IJISET - International Journal of Innovative Science, Engineering & Technology, Vol. 6 Issue 4, April 2019
ISSN (Online) 2348 – 7968
www.ijiset.com

Cloud privacy protection based on reversible data hiding and chaotic approach

G A Navya
M.Tech Student
Electronics and Communication Engineering
Jain University
Bangalore, India
Navyagondi222@gmail.com

Dr. Sukumar
Associate Professor
Electronics and Communication Engineering
Jain University
Bangalore, India
rsugumdevi@gmail.com

***Abstract*— In today's world, large amount of data communication happens over the internet. In all aspects, securing the data becomes a challenging issue. The hiding of data into image provides more security as well as tried to improve embedding capacity. At the point when the measure of data to be inserted into the image expands it can adversely influence the image quality making it unacceptable for specific applications. The important concern for data hiding into images is its greater visual feature, increased hiding capacity etc. In this project, a data hiding and encryption method proposed for images. At first, data is hidden using reversible data hiding method. Second, proposed a chaotic image encryption approach to change stego image into encrypted image using confusion and diffusion process. The outcome of our project gives more security to protect data and that has been shown using security analysis factors comparing with existing methods which are not able to survive for present attacks.**

Keywords- Image Steganography, Henon and Lorentz Map, Confusion and Diffusion Process, Reversible data hiding.

I. INTRODUCTION

In today's world, communication is achieved in a faster rate compared to past. But will get vulnerable data due to added information in between the source and destination. Hence security is the main concern, as a part of it will have both encryption from sender side and decryption from receiver side.

The advancement of Information and Communication Technology (ICT) plays a significant role in society; it draws noteworthy consideration towards security and honesty of information. Be that as it may, presently the meaning of passing secret information in a customary manner is currently changed. ICT drives specialists to create applications which are utilized to impart subtly. There are different advances which are utilized for Information stowing away, for example, Steganography and Cryptography. These are well known strategies accessible for data security which in terms helps to acts as a prime concern while conveying on net. Web is an open asset for all, so this innovation is particularly valuable to transmit information from one end to other in all respects effectively and rapidly. In this way data security draws consideration of specialists, government offices; legislators, military, insight organizations just as culprits who require continuous correspondences. They are keen on understanding these advancements and their shortcomings, in order to recognize and screen shrouded messages. A few governments carefully limit web free conversation and the regular citizen utilization of cryptography has made individuals worried about autonomy to create systems for undesirable interchanges on the net, including unethical programmers and Web intermediaries. Advanced Images are electronic previews taken of a scene or filtered from reports, for example, photos, compositions, printed writings, and work of art. The computerized picture is tested and mapped as a matrix of spots or picture components (pixels). Every pixel is appointed a tonal esteem (dark, white, shades of dim or shading), which is spoken to in paired code (ones). The paired digits ("bits") for every pixel are put away in a grouping by a PC and regularly decreased to a numerical portrayal (compacted). The bits are then deciphered and perused by the PC to deliver a simple adaptation for showcase or printing.

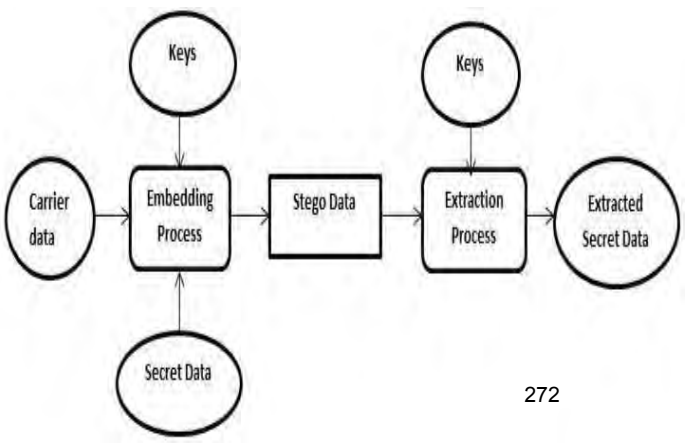


Fig 1. Steganographic Process

The steganography is a discipline or ability of covering information to available source of data say for example documents, texts, video or audio, images so on. Hence we cannot able to predict and get the data easily by unauthorized person [5]. The three components play a major role while using steganography process. First component which stores the data securely is known as cover object, second is one message which we need to place it secret, third one is stego-object which will have combination of cover object and embedded message present in it [6]. The key is used to share between process of embedding and extraction. The data to be protected during the embedding approach and is become unprotected after the process of extraction. [7] The way to carry our secret information will prefer to have several different forms of data such as audio, video, text, image and network so on and its process shown in fig1.

