An Effectual Hybrid Approach Using Data Encryption Standard (DES) and Secured Hash Algorithm (SHA) for Image Steganography

Rituraj Gaur, Dr. RekhaVig and Ms. AmanpreetKaur
1M.Tech Student, 2 Associate Professor,3 Assistant Professor
Department of Electrical, Electronics and Communication Engineering
The North Cap University, Gurugram, Haryana, India.

Abstract:- Today Security of data is of foremost importance in today's world. Security has become one of the most important factor in communication and information technology. For this purpose steganography is used. Steganography is the art of hiding secret or sensitive information into digital media like images so as to have secure communication. In this paper we present and discuss LSB (Least Significant Bit) based image steganography with DES SHA algorithm so as to provide an extra layer of security

*****

1. INTRODUCTION

Steganography is the art of hiding secret or sensitive information into digital media like images so as to have secure communication. In steganography we hide our secret information in some cover image such that one cannot track the message. The original Image is called cover image and the image in which message is embedded is called Stego Image. Steganography can also be done with Text, video, audio and protocol steganography.

There is a difference between cryptography and steganography. Cryptography helps us to keep message content in secret form while steganography helps to keep the existence of the message as a secret. If cryptography is forbidden to use then in that case steganography is very useful.

Today there are many applications of steganography. It is used in defense organizations so that data can be safely circulated, it is used in smart identity cards where the information of the person is secretly stored in the image of the person itself. Some other applications are medical imaging, online voting system Etc.

COVER IMAGE: This image is used to hold the secret information.
STEGO IMAGE: Image holding the embedded message.
SECRET MESSAGE: This is the secret information which is to be embedded with the cover image.

2. LITERATURE REVIEW

The principle parts of data covering up are steganography and steganalysis. Steganography is the craft of concealing mystery or touchy data into advanced media like pictures in order to have secure correspondence. Steganalysis is the specialty of identifying the nearness of steganography. This paper talks about the essential ideas of steganography, the advance of techniques for steganography for pictures in spatial portrayal. The synopsis of strategies for steganography is examined.

GiovaniArdiansyah and Christy Atika et al. [8] Open systems, for example, the Internet are winding up more complex, speedier, and less expensive, so more utilized for data trade. This may improve the probability of secret data from being stolen and abused by unapproved people. This examination proