International Journal of Innovative Research in Science and Engineering
Vol. No.3, Issue 02, February 2017
www.ijirse.com
ISSN (O) 2454-9665
ISSN (P) 2454-0663

COMPARATIVE STUDY ON IMAGE SECURITY TECHNIQUES

M.Hariharalakshmi [1], Dr.M.Sivajothi [2], Dr.M.Mohamed Sathik[3]

[1]*Department of Computer Science, Sri Parasakthi College for Women, (India)*

[2]*Department of Computer Science, Sri Parasakthi College for Women, (India)*

[3]*Department of Computer Science, Sadakathullah Appa College , (India)*

ABSTRACT

The main objective of this paper is to match the performance of two techniques that unit of measurement used to hide the information for providing security exploitation watermarking. Digital watermarking might be a technology for embedding varied varieties of information in digital content. In general, information for shielding copyrights and proving the validity of data is embedded as a watermark. I would prefer to plant such information in digital content exploitation digital watermark technology. Throughout this paper, a couple of unit of measurement is implemented and their performance is compared to look out the only technique to hide the information with high quality. The first technique providing data concealment security exploitation the blind spot of C-PEE approach. The second technique uses SMVQ approach for providing the security by concealing the information. To analyze the performance of these techniques, several performance metrics are used. This paper uses Peak Signal Noise Ratio(PSNR), Structural Similarity Index (SSIM), Mean square Error (MSE), and Root Mean square Error (RMSE) to analyze the performance. From the experimental results, it is shown that the SMVQ technique performs higher than the alternative technique.

Keywords— Block Dividing, C—PEE, Extraction Process, Histogram Based Embedding, SMVQ.

I INTRODUCTION

In the last decade, the event in technology and networking has created serious threats to get secured electronic communication. This has actuated the interest among system security researchers to beat the intense threats for secure information transmission. One technique of providing a lot of security to information is data activity. Steganography could be a singular technique of data activity techniques. Steganography could be a technique to cover data in many ways in which forestall the detection of hidden messages. It uses digital media as carriers for secret communication. It embeds messages into a bunch medium to hide secret messages therefore it does not arouse suspicion by AN auditor. Cryptography and Steganography don't seem to be one and also the same. Whereas Cryptography scrambles a message in order that it can't be understood, Steganography hides the messages in a sequence that it can't be seen. Un-detect ability, hardiness, and capability of the hidden

ISSN (O) 2454-9665
ISSN (P) 2454-0663

information area unit of the most options that differentiate Steganography from cryptography. In Steganography the key image is embedded within the cowl image and transmitted in such the simplest way that the existence of data is undetectable. The digital pictures, videos, sound files and different system files will be used as a carrier to enter the knowledge. The thing within which the key data is hidden is named covert object. Conceal image is referred as a picture that's obtained by embedding the secret image into a covert image. The hidden message could also be plain text, cipher text or pictures etc. The Steganography technique provides embedded information in an unsealed manner with high payload capability. Encrypting information provides information confidentiality, authentication, and information integrity.

A several analysis works are dole out on LSB based mostly Steganography. Totally different researchers utilized different techniques for the aim of concealment secret information in a very cowl image. Following are the few connected works dole out by varied analysis teams. A number of the foremost techniques utilized in the sector of Image Steganography are mentioned below. Some trivial algorithms utilizing the techniques are listed. Neil F. Johnson and sushil JA Jodie et al., [1] have provided many characteristics in information concealment strategies determine the existence of the hidden messages and additionally identify the hidden information. The images are reviewed manually for hidden messages and Steganography tool to change the method. The developed tool is to check hardiness of knowledge concealment techniques in pictures similar to deformation, cropping , rotating and blurring. Lisa M. Marvel and Charles T. Retter., [2] have given a way of embedding information within digital pictures, known as Spread Spectrum Image Steganography (SSIS). SSIS conceals a message of considerable length within digital pictures whereas maintaining the first image size and dynamic vary. A hidden message will be recovered using distinct suitable keys with none information of the first image. Giuseppe Mastronardi et al., [3] have studied the consequences of Steganography in several image formats (BMP, GIF, JPEG and DWT) and planned two totally different approaches for the lossless and lossy image. They have supported the creation of associate degree “ad-hoc” palette for BMP and GIF pictures. LUI Tong and QIU Zheng-ding., [4] have planned a Quantization-based Steganography theme. During this technique the key message is hidden in each chrominance part of a color image and also the concealment capability is on top of that of the popular Steganography package. Since the Quantization-based concealment technique is free from the interference and simulation results the hidden message will be extracted at low BER and our theme is strong to common attacks. M. Mahdavi et al., [5] given a steganalysis technique for the LSB replacement. The tactic relies on the changes that occur in the bar graph of a picture once the information is embedded. It is less advanced and high accurate than the RS steganalysis technique for the photographs that are no heritable directly from a scanner with none compression. The RS technique has to count the quantity of standard and singular teams double and additionally need LSB flipping for the entire image. This technique has higher average and variance of error examination to RS steganalysis technique. Shilpa p. Hivrale et al., [6] have given varied applied math measures and PMF-based mostly technique of detection. It uses the frequency count of the constituent intensities within the image to check for the detection of stego image or not. Here LSB embedding technique is used. K. B. Raja et al., [7] have proposed a novel image adaptive stegnographic technique in the integer wavelet transform domain called as the Robust Image Adaptive Steganography using Integer Wavelet Transform. According to data metaphysical prescriptions for parallel Gaussian models of pictures, information