II. REVIEW OF THE RELATED WORK

[1] Paper introduced a high-limit reversible information concealing plan for encoded interactive media information by utilizing Homomorphism Encryption. In a picture, three adjoining pixels are chosen as a gathering for the entire procedure. In the encryption part, the first picture is encoded by a picture supplier. At that point, the encoded picture is sent to information hider. In the information concealing section, two supreme contrasts can be acquired in each gathering. The extra information is inserted into the encoded picture by moving histogram of the total contrasts. [2] Besides, an arranging procedure that sorts the entirety of two supreme contrasts in each gathering effects only affects on decreasing picture bending. The encryption and inserting tasks are constrained by encryption and inserting/information stowing away keys, individually. In the event that a beneficiary just has the information concealing key, the extra information can be removed and the figure content can be re-established. On the off chance that the collector has the unscrambling key and the information concealing key, the extra information can be removed and the first picture can be re-established.

[3] Late Interpolation-based Reversible Data Hiding (IRDH) plans exhibited fundamentally higher inserting limit, be that as it may, their inserted picture quality isn't much noteworthy, especially for higher size payload. This paper introduces an improved IRDH conspire with neighbourhood scattering for better quality inserted picture. For high payload capacity, correlation based inserting is used in every embedded piece just in the added pixels. The mistake between an installed pixel and its unique adaptation is then diminished utilizing the nearby (i.e., block-wise) standard deviation to additionally improve the inserted picture quality [4]. Since the standard deviation is registered from the first pixels and their separate added pixels in a square, the improved inserting process stays reversible to loss less extricate the embedded information. The host pixels are likewise kept unblemished for ideal recuperation of the original picture. A critical improvement in inserted picture quality is consequently recorded in contrast with the best in class IRDH plans.

[5] The reversible information covering up is a developing innovation that utilizes the repetition of the transporter (regularly advanced pictures) to put secret data and guarantee the reversibility of the bearer and concealed data. In ongoing year, a number of reversible information concealing calculations dependent on error expectation related extension have been created. In forecast error extension, expectation on the inside pixel is made dependent on its neighbour pixels. The information inserting is led by the adjustment on the histogram produced using forecast extension. Consequently, the precision of expectation on pixel is the way to improve the presentation of the calculation. In this paper, we propose reversible information covering up dependent on directional forecast and various histograms adjustment and plan the relating reversible concealing standards. Contrasted with the current calculations, trial results demonstrate that proposed technique can reduce picture flexibility for a given limit.

[6] Reversible picture information stowing away is (RIDH) is an exceptional classification of information concealing procedure. This system will guarantee ideal recreation of the spread picture upon the extraction of the implanted message. Information extraction is accomplished through a component, in which access to secret encryption key isn't necessary. The method are especially connected in the basic situations, for example, military and remote detecting, restorative picture sharing, copyright validation and law criminology, where the reproduced spread picture is required in high loyalty. large numbers of the analysts have

contemplated reversible picture information concealing methods in late year. This paper fundamentally condenses the current strategies of reversible picture information concealing calculations, and it gives the essential method of the methods utilized.

[7] Distributed computing is one of the mainstream techniques for getting too shared and progressively configurable assets through the PC organize on interest. The protected information storage on cloud platform is the essential prerequisite of such applications, where information are being exchanged or transmitted between the servers and their clients. A standout among the best methods for secure imparting is steganography in cloud. The steganography includes technique for composing hidden messages in a way that nobody other individual however sender and recipient would most likely safely comprehend and impart the data covered up in the methods for correspondences [8]. To guarantee security of information in distributed computing, this paper exhibits another content steganography approach for stow away stacked secret English content record in a spread English content document. The proposed methodology improved information security, information concealing limit, and time.

