Develop Cloud Information Safety with Steganography Method

Tejinder Pal Singh Brar[1], Ravi Kumar Sharma[2]
[1]*Chandigarh Group of Colleges, Landran, PB*
[2]*Chandigarh Group of Colleges, Landran, PB*
Email: [1]*tpsbrar@gmail.com and* [2]ravirasotra@yahoo.com

***Abstract*—Steganography is useful to Enhance Cloud Data Security. During the interaction of this strategy, as classified data, private messages are additionally kept accessible. Its conduct through data from different sources can be stowed away from different pearls known as these sorts of games. Crafted by study presenting the idea of picture steganography. The hereditary calculation and edge discovery are utilized in the past work of the steganography module. The custom code presented in this exploration depends on the GLCM calculation for the distributed segment. The PSO calculation was acquired to take a gander at the part from the picture we need to shading. The PCA Algorithm was acquainted with remove the valuable highlights of the picture. The presentation of the proposed modular is tried in MATLAB and is assessed by an obvious technique that is following the PSNR and the MSE. The PSNR worth of the record esteem is raised to fifteen percent contrasted with the current calculation. The MSE worth of the proposed calculation is decreased to 10 percent contrasted with the current calculation.**

Keywords-*Steganography, the PSO Algorithm, GLCM Algorithm, Cloud, Data Security.*

I. Introduction

The way toward changing over computerized to advanced by playing out numerous procedure on it is known as advanced picture handling. The capacity [1,2,3] with two sections ff (x, y) of x and y is communicated along with the chart of the predefined picture by the thickness of f any place the organize (x, y) is known as [12] the diagram . A picture is known as an advanced picture if there are positive qualities in x, y and the thickness of f. There are some unmistakable highlights here that drawings depend on advanced [8,9] painting. The principle motivation behind picture preparing is to separate some significant data on the picture. The data sources gave in the framework are advanced, yet the video content gives extra data about the[15] picture being delivered. Regularly, the pictures are perused as two-dimensional images by applying a [4,5] graphical handling technique over them. To be effective in numerous applications, this strategy is utilized today.

II. Review of Literature

Man has learned and created from various perspectives ordinarily himself. The calculations of this hunt dependent on normal choice and qualities are hereditarily changed life forms (GAs). Bigger branches known as the Evolutionary Assembly incorporate GAs as information. Advancement issues were tackled dependent on these calculations. For a given issue, a pool or number of potential arrangements is given by GA. Advances and changes are produced using these components, so infants can be gained. Over the ages, this cycle has been rehashed here. Contingent upon the particular reason for the individual, quality is allocated. Additionally, the individuals who are appropriate are offered the chance to be tidied up and more reasonable individuals are given. Along these lines, in past ages, better arrangements arose out of this cycle until this interaction was halted. The construction of the genome is unequaled. Be that as it may, with precise testing, these calculations function admirably where these calculations abuse chronicled data. There are a few watchwords in this arrangement that is set out underneath:

1. Population: The quantity of potential reasons for your issues is outstanding. The number of inhabitants in GAs is fundamentally unrelated, and there is a bunch of relapses that are given rather than those of the GAs.
2. Chromosomes: How to determine a realized issue is a chromosome.
3. Gene: A typical chromosome is known as a quality.
4. Compensation: The worth of the organic instrument for this chromosome is otherwise called the allele.
5. Genotype: The quantity of people in the combination space is known as the genotype. With a basic and adaptable arrangement, the items that are searching for them in a little manner compensate for them.
6. Phenotype: The figures in reality domain of essence that incorporate visual components and genuine circumstances are notable.
7. Remedies and Admissions: There is an aggregate and genotype space for basic issues. Notwithstanding,

there is a distinction if these two-dimensional spaces are engaged with numerous situations. The change from fix to genotype to risk aggregate is the thing that is called fix. In any case, the change from aggregate to genotype space is known as data sources. From that point forward, re-coding has been acted in GA during the computation of medical advantages; the maintenance expenses ought to be high.