ISSN (O) 2454-9665
ISSN (P) 2454-0663

ought to be hidden in low and middle frequencies ranges of the host image, that have giant energies. Jan Kodovsky and Jessica Fridrich., [8] figured out the precise style principles and components of Steganography schemes for the JPEG format and their security. The perceive ability is evaluated by experimentation employing a state of art blind steganalysis. L.Y. Por et al., [9] have planned a mix of three totally different LSB insertion algorithms on GIF image through the stegcure system. The distinctive feature concerning the secure is having the ability to integrate three algorithms in one Steganography system. By implementing public key infrastructure, an unauthorized user is forbidden from intercepting the transmission of the covert information throughout a communication as a result of the stegokey is merely notable by the sender and also the receiver. Gaetan autoimmune disease Guelvoit., [10] planned a piece that deals with public- key Steganography in presence of passive warden. The most aim is cowl the key data among cover documents while not giving the warden any clue and with none preliminary secret key sharing. This work explores the employment of trellis coded quantization technique to style additional economical public key theme. Mahomed Ali Bani Younes and Aman Jantan., [11] have planned a Steganography approach for information activity. This approach uses the Least Significant bits (LSB) insertion to cover information among encrypted image information. The binary illustration of the information is employed to write the LSB of every computer memory unit among the encrypted image indiscriminately. The hidden information would not alter the receiver to reconstruct constant secret transformation table when extracting it and thus the first image will be reproduced by the inverse of the transformation and cryptography processes. Chang-Chu Chen and Chin-Chen Chang., [12] have planned that information activity theme may be a modification of the LSB-based Steganography exploitation the rule of reflected gray code. The embedding ability and distortion level of our novel methodology square measure almost like those of the easy LSB substitution theme. The distinction is that the LSBs of stego-image don't seem to be continuously constant because the secret bits whereas the easy LSB substitution keeps them equally. Babita Ahuja and, Manpreet Kaur., [13] have given LSB based mostly Steganography formula with high information activity capability, as four LSB's square measure would not hide information, high confidentiality as distortions which might cause suspicions for the intruders, square measure removed through filtering techniques and two level high security is applied. Debnath Bhattacharyya et al., [14] a security model is planned that imposes the idea of secrecy over privacy for text messages. The planned model combines cryptography, Steganography and beside an additional layer of security has been obligatory in between them. Chin-Chen Yangtze et al.,[15] planned a theme embeds a larger-sized secret image whereas maintaining acceptable image quality of the stego-image and conjointly improved image activity theme for grayscale pictures supported wet paper committal to writing.

This paper is to match the performance of two methodologies that square measure accustomed to hiding the information for providing security using watermarking. Digital watermarking could be a technology for embedding numerous styles of data in digital content. In general, data for shielding copyrights and proving the validity of knowledge is embedded as a watermark. I would like to insert such data in digital content using digital watermark technology. During this paper two ways, square measure enforced and their performance square measure compared to seek out the most effective methodology to cover the information with top quality. The primary methodology providing information activity security using the point using C-PEE approach. The

ISSN (O) 2454-9665
ISSN (P) 2454-0663

second methodology uses SMVQ approach for providing the protection by hiding the information. To analyze the performance of that methodology many performance metrics are used. This paper uses Peak signal-to-noise (PSNR), Structural Similarity Index (SSIM), Mean square Error (MSE), and Root Mean square Error (RMSE) to analyze the performance. From the experimental results, it is shown that the SMVQ methodology performs higher than the opposite methodology.

The remainder of the paper is organized as follows: In Section II, the overview of the first method is presented. In Section III, the second method is specifically depicted, including its design idea and practical implementation approach. In Section IV, the performance of the three methods is compared. Finally, conclusions are made in Section V.