[9] In the restorative distributed computing, the medical clinic overseer encodes the pictures before re-appropriating it in to the cloud server. For this situation, just approved specialists are permitted to get to the pictures since the restorative pictures are exceptionally private. Scrambling the pictures before redistributing is a normally utilized methodology, where the patient just needs to send the comparing encryption key to the approved specialists. This, be that as it may, altogether confines the privacy of the pictures. In this paper, we propose two Secure and Efficient Encryption conspires over restorative pictures. Right off the bat, we influence the Elgamal and Ron Rivest, Adi Shamir, and Leonard Adelman (RSA) encryption methods to propose a twofold encryption, which can accomplish secure capacity of pictures in the cloud. Furthermore, we propose an upgraded plan to give security by giving Schnorr Protocol so as to accomplish Proof of Knowledge. Contrasted and existing recommendations, our plans are better as far as security. At that point, we propose an improved plan to give Blocker Protocol, to realize who is recovering the picture from the cloud server.[10] Information covering up in video streams turned out to be progressively famous in the present world, since there is a high recurrence of information correspondence over the web. Concealing the information in video streams gives greater security just as increments installing limit than stowing away inside the pictures. Right when the proportion of information to be embedded into the video extends it can unfavorably impact the video quality making it unsatisfactory for explicit applications. The significant worry for information stowing away into recordings is its more noteworthy visual element, expanded concealing limit, gushing video measure and so forth. [11]In this paper, another information concealing strategy is proposed in compacted H.264 Video Streams. At first, the technique misuses choosing the IPCM squares which does not experience bury and intra expectation amid H.264 video density. Second, changing the spatial area IPCM hinders into recurrence space by utilizing discrete wavelet change (DWT). Third, the surge of message bits are inserted into sub bands of the exchanged IPCM squares utilizing Least Significant Bit system.

III. PROPOSED SYSTEM OVERVIEW

The proposed model of steganography consists of Carrier, Message and Password. Carrier is also known as cover-object, which the message is embedded and serves to hide the presence of the message. Basically, the model for steganography is shown on Fig.1. Message is the data that the sender wishes to remain it confidential. It can be plain text, cipher text, other image, or anything that can be embedded in a bit stream such as a copyright mark, a covert communication, or a serial number. Password is known as stego-key, which ensures that only recipient who knows the corresponding decoding key will be able to extract the message from a cover-object. The cover-object with the secretly embedded message is then called the stego object. The Stego image is encrypted using chaotic system .Recovering message from a stego-object requires the cover-object itself and a corresponding decoding key if a stego-key was used during the encoding process. The original image may or may not be required in most applications to extract the message. Recovering message from a stego-object requires the cover-object itself and a corresponding decoding key if a stego-key was used during the encoding process. The original image may or may not be required in most applications to extract the message. Figure 2 (a) and (b) illustrate the proposed approach.

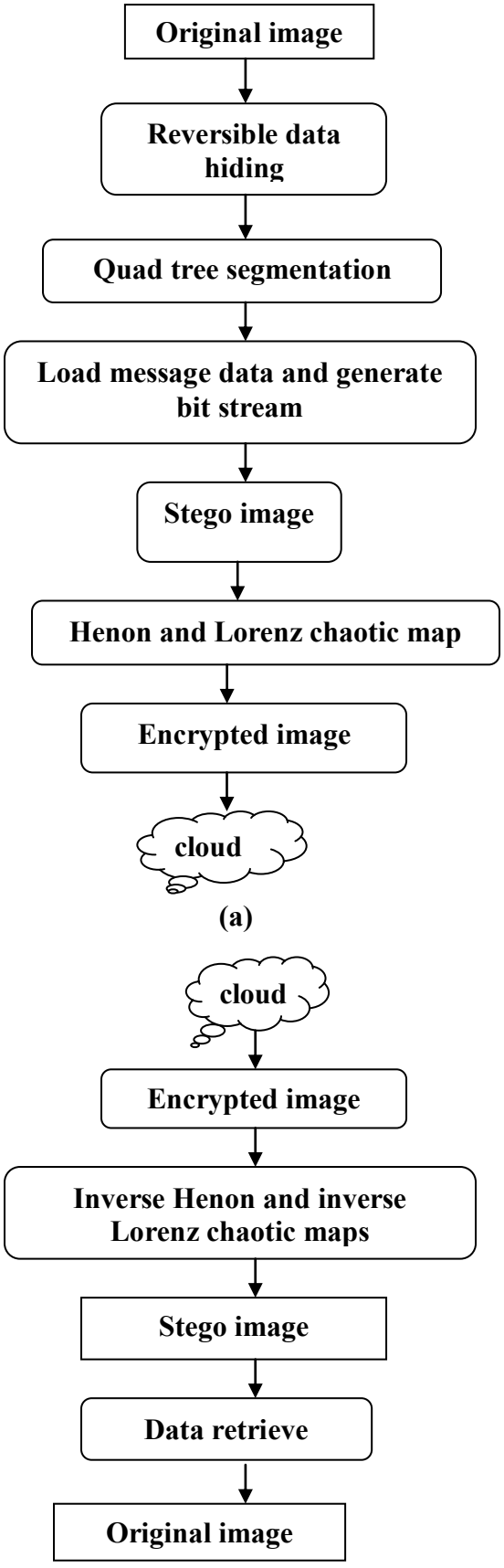


Fig 2 (a) & (b) Block diagram of the embedding framework with Encryption & extraction framework with Decryption