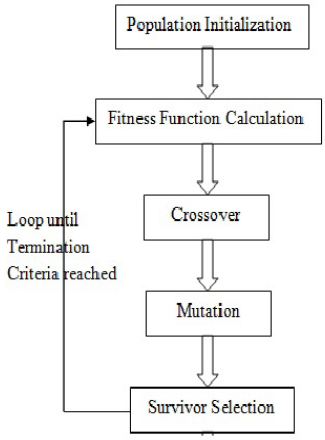

Fig. 1: Edge Detection Process

III. Proposed Work

The process that can hide sensitive information within the cover image so that the image is not decomposed is known as steganography image. Hidden information is secured and therefore, unauthorized users cannot access this information. There are some imaging techniques that scientists propose and objective.

Following are the various research objectives:-

1. To propose improvement in the DWT technique for the generation of semi blind steganography.
2. The proposed technique will be based on the GLCM algorithm to analyze features of the original image.
3. To implement proposed technique and compare with existing in terms of PSNR, BER and MSE

A. Spatial Domain

There is a variation of some bits within pixel values for encrypting data in spatial domain [14] steganography. The least expensive is the most commonly used method among this species. Here are some key departmental procedures:

1. Most Important Bit (LSB): To put information into an encrypted file, the most common and simplest method is an LSB entry. There are two types of digital photos that are used as cover files, which [37] are 24-bit and 8-bit images. Three message pieces can be inserted into any pixel in 24-bit images. One message can be hidden in an 8-bit image. What Stego's image is identified as an image that[10] includes the coded information that is embedded in the implementation of the LSB algorithm. Replace small pixels with information that will be hidden in the LSB format. The crypto currency has no cache when LSB is replaced [13] and the idea of encrypting the information behind the image cannot be known to an unwanted user. The dimensions [12] of the original and modified pixels do not change here even though visualization is impossible.

A can be hidden within three pixels that is eight bytes of an 24-bit image is shown with the example below:

Pixels: (00100111 11101011 11001010)
(00100111 11011000 10101001)
(11001000 00110111 11011001)
A: 010100111
Result: (00100110 11101011 11001010)
(00100111 11011000 10101000)
(11001001 00110111 11011001)

Implementation with high-speed communication systems is made possible with the help of LSB technology. The amount of first image went down a little bit here. Notwithstanding this [6] method there is a risk that the addition or destruction of information is possible due to the simple attack. Also, for the use of images, this approach is difficult and simple.

B. Transformation Domain Technique

In an important part of the cover code, the information is encrypted using the change section method. In the case of other imaging modalities, this process is known to be more complex. Many researchers have devised a method for the domain of change. Changing the cover image, typing the numbers and adding the parameters of the changes is an important way of working.

During the interval, all the hidden information is generated with the help of the DFT system. In a series of video clips, the information is hidden in a complex format. With the addition of DFTs, the cover vector is transformed from a broad domain in the form of domain frequency [11]. There are two parts where each pixel is transformed and the spatial dimension is the real dimension and the mental dimension. Within a real area of frequency, hidden information is added and the original pixels are excluded here. The frequency domain is changed to a related domain once the IDFT host is created. This image is converted [11] from a wide area to a frequency domain once the message is mapped or removed. The original DFT image with the addition algorithm is restored to the original image.