II DATA EMBED AND EXTRACT USING C-PEE ALGORITHM

In this paper, an efficient RDH method is proposed based on PEE of multiple histograms. For each pixel, its prediction value and complexity measurement are first computed according to its context, then multiple histograms are generated by counting the prediction-errors for different complexity levels. Finally, data embedding is implemented according to the proposed embedding strategy based on multiple histograms modification. Moreover, to optimize the embedding performance, the expansion bits are adaptively selected in each generated histogram such that the distortion is minimized. Experimental results have shown that the proposed method outperforms the previous PEE-based techniques and some state-of-the-art methods by improving the marked image quality. However, one drawback of our method is the limited embedding capacity. In the future, we plan to extend the technique of multiple histograms modification to high capacity RDH to further enhance its practicability. In addition, incorporating advanced predictor into our method is also a topic worthy of investigation in the future study.

The flowchart of the embedding and extraction method is illustrated in Fig. 1 and Fig. 2. The further details of these modules are discussed below:

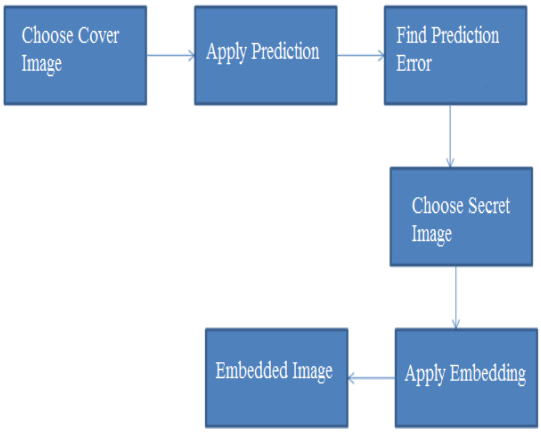

Fig. 1. Overall Embedding Block Diagram of Method1

International Journal of Innovative Research in Science and Engineering
Vol. No.3, Issue 02, February 2017
www.ijirse.com
ISSN (O) 2454-9665
ISSN (P) 2454-0663

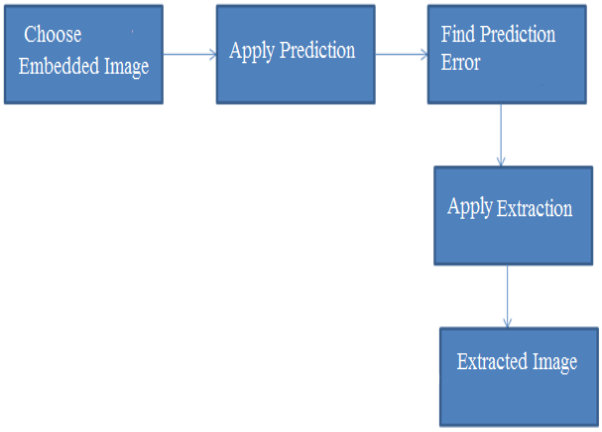

Fig. 2. Overall Extraction Block Diagram of Method1

2.1. Embedding

The first step of these PEE-based methods is the generation of PEH. First of all, in a specific scanning order, the cover pixels are collected into a one-dimensional sequence as (x1, . . . , xN) where N is the total number of collected

pixels. Then, a predictor is employed to predict each xi, and the prediction value denoted by xi should be rounded off if it is not an integer. Next, the prediction-error is computed by

$$e_i = x_i - \widehat{x_i}.$$

Finally, the prediction-error sequence (e1, . . . , eN) is derived and the corresponding PEH denoted by h can be established as

$$h(e) = \#\{1 \le i \le N : e_i = e\}, \quad \forall e \in \mathbb{Z}$$

where # means the cardinal number of a set. The second step of PEE-based methods is the modification of PEH. We now introduce the PEH modification mechanisms for the above four types of PEE-based methods, respectively.

After PEH generation, the C-PEE embedding procedure contains following steps. First, for a Prediction-Error (i.e.), it is expanded or shifted as

$$\widetilde{e_i} = \begin{cases} e_i + m, & \text{if } e_i = 0 \\ e_i - m, & \text{if } e_i = -1 \\ e_i + 1, & \text{if } e_i > 0 \\ e_i - 1, & \text{if } e_i < -1 \end{cases}$$

where m ∈ {0, 1} is a to-be-embedded data bit. With (3), the bins −1 and 0 are expanded to embed data, while other bins are shifted to create vacancies to ensure the reversibility. Then, the cover pixel xi is modified to _xi = _xi + _ei to

International Journal of Innovative Research in Science and Engineering
Vol. No.3, Issue 02, February 2017
www.ijirse.com
ISSN (O) 2454-9665
ISSN (P) 2454-0663

generate the marked pixel. Notice that the above procedure will stop once all data bits are embedded, i.e., only the cover pixels (x1, . . . , xNend) need to be processed where Nend ≤ N is the smallest index such that the payload can be embedded into the first Nend cover pixels.