IV. PROPOSED DESIGN

The following algorithm explains the proposed design strategies.

A. Quad-tree segmentation

The proposed algorithm aims at embedding the secrete data to non-overlapped blocks of pixels using histogram shifting technique. These blocks are generated by partitioning input image and organized as a form of quad-tree structure.

Algorithm

- For any incoming block, the first step in the partition process is to make a decision on whether a further division is required or not.
- Before the decision, is tentatively partitioned into 4 sub-blocks.
- The hiding capacities of the incoming block and the 4 sub-blocks are evaluated individually.
- If the total capacity of the 4 sub-blocks is larger than that of the incoming block, then the incoming block is decided to be partitioned into four sub-blocks.
- Otherwise, the incoming block is considered as a terminal node of quad-tree structure, indicating no further partition required.
- After the incoming block is divided, each of the four sub-blocks is considered again to be the incoming block for further quad-tree partition.
- The process is keep on recursively in depth-first manner until all possible block partitions are traversed.

B. Embedding Algorithm

After we get embeddable blocks from quad-tree segmentations, we embed secrete data in these blocks using Histogram Shifting.

- Create the histogram of block. Find the maximum & minimum points.
- Shift the histogram between maximum point and minimum point. For example, the pixel gray level which is between 3 & 7 should be increased by 1.
- Convert the secret image into number of bit streams.
- Scan all of the pixels in the block. If a pixel gray level which is equal to 3 is found, check to-be embedded data bits; if to-embedded-data is “1”, the pixel value increase by 1, otherwise the pixel gray-level remains intact.

C. Extraction Algorithm

- The whole image is scanned. If the grayscale value of a pixel equals the key, a bit "0" is extracted. If the pixel value is key +1, a bit "1" is extracted.
- Shift histogram of the whole image back.
- We can get the maximum point & minimum point information of a block and the quad-tree bit stream Use quad-tree bit-stream to generate the embeddable blocks in the quad-tree of image segmentation.
- We can get each payload invisible in each block. Do extracting process block by block.
- Combine block-payload data and get the notvisible data.

V. REVERSIBLE DATA HIDING APPROACH

Presently in our daily life, data security is one of the significant methods which are increasing more significance for exchanging the data starting with one end then onto the next end over system. Information stowing away is one of the answers for security that keep the information secure in media of the host while exchanging the data however there exists some contortion.

Reversible Image Data Hiding is a system used to implant a snippet of data into the host pictures to produce the concealed one or checked one. By using hidden picture unique picture can be actually recuperated subsequent to separating the installed information. The first spread can be reversibly re-established from the concealed picture after the installed data is separated. Fig3 demonstrates the sketch of reversible picture information concealing methods.

The Reversible Image Data Hiding process takes out the disservices of one of the strategy called reversible watermarking. In the process to turn around the stamped pictures back to the first spread pictures after the concealed information are separated another strategy can be utilized to check the nature of re-established picture. The procedure which is utilized is the Peak Signal Noise Ratio (PSNR) to check the nature of turned around picture.

Reversible picture information stowing away isn't utilized for pictures however it can likewise be utilized for embedding data into spreads, for example, picture, sound, and video records. Reversible picture information concealing can likewise be utilized for media documentation, copyright assurance and so on.