IV. Edge Detection Process

The fundamental instruments utilized in visual keenness as face identification. With the change of

ISBN: 978-93-91355-11-1

the dark tone in the picture the first picture is changed over to the picture utilizing the pursuit technique. Connection of the significant contrasts of dark diagrams is tackled through a mathematical examination by picture investigation. From an actual outlook, the physical and mathematical properties of the material are identified. Through this interaction, the degree and extent of the article are resolved. To distinguish the significant discontinuities and impediments, face identification is a generally utilized technique. Inside the force range, nearby changes are seen in the outskirts. Around the boundary between the two districts, the pinnacles are distinguished. With the tip of the picture, the essential components can be separated. For advanced imaging, the main thing to focus on is the face location. In cutting edge PC vision frameworks, these highlights are utilized. For the identification of articles, a productive location framework is applied in numerous applications. From that point forward, a significant degree of picture examination has been performed; face identification is acquiring genuine prevalence. The head, line and shading are three unique kinds of discontinuities inside the dark level. In recognizing every one of the three sorts of solvents in a single picture, clear veils are utilized.

V. Least Significant Bit (LSB)

For every one of the bytes in the picture, the most unsignificant pieces are changed over to secret messages. 24-cycle pictures and 8-bit pictures are the two distinct structures where computerized pictures are found. Three pieces of data are implanted in every pixel in a 24-bit picture. For each LSB position of three eight-cycle esteems, the slightest bit is accessible. The picture show doesn't change because of increment or decline in esteem through adjustment at LSB. Along these lines, the cover picture and the subsequent stego picture appear to be comparative. The slightest bit of data can be covered up in a 8 bit picture. Encryption and unscrambling are the two calculations gave in this methodology. Due to minimal significance of this layer, the composing information begins from the last layer. From the layer beneath, the importance is multiplied for every upper layer . Picture quality is decreased and picture correcting is moved while moving towards the upper layer.

Data can be covered up in the picture through encryption procedures. Certain encoded documents can't be seen by different clients. A wide range of pictures and messages can be given through this module. The solitary picture document in the objective is given here.

To remove concealed data from picture records, unscrambling procedures are utilized. The picture record is given as yield in this cycle. In the objective organizer, two documents are given, which are comparative picture records and the message document covered up inside is another record.

VI. Grey Level Co-Occurrence Matrix (GLCM)

For every one of the bytes in the picture, the most unsignificant pieces are changed over to secret messages. 24-bit pictures and 8-bit pictures are the two unique structures wherein advanced pictures are found. Three pieces of data are inserted in every pixel in a 24-cycle picture. For each LSB position of three eight-bit esteems, the slightest bit is accessible. The picture show doesn't change because of increment or reduction in esteem through alteration at LSB. Subsequently, the cover picture and the subsequent stego picture seem to be comparable. The slightest bit of data can be covered up in a 8 cycle picture. Encryption and unscrambling are the two calculations gave in this methodology. Due to minimal significance of this layer, the composing information begins from the last layer. From the layer underneath, the importance is multiplied for every upper layer . Picture quality is decreased and picture modifying is moved while moving towards the upper layer.

Data can be covered up in the picture through encryption methods. Certain encoded documents can't be seen by different clients. A wide range of pictures and messages can be given through this module. The lone picture record in the objective is given here. To separate concealed data from picture documents, unscrambling strategies are utilized. The picture record is given as yield in this interaction. In the objective envelope, two documents are given, which are comparable picture records and the message document covered up inside is another record.

VII. Particle Swarm Optimization

To solve optimization issues within the systems, another commonly inspired algorithm by nature is a particle arms optimization algorithm. It is a community-based meta-heuristic algorithm that encourages the operation of the algorithm from flying birds and schooling fish. Using the quality measures improves the solutions. The initially distributed series of particles is generated randomly. In addition, humans are executed by particle mobility around a search space by including mathematical expressions. With the help of these mathematical expressions, a small inter-particle communication model is simulated. In its simplest form, these expressions suggest the mobility of each particle. Each particle is moved towards the best experienced position as well as the best known location in the swarm. Various versions include a large number of updated rules. The initial objective here is to create a set of points and then have an initial velocity vector assigned to each. By adjusting the velocity vectors by using a few random factors in combination with the velocity vectors, the position is changed in an iterative form.