2.2 Extraction

The C-PEE extraction and image restoration procedure can be summarized as follows. First, determine the prediction_xi of marked pixel _xi for each i ∈ {1, . . . , Nend}. The marked The C-PEE extraction and image restoration procedure can be summarized as follows. First, determine the prediction_xi of marked pixel _xi for each i ∈ {1, . . . , Nend}. The marked

$$e_i = \begin{cases} \widetilde{e}_i, & \text{if } \widetilde{e}_i \in \{-1, 0\} \\ \widetilde{e}_i - 1, & \text{if } \widetilde{e}_i > 0 \\ \widetilde{e}_i + 1, & \text{if } \widetilde{e}_i < -1. \end{cases}$$

Meanwhile, the embedded data bit can be extracted as m = 0 if _ei ∈ {−1, 0}, or m = 1 if _ei ∈ {−2, 1}. Finally, restore the cover pixel as xi = _xi + ei . A key issue for the reversibility of C-PEE is that the prediction values obtained by decoder should be the same as those of encoder. For example, by using Median-Edge-Eetector (MED) or Gradient-Adjusted-Predictor (GAP) which is based on half-enclosing casual pixels for prediction, the decoder can inversely scan and process pixels to get the same prediction values.

III DATA EMBED AND EXTRACT USING SMQV ALGORITHM

A number of data hiding and compression schemes are proposed in the communication system due to the development of technology. As it is an open network environment the secret or private data should be secured. By using the data hiding and compression schemes this system can be possible effectively. The present machine leads to a more wide variety of drawbacks like steeply-priced value, extra facts will be lost, greater distortion, confined hiding capacity and so forth. Many statistics hiding schemes for compressed codes are JPEG, JPEG2000, vector quantization. Within the above 3 schemes vector quantization is pretty simple and the cost is effective. By using the strategies like adaptive information hiding method for VQ compressed photograph, using code phrase clustering strategies the attacker has the possibility to intercept the compressed photograph without the watermark records embedded.

International Journal of Innovative Research in Science and Engineering
Vol. No.3, Issue 02, February 2017
www.ijirse.com
ISSN (O) 2454-9665
ISSN (P) 2454-0663