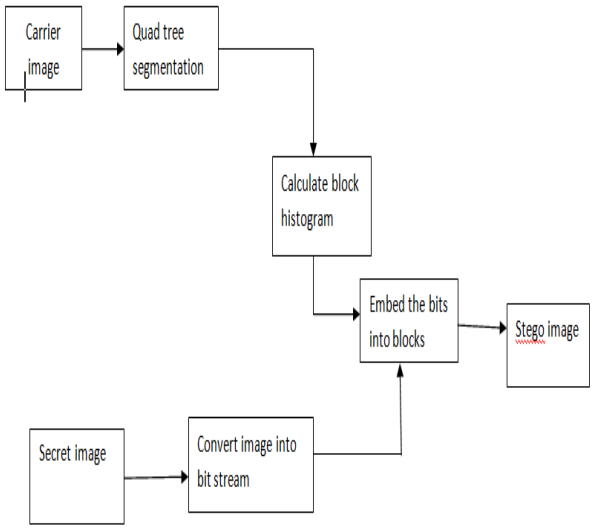


Fig 3 Reversible data hiding approach

VI. ENCRYPTION METHOD

The process of getting encrypted image from the secret image follows two mapping techniques such as Henon plus Lorentz map to generate chaotic sequence, by the way will get confused and diffused image.

A. Henon Map

Henon map is an instance of discrete time dynamical frameworks that prove chaotic behaviors. It takes a point (x_n, y_n) in the plane and maps it to another point. It is characterized by the accompanying arrangement of distinction conditions.

It was a modified course of action in which Poincare portrays the Lorenz technique, the overall considered Henon layout a clear two-dimensional guide with quadratic non-linearity. This guide gave a first instance of unusual attacker with structure. Because of its straight imposition, the Henon map suits numerical examinations. Thusly a great deal of PC examinations took after. Regardless, the complete image of each possible bifurcation under the distinction in the parameters a and b is far from completion.

$$x_{n+1} = y_n - 1 + a \times x_n^2$$

$$y_{n+1} = b \times x_n$$

B. Lorenz Map

Lorenz framework recognized as a unmanageable structure, the chaotic actions formed by Lorenz structure have composite structure, unpredictably certified regarding progression of the structure factors, and three factors of system

can be the starting keys of chaotic encryption planning and the key space of this computation is significantly more important than low dimensional animated structures. The Lorenz conventional differential condition was given by E.N. Lorenz in 1963 and Lorenz arrangement of dynamic condition is

$$\frac{dX}{dt} = s \times (X - Y)$$

$$\frac{dY}{dt} = Y \times (r - Z) - Y$$

$$\frac{dZ}{dt} = X \times Y - b \times Z$$

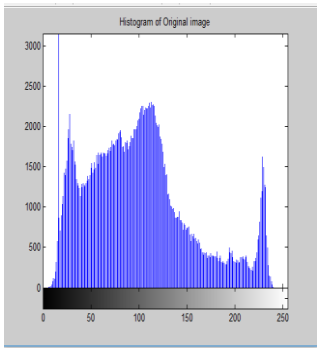
Here X, Y & Z make up the coordination circumstances
Where t is the time
s, r & b are the arrangement parameters.

VII. EXPERIMENTAL RESULTS

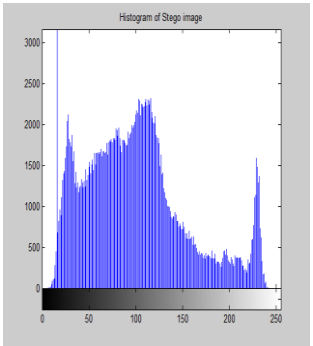
Input image

quad tree partition

Data hidden image



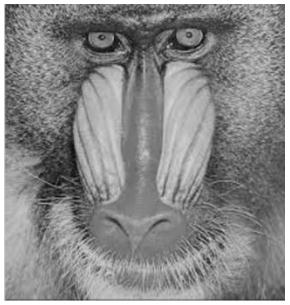
a)



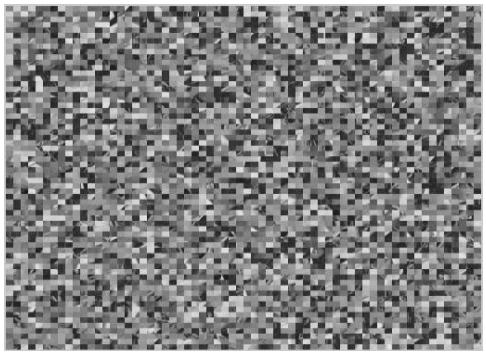
b)