ISBN: 978-93-91355-11-1

VIII. Principal Component Analysis (PCA)

The dimension of the dataset where a large number of related variables are present is minimized by PCA algorithms. This algorithm ensures that within the database the maximum potential variability is maintained. To ensure this, the main components of the new set of variables are transformed. The newly developed computers are uncoordinated and to maintain the greatest variance present in all the original edits, these computers are ordered. With the help of statistics and mathematical technology such as Eigen attitudes and Eigen vectors, an increased understanding of PCA is made. The use of some research such as compression and imaging can be done by performing a statistical PCA. For mapping data from high-dimensional space to low-dimensional space, there is a linear transformation used within PCA. With the help of Eigen vectors of a matrix, you can control a small dimensional space.

- For a given data set "S", the mean valve S is achieved.
- From say S, the mean value is subtracted. A new matrix is achieved from these valves which are named as "A".
- From the matrix C = AAT, covariance is achieved. From the covariance matrixes V1V2V3V4…VN, the Eigen values are achieved.
- For the covariance matrix C, the Eigen vectors are computed finally.
- As shown in the equation below, any vector represented by S or can be written in the form of linear combination.
- The basis is generated due to the symmetric nature of covariance matrix.

$$V_N S - \bar{S} = b_1 u_1 + b_2 u_2 + b_3 u_3 + \cdots + b_N u_N$$

- In order to generate lower dimension data set, only the highest Eigen values are held.

$$\hat{S} - \bar{S} = \sum_{I=0}^{1} b_1 u_1 ; 1 < N$$

IX. Proposed Method

This work is based on image encryption and base paper technology is used in encryption programs where image is sent to unsecured channels. To encrypt the image for transmission over unsecured channels image is divided into boxes. The image is split into blocks and these split blocks are rearranged to encrypt the image. The blocks are arranged in a fixed pattern and this pattern is determined by the key used for encryption. The key is derived from the link between the pixels of the image. The proposed technology is progressing well and it is reported that the proposed technology is performing well against various attacks. In the future, we will work on a key formation stage to run a key based on the image's text properties so that pixel loss is minimized during decoding. The proposed algorithms can be used in the following steps:

1. Pre-processing phase: In the pre-processing stage, the two images are taken as input. The first image is the image that needs to be encrypted and the second image is the image that the key needs to create.
2. Extracting features: In the second phase, the text properties of the first image are extracted using the glcm algorithm. The Glcm algorithm extracts features such as energy, chaos, etc.

A. GLCM Algorithm

1. Count all the number of pixels in the matrix in which the data is saved.
2. Store the counted pixels in matrix P[I,j].
3. Check similarity between pixels in the matrix by applying histogram technique.
4. Calculate contrast factor from the matrix:
5. The elements of g need to be normalized by dividing the pixels.

$$g = \begin{bmatrix} 0.8 \; if \; g < 0.8 \\ 1.2 \; if \; g > 1.2 \\ g \; otherwise \end{bmatrix}$$

B. Experimental Results

An example of the proposed algorithm is shown. All of the simulations were performed using standard images set by SIPI . The data format is available online and accessed by volume of 512x512 pixels. The empirical results show that the image obtained by the stego is similar to the original cover image but the difference is not visible to the human eye. If the algorithm is exposed by steganalysis, the attackers will still have to break through encryption to retrieve sensitive data and then from the algorithm provide high security levels for the underlying system.

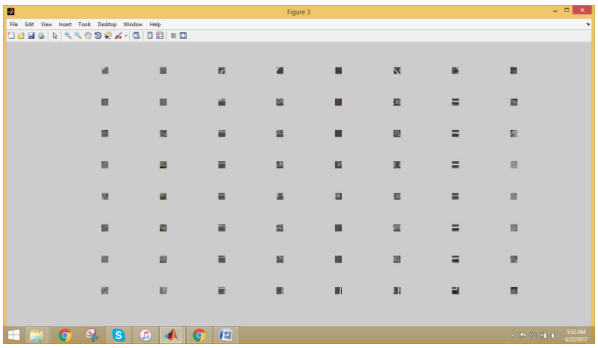

Fig. 2: Division of Image Into Blocks

The image stegno is divided into a block of size and in the execution of this rule 8 * 8 is considered for division. To distribute this image for transmissions there