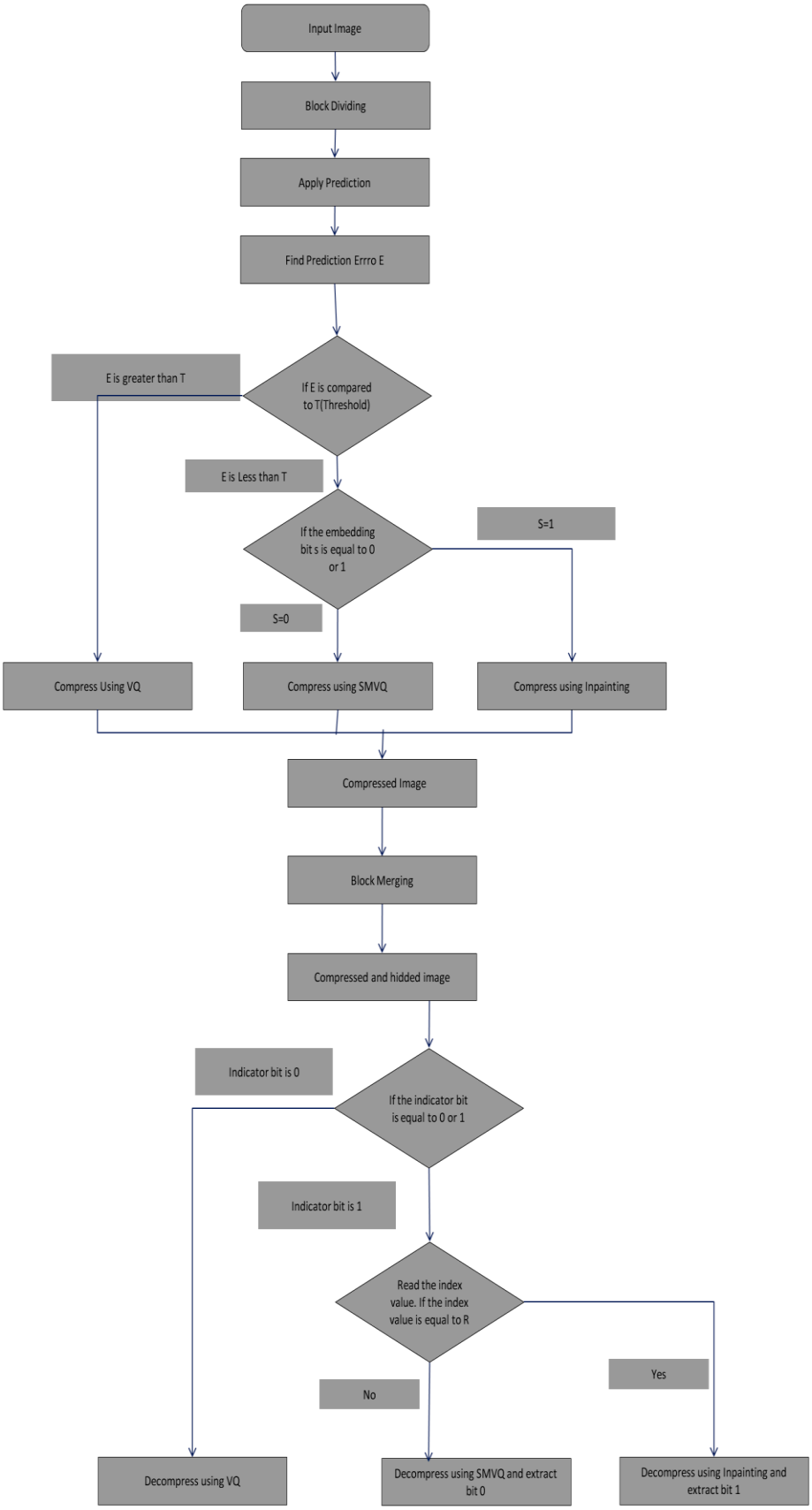

Fig. 3. Overall Block Diagram of Method2

ISSN (O) 2454-9665
ISSN (P) 2454-0663

Therefore the two schemes once performed separately can provide lower potency in applications. The improved version of vector quantization is facet match vector quantization to extend the compression magnitude relation. Using compression with knowledge activity hiding using SMVQ and image inpainting offers high activity capacity; improved implementation and image recovery. It also can avoid the chance of the attack from interceptors. To avoid this downside, the joint knowledge activity and compression techniques for digital image process. This technique supported the facet match vector quantization (SMVQ) and image inpainting. This SMVQ and Image inpainting rely on the embedding bits. The planned methodology has the activity capability, compression magnitude relation, and decompression quality. Flow sheet of the general rule area unit given in Fig.3. The implementation details of the steps of the rule area unit mentioned within the following subsections.

3.1 Choose an image

To choose the image for embedding method. The pictures area unit JPEG, Gif, PNG and the other format. Opt for anyone image and given to the block dividing.

3.2 Apply Block dividing

First provide the block size and apply the block dividing. The image is split into little blocks and also the perform applies in every block. During this paper, block dividing is employed to divide into blocks as an instance 32, 64 etc. Every block applies all operations.

3.3. Apply prediction

After block dividing applies the prediction. Get the input image from information. And apply prediction to envision the image to be redundant. Repeat this method once more and once more. Finally, it produces the reconstructed image. The advantage of prediction secret writing to get rid of the redundancy from the image pattern.

3.4. Prediction error

After prediction verify the prediction error. The prediction can not be properly foretold. That the prediction errors occur and take away the redundant pictures. A prediction error term contains the common and also the least variety of 1's that is to spot the prediction errors.

3.5 Embedding

Embedding is that the method of mixing the initial and key image. The key image prices area unit arbitrarily selected and every value is embedded with the initial image. The embedded image looks to be just like the original image. Then the embedded image is employed to send to the receiver facet.

3.6 Finding the threshold Value:

1. choose an initial estimate for T (typically the typical gray level within the image)

ISSN (O) 2454-9665
ISSN (P) 2454-0663

2. Segment the image using T to supply two groups of pixels: G1 consisting of pixels with gray levels >T and G2 consisting pixels with gray levels ≤ T

3. Cipher the typical gray levels of pixels in G1 to relinquish μ1 and G2 to relinquish μ2

4. Cipher a brand new threshold value:

5. Repeat the steps 2 – 4 until the difference in T in successive iterations is less than a predefined limit T_∞

3.7 Extraction

Extraction is that the method of separating the first and key image from the embedded image.

3.8 Algorithmic program for Embedding

This embedding algorithmic program is employed to mix the key image and original image. This project the embedding is employed for the compression.