a)Histogram of original image

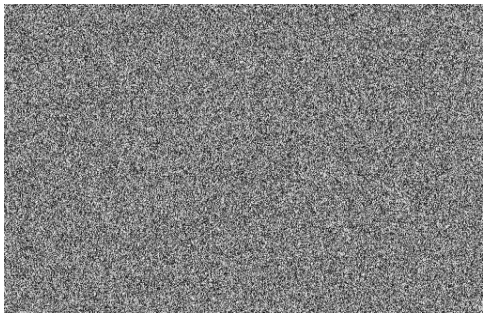
b)Histogram of stego image



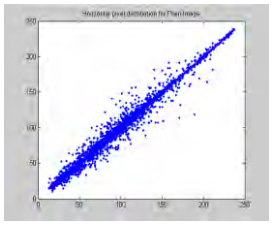
Test images



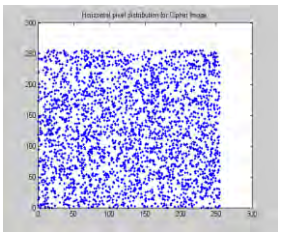
Confused image



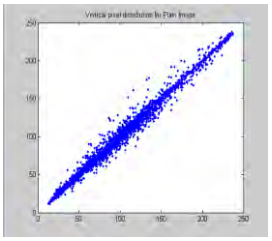
Diffused image

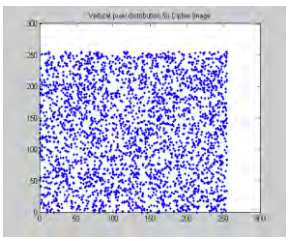


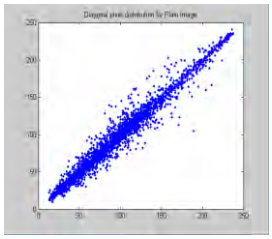
a)

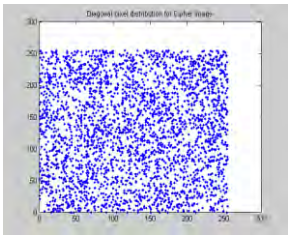


b)









e) f)

key sensitivity test:

a)Horizontal pixel distribution of plain image

b)Horizontal pixel distribution of cipher image

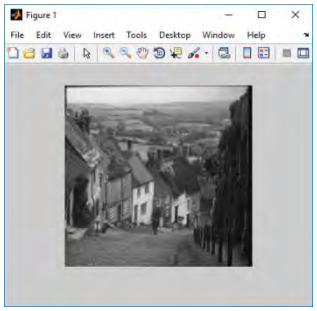
c)Vertical pixel distribution of plain image

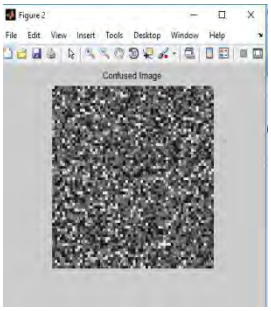
d)Vertical pixel distribution of cipher image

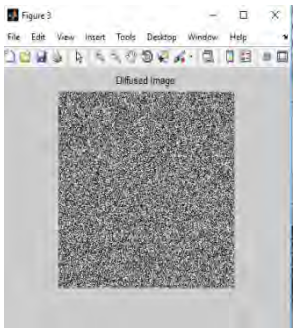
e)Diagonal pixel distribution of plain image

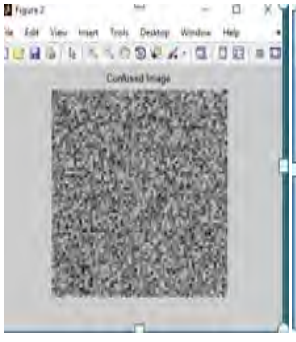
f)Diagonal pixel distribution of cipher image