ISBN: 978-93-91355-11-1

is no safe way to analyze the number of obstacles. Submit the corrected image for applying this image. The blocks are grouped into a set sequence and the sequence is determined using a set of keys. The key is obtained based on the relationship between the pixels of an image.

$$g = \exp[\frac{mean(I) - minimum(I)}{maximum(I) - mean(I)}]$$

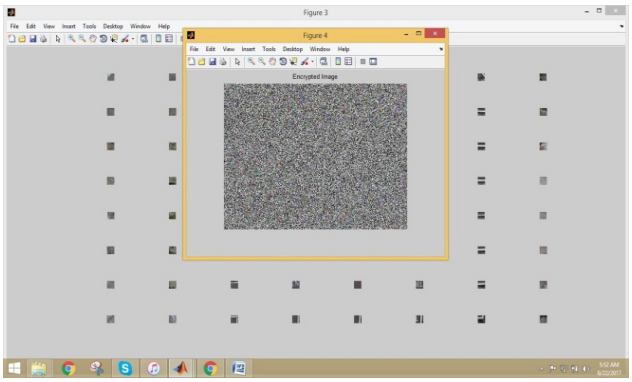

Fig. 3: Generate Final Encrypted Image

The second picture is taken as input and divided into fixed size blocks. The key is generated from the image by evaluating the texture features using the GLCM algorithm.

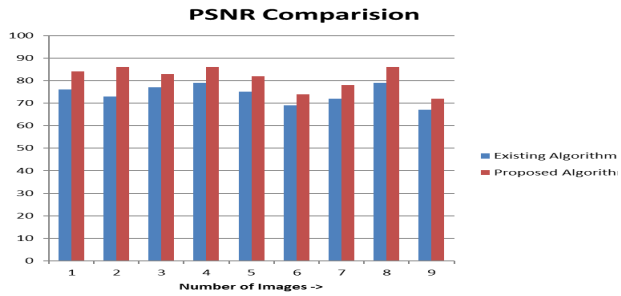

Fig. 4: Apply Salt & Pepper Attack

The textual features of the first image were extracted with the GLCM algorithm. The GLCM algorithm will extract features such as energy, entropy, etc. from images. After this, the PCA algorithm applied will choose the features extracted from the primary image.

In the next step, the button is generated from the subsequent image which increases security. To increase security, the next stage of the encryption process aims to change the value of each pixel in the whole image. The Chaotic Encryption Algorithm is applied to produce the final encrypted image. Secreted secretions are revealed using the Chaotic Encryption Algorithm. Evaluate the reliability of the hidden map of salt & salt concentration which changes the basis of the stored salt content. Salt & pepper noise is added to the hidden image. This will check the safety of hidden images and how many photos of destruction are reduced when salt & salt is applied to this image.

X. Analysis

The PNSR value of the proposed and current method is calculated. The performance of the algorithm is tested on stegnography, contrast to image, sharp image, salt and salt. It is checked that the proposed method works well in all cases.It is also investigated that the proposed method has a higher PSNR value due to the use of the GLCM and PCA algorithm.

Table 1: PSNR Comparison

Image	Existing Algorithm	Proposed Algorithm
1	76	82
2	72	86
3	78	81
4	79	86
5	77	82
6	69	83
7	68	72
8	89	94
9	68	72

As shown in the second table, the MSE value of the current algorithm is compared to the estimation algorithm for performance analysis. It is tested on the performance of the high-resolution algorithm compared to the existing algorithm. The MSE value of the algorithm is lowered to 15% compared to the current algorithm that improves image quality.