1. The input image is split into blocks. The blocks are predicted and find the prediction error.

2. The prediction error is larger than the threshold value then vector quantization is employed for compression.

3. The prediction cost under or adequate the threshold value then embedding the watermark bit zero or one.

4. If the embedding bit adequate zero then aspect Matching Vector quantization is employed for compression.

5. The embedding bit is adequate one then image inpainting is employed for compression.

3.9 Algorithmic program for Extraction

This Extraction algorithmic program is employed to separate the first image and this project extract the watermark bit.

1.The embed image is given to the input of extraction. The input image is split into blocks.

2. Take the indicator bit zero and one.

3. The indicator bit is adequate zero then browse the index price and apply the inverse method of VQ compression and conjointly extract the watermark bit.

4. The indicator bit is adequate one. Browse the index values for the key pictures.

5. If the index values area unit equal then apply the inverse method of SMVQ compression and extract the watermark bit zero.

6. Otherwise apply the inverse method of image inpainting and extract the watermark bit one.

IV PERFORMANCE ANALYSIS

4.1Expiremental Images

Experiments were performed on a group of color snapshots to verify the effectiveness of the proposed scheme. For the experimental reason, numerous requirements, 512 × 512 cowl snapshots are taken. A number of those pixels, i.e., Lena, Barbara, Babbon, Peppers, Sailboat, and Tiffany, are proven in Figure 4.

International Journal of Innovative Research in Science and Engineering
Vol. No.3, Issue 02, February 2017
www.ijirse.com
ISSN (O) 2454-9665
ISSN (P) 2454-0663

Fig. 4. Expiremental Images

4.2. Performance Analysis

To evaluate the performance of the Steganography techniques many performance metrics area units obtainable. This paper uses the PSNR, SSIM, MSE and RMSE to analyses the performance

.4.2.1. Peak Signal-to-Noise-Ratio

The peak S/N (PSNR) is employed to gauge the standard between the stego image and also the original image. The PSNR formula is outlined as follows:

$$PSNR = 10 \times \log 10 \frac{255 \times 255}{\frac{1}{H \times W} \sum_{x=0}^{H-1} \sum_{y=0}^{W-1} [f(x,y) - g(x,y)]^2} dB$$

where H and W area unit the height and width of the image, severally; and f(x,y) and g(x,y) area unit the gray levels situated at coordinate (x,y) of the first image and attacked image, respectively.

4. 2.2 Structural Similarity Index

The structural similarity index may be a technique for measuring the similarity between the stego image and also the original image.

$$SSIM\ (y, \hat{y}) = \frac{\left(2_{\mu_y \mu_{\hat{y}}} + c_1\right)(2\sigma_{y\hat{y}} + c_2)}{(\mu_y^2 + \mu_{\hat{y}}^2 + c_1)(\sigma_y^2 + \sigma_{\hat{y}}^2 + c_2)}$$

where, $\hat{Y}$ is that the stego image, the Y is that the original image, μ is that the mean and also the variance.

4.2.3. Mean Square Error

The Mean Square Error (MSE) is employed to gauge the distinction between a stego image and also the original image. The MSE are often calculated by

International Journal of Innovative Research in Science and Engineering
Vol. No.3, Issue 02, February 2017
www.ijirse.com
ISSN (O) 2454-9665
ISSN (P) 2454-0663

$$MSE = \frac{1}{n}\sum_{i=1}^{n}(\hat{Y}_i - Y_i)^2$$

,

where, $\hat{Y}$ is the stego image and the Y is the original image.

4.2.4 Root Mean Square Error

The Root Mean Square Error (RMSE) may be a often used live of the distinction between stego image values and

$$RMSE = \sqrt{\frac{\sum_{i=1}^{n}(\hat{Y}_i - Y_i)^2}{n}}$$

also the original image values.

where $\hat{Y}$ is stego image and Y is original image.

To evaluation the performance of the proposed gadget, it is in comparison with numerous strategies by the use of the performance metrics that are stated above. That is shown inside the below tables and graphs.

Table. 1 PSNR for two methods

Methods	***PSNR***
C-PEE	52.42
SMVQ	54.63

This indicates that data hiding using SMVQ method is better than C-PEE technique. In vacating room after encryption space for embedding data is found out after encrypting the image. Therefore exact recovery of original image cannot be guaranteed.

