E. Mohamed, “A secure image steganography algorithm based on least significant bit and in- teger wavelet transform”, Journal of Systems Engineering and Electronics,Vol. 29, pp. 639-649, 2018.

[9] K. Joshi, S. Gill and R. Yadav, “A New Method of Image Steganography Using 7th Bit of a Pixel as Indicator by Introducing the Successive Tempo rary Pixel in the Gray Scale Image”, JJournal of Computer Networks and Communications, Vol. 2018, Article ID 9475142, pp. 10 pages, 2018.

[10] P. A. Watters, F. Martin and S. H. Stripf, ”Visual steganalysis of LSB- encoded natural images”, Third International Conference on Informa- tion Technology and Applications (ICITA’05), Vol.1, pp. 746-751 , doi: 10.1109/ICITA.2005.308, 2005.

[11] I. Avcibas, N. Memon and B. Sankur, “Steganalysis using image quality metrics”, in IEEE Transactions on Image Processing, Vol. 12, No. 2, pp. 221-229, doi: 10.1109/TIP.2002.807363, 2003.

[12] I. Avcibas, N. Memon and B. Sankur, “Image steganalysis with binary similarity measures”, Proceedings. International Conference on Image Processing, Vol.3, pp. 645-648 , doi: 10.1109/ICIP.2002.1039053, 2002.