XI. Conclusion

This research work is based on the generation of sound steganography that increases the storage of sensitive data. The conclusion is given below:

1. The proposed method is based on the GLCM and PCA algorithm for the generation of steganographic images that increase the storage of affected dat
2. In the recommended format, the security of the stegno interface is increased by using the casino schema
3. This feature was implemented in MATLAB and a comparison of the existing algorithm was used to evaluate the reliability of the proposed algorithm
4. The performance of the algorithms in the PSNR and MSE systems is tested. It is explored in the nature of high-resolution digital imaging as compared to real-time techniques
5. The PSNR value of the proposed algorithm is up to 10 per cent and the MSE value of the proposed algorithm is reduced to 15 per cent compared to the existing method.

ISBN: 978-93-91355-11-1

Refercnes

[01] Sharma, R.K.; Ghandi, P. 2017. Estimate Reliability of Component Based Software System Using Modified Neuro Fuzzy Model. International Journal of Engineering & Technology, v.6, n.2, pp. 45-49.

[02] Diepenbeck M, Soeken M, Grobe D, Drechsler R: Towards automatic scenario generation from coverage information. 2013 8th International Workshop on Automation of Software Test (AST) 2013; 82-88.

[03] TPS Brar, D Sharma, SS Khurmi, "Vulnerabilities in e-banking: A study of various security aspects in e-banking" International Journal of Computing & Business Research,

[04] Ravi Kumar Sharma & Parul Gandhi, "Quality Assurance of Component Based Software Systems", 2016 International Conference on Computing for Sustainable Global Development (INDIACom), 978-9-3805-4421-2/16$31.00@2016 IEEE.

[05] Tejinder Pal Singh Brar, Dhiraj Sharma, Sawtantar Singh Khurmi," Influence of Trust in espousal of e-banking in India", "International Journal of Research in Electronics and Computer Engineering", vol 1 no 1, pp 9-16.

[06] Ali Z: Behavior-Driven Development as an Error-Reduction Practice for Mobile Application Testing, 2019.

[07] R Sharma," Embedded Systems Dilemma of Chip Memory Diversity by Scratchpad Memory for Cache On-chip Memory", "International Journal of Engineering, Pure and Applied Sciences", Vol 1 No 1, PP 1-4.

[08] Tejinder Pal Singh Brar, Sawtantar Singh, Dhiraj Sharma," Disaster management and business continuity system in Indian banking: Review and assessment", 2016 3rd International Conference on Computing for Sustainable Global Development (INDIACom), pp 3305-3308.

[09] Ravi Kumar Sharma, Parul Ghandi," Reliability Estimation and Optimization: A Neuro Fuzzy Based Approach", "International Journal of Computer Science and Information Security (IJCSIS)", Vol 16 No 12.

[10] Ravi Kumar Sharma, Parul Gandhi," Evaluation of Software Consistency for Component Based System Through Soft Computing Technique", "MR International Journal of Engineering & Technology", Vol 8 No 1, PP 40-43.

[11] Zhang X, Stafford T, Dhaliwal J, Gillenson M, Moeller G: Sources of Conflict between Developers and Testers in Software Development. Information & Management 2014; 51:13-26

[12] Sharma, R.K., Brar, T.P.S. and Gandhi, P., 2021. Defense and Isolation in the Internet of Things. Internet of Things in Business Transformation: Developing an Engineering and Business Strategy for Industry 5.0, pp.141-168.

[13] de Carvalho RA, de Carvalho e Silva FL, Manhães RS, de Oliveira GL: Implementing Behavior Driven Development in an Open Source ERP. Enterprise Information Systems of the Future2013; 242-249

[14] Sharma, R.K. and Brar, T.P.S., Proposed Upbeat Digital Forensic Method for Cloud Computing Impression.

[15] Solis C, Wang X: A Study of the Characteristics of Behaviour Driven Development. 2011 37th EUROMICRO Conference on Software Engineering and Advanced Applications 2011; 383-387.

ISBN: 978-93-91355-11-1