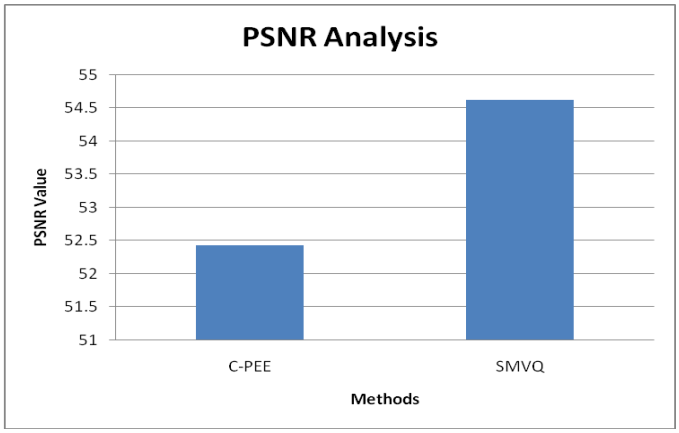

Fig. 5 PSNR Analysis

Methods	***SSIM***
C-PEE	0.94
SMVQ	0.96

Table. 2 SSIM for Two methods

International Journal of Innovative Research in Science and Engineering
Vol. No.3, Issue 02, February 2017
www.ijirse.com
ISSN (O) 2454-9665
ISSN (P) 2454-0663

It was observed that irrespective of image format, showing best results of structural similarity Index (SSIM) is SMVQ than C-PEE.

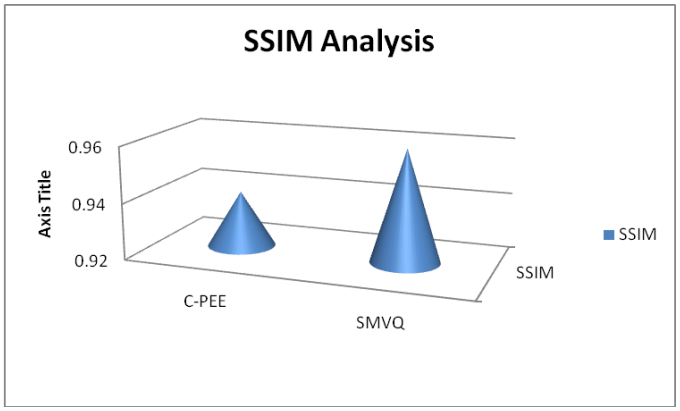

Fig. 6 SSIM Analysis

Table. 3 MSE for two methods

Methods	*MSE*
C-PEE	3.95
SMVQ	2.61

Compared the two methods SMVQ is less MSE value in C-PEE methods.

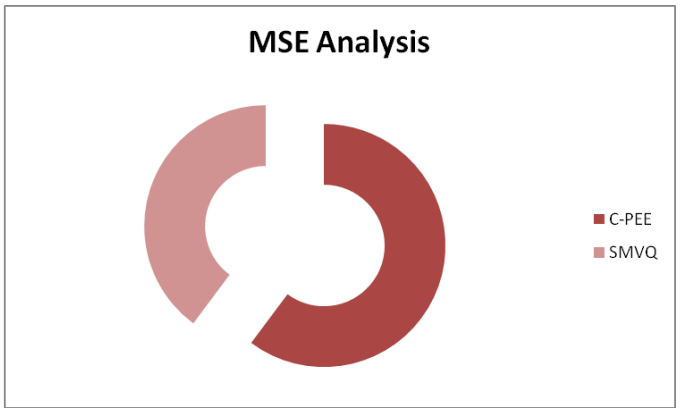

Fig.7 MSE Analysis

Table.4 RMSE for two methods

Methods	*RMSE*
C-PEE	1.98746069
SMVQ	0.8362638

Compared the two methods SMVQ is less RMSE value in RMSE Analysis.