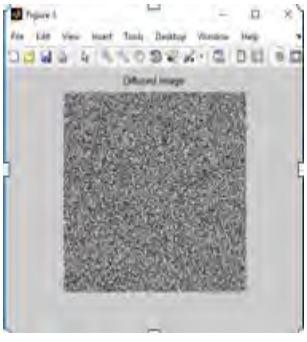
comparison on 2 different images



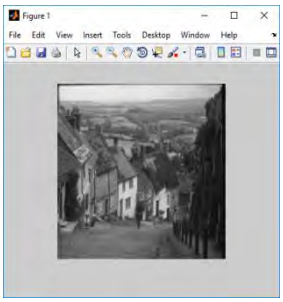


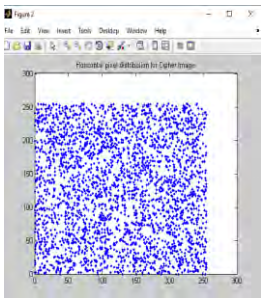


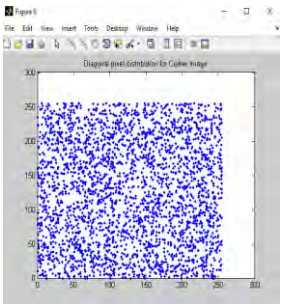


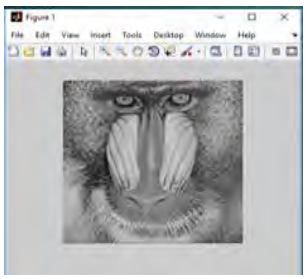


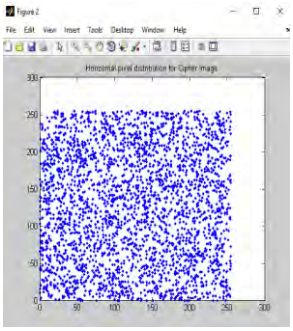
Comparison on different correlation on 2 images:

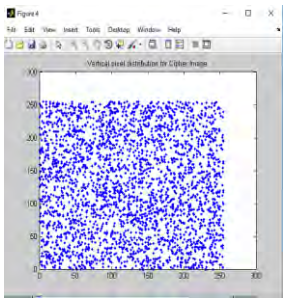




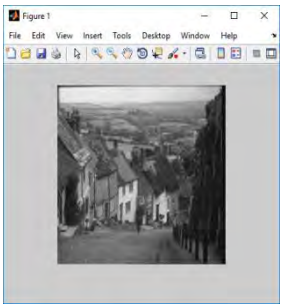


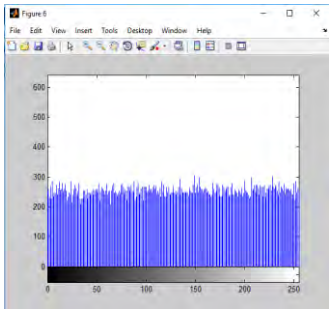


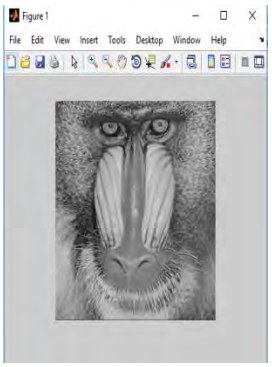


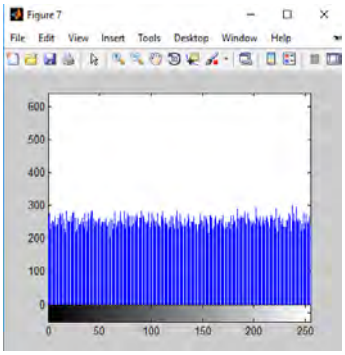


Comparison on histogram of 2 different images:









Decryption work

Decrypted image recover image

VIII. PERFORMANCE ANALYSIS

A.Data Entropy

Entropy of a host gives idea with respect to self-information. Information entropy is essential segment of susceptibility. The particular consistency level is achieved when entropy value is less than 8 bits. For a crypto framework to restrict the entropy ambushes, crypto framework ought to be close impeccable regard 8.The calculated entropy for pictures is almost near to 8.

$$H(m) = -\sum_{i=0}^{F-1} p(m_i) \times \log_2(p(m_i))$$

Where F- Grey level value count

P (m_i) - Grey level value occurrences in probabilities

B. Peak Signal to Noise Ratio

PSNR calculate ratio between maximum signals power to its larger possible corrupting a noise signal.

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

C. Mean Square Error

One clear way of determining similarity is to calculate an error sign by deducting trial sign from reference, and used to compute the average energy of the error sign. The mean-squared-error (MSE) is the obvious, and the most extensively used, complete-reference picture superiority measurement.

$$MSE = \frac{\sum_{i=1}^{M}\sum_{j=1}^{N}[plain(i,j)-cipher(i,j)]^2}{M*N}$$

Where Plain (i,j) – reference image

Cipher (i,j) – modified image

i & j are position of pixel in M*N picture

D. Structured Similarity Index Metric

SSIM is one of the best approaches for evaluating image quality.

The equation for SSIM is given by

$$SSIM = \frac{(2*\bar{x}*\bar{y}+c1)*(2\sigma_{x,y}+c2)}{(\bar{x}^2+\bar{y}^2+c1)*(\sigma_x^2+\sigma_y^2+c2)}$$

Where $\bar{x} = \frac{1}{M*N}\sum_{i=1}^{M*N} x_i$

$$\bar{y} = \frac{1}{M*N}\sum_{i=1}^{M*N} y_i$$

$$\sigma_x^2 = \frac{1}{M*N}\sum_{i=1}^{M*N}(x_i - \bar{x})^2$$

$$\sigma_y^2 = \frac{1}{M*N}\sum_{i=1}^{M*N}(y_i - \bar{y})^2$$

$$\sigma_{x,y} = \frac{1}{M*N}\sum_{i=1}^{M*N}(x_i - \bar{x}) * (y_i - \bar{y})$$

IX. CONCLUSION

This paper gives an examination of information concealing techniques utilizing reversible data hiding approach followed by encryption using chaotic approach. Reversible picture information concealing in encoded pictures is one of the new subject illustration consideration into approach where now a day's result of the security safeguarding necessities from numerous applications. Reversible picture information concealing plans are investigated with a low calculation unpredictability, later which comprises of picture encryption, information covering up and information extraction/picture recuperation stages. Ordinarily in every one of these strategies the original pictures are gone through hiding process, further it follows encryption to make data more secure and should resist the attack from the environment as well as outside world. The present approach utilizes a blend of the two strategies – confusion and diffusion for encryption. Disarray is accomplished utilizing an arrangement of arbitrary numbers produced from Henon map. Diffusion is done in two stages, where the initial step changes pixel esteems dependent on a succession of arbitrary numbers created from Lorenz condition, while the other advance changes the pixels dependent on the original picture. The

image steganography is done by using RDH technique and it gives better results compared with existing techniques by comparing security analysis parameters such as PSNR, MSE and SSIM. Followed by, chaotic encryption approach gives better performance by treating parameters such as PSNR, MSE, SSIM, Correlation and Entropy.

REFERENCES

[1] Feng, B., Lu, W., Sun, W.: 'Secure binary image steganography based on minimizing the distortion on the texture', IEEE Trans. Inf. Forensics Secur., 2015, 10, (2), pp. 243–255.

[2] Mahajan, P., Gupta, H.: 'Improvisation of security in image steganography using DWT, huffman encoding & RC4 based LSB embedding'. IEEE Int. Conf. Computing for Sustainable Global Development (INDIACom), February 2016, pp. 523–529.

[3] Sehgal, P., Sharma, V.K.: 'Eliminating cover image requirement in discrete wavelet transform based digital image steganography', Int. J. Comput. Appl., 2013, 68, (3), pp. 37–42.

[4] Morkel, T., Eloff, J.H.P., Olivier, M.S.: 'An overview of image steganography'. Proc. Fifth Annual Information Security South Africa Conf., June 2015.

[5] P. Selvigrija and E. Ramya, "Video by Linked List Method," no. March, (2015).

[6] M. Hussain and M. Hussain, "A Survey of video Steganography Techniques," Int. J. Adv. Sci. Technol., vol. 54, pp. 113–124,(2017).

[7] G. Kaur and A. Kochhar, "A Steganography Implementation based on LSB & DCT," vol. 4, no. 1, pp. 35–41, (2015).

[8] Akhtar, N.; Johri, P.; Khan, S., "Enhancing the Security and Quality of LSB Based Image Steganography," Computational Intelligence and Communication Networks (CICN), 2013 5th International Conference on , vol., no., pp.385,390, 27-29 Sept. 2016.

[9] Das, R.; Tuithung, T., "A novel steganography method for image based on Huffman Encoding," Emerging Trends and Applications in Computer Science (NCETACS), 2014 3rd National Conference on , vol., no., pp.14,18, 30-31 March 2014.

[10] Prabakaran, G.; Bhavani, R.; Rajeswari, P.S., "Multi secure and robustness for medical image based steganography scheme," Circuits, Power and Computing Technologies (ICCPCT), 2013 International Conference on , vol., no., pp.1188,1193, 20-21 March 2015.

[11] Thenmozhi, S.; Chandrasekaran, M., "Novel approach for image stenography based on integer wavelet transform," Computational Intelligence & Computing Research (ICCIC), 2016 IEEE International Conference on , vol., no., pp.1,5, 18-20 Dec. 2016.