ISSN (O) 2454-9665
ISSN (P) 2454-0663

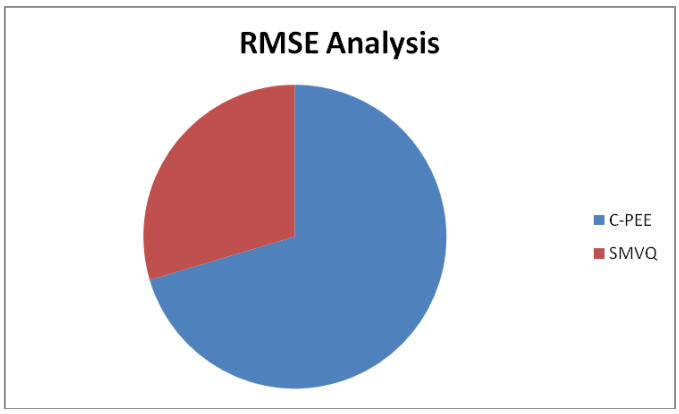

Fig. 8 RMSE Analysis

V CONCLUSION

This paper is to check the performance of two techniques which are used to hide the information for providing security exploitation watermarking. Digital watermarking may be a technology for embedding varied varieties of information in digital content. In general, information for shielding copyrights and proving the validity of the information is embedded as a watermark. We want to introduce such information in digital Content exploitation digital watermark technology. During this paper two ways, square measure compared to search out the most effective technique to cover the information with prime quality. The primary technique providing information concealment security exploitation the blind spot exploitation C-PEE approach. The second technique uses SMVQ approach for providing the protection by concealment the information. To analyze the performance of those technique many performance metrics square measure used. This paper uses Peak ratio (PSNR), Structural Similarity Index (SSIM), Mean square Error (MSE), and Root Mean square Error (RMSE) to analyses the performance. From the experimental results, it's shown that the SMVQ technique performs advanced than the opposite technique.

REFERENCES

[1] Neil F. Johnson and Sushil Jajodia, "Steganalysis: The Investigation of Hidden Information," *IEEE conference on Information Technology, pp. 113-116, 1998.*

[2] Lisa M.Marvel and Charles T. Retter, "A Methodlogy for Data Hiding using Images," *IEEE conference on Military communication, vol. 3, Issue. 18-21, pp. 1044-1047, 1998.*

[3] Giuseppe Mastronardi, Marcello Castellano, Francescomaria Marino, "Steganography Effects in Various Formats of Images. A Preliminary Study," *International Workshop on Intelligent data Acquisition and Advanced Computing Systems: Technology and Applications, pp. 116-119, 2001.*

[4] LIU Tong, QIU Zheng-ding "A DWT-based color Images Steganography Scheme" *IEEE International Conference on Signal Processing, vol. 2, pp.1568-1571, 2002.*

ISSN (O) 2454-9665
ISSN (P) 2454-0663

[5] M. Mahdavi, Sh. Samavi, N. Zaker and M. Modarres-Hashemi, "Steganalysis Method for LSB Replacement Based on Local Gradient of Image Histogram," *Journal of Electrical and Electronic Engineering, vol. 4, no. 3, pp. 59-70, 2008.*

[6]Shilpa P. Hivrale, S. D. Sawarkar, Vijay Bhosale, and Seema Koregaonkar "Statistical Method for Hiding Detection in LSB of Digital Images: *An Overview World Academy of Science, Engineering and Technology, vol. 32, pp. 658-661, 2008.*

[7]K. B. Raja, S. Sindhu, T. D. Mahalakshmi, S. Akshatha, B. K. Nithin, M. Sarvajith, K. R. Venugopal, L. M. Patnaik, "Robust Image Adaptive Steganography using Integer Wavelets" *International conference on Communication Systems Software, pp. 614-621, 2008.*

[8]Jan Kodovsky, Jessica Fridrich "Influence of Embedding Strategies on Security of Steganographic Methods in the JPEG Domain" *Proceedings of SPIE, the International Society for Optical Engineering, vol. 6819, pp. 681902.1-681902.13, 2008.*

[9] L. Y. Por, W. K. Lai, Z. Alireza, T. F. Ang, M. T. Su, B. Delina, "StegCure: A Comprehensive Steganographic Tool using Enhanced LSB Scheme," *Journal of WSEAS Transctions on Computers, vol. 8, pp. 1309-1318, 2008.*

[10]Gaetan Le Guelvouit, "Trellis-Coded Quantization for Public-Key Steganography," *IEEE International conference on Acostics, Speech and Signal Processing, pp.108-116, 2008.*

[11]Mohammed Ali Bani Younes and Aman Jantan, "A New Steganography Approach for Images Encryption Exchange by Using the Least Significant Bit Insertion," *International Journal of Computer Science and Network Security, vol. 8, no. 6, pp.247-257, 2008.*

[12]Chang-Chu Chen, and Chin-Chen Chang, "LSB-Based Steganography Using Reflected Grey Code," *The Institute of Electronics, Information and communication Engineers Transaction on Information and System,", vol. E91-D (4), pp. 1110-1116, 2008.*

[13]Babita Ahuja and, Manpreet Kaur, "High Capacity Filter Based Steganography," *International Journal of Recent Trends in Engineering, vol. 1, no. 1, pp.672-674, May 2009.*

[14]Debnath Bhattacharyya, Poulami Das, Samir kumar Bandyopadhyay and Tai-hoon Kim, "Text Steganography: A Novel Approach," *International Journal of Advanced Science and Technology, vol.3, pp.79-85, February2009.*

[15]Chin- Chen Chang, Yung- Chen Chou and Chia- Chen Lin, "A steganography scheme based on wet paper codes suitable for uniformly distributed wet pixels," *IEEE International Symposium on circuits and Systems, pp. 501-504, 2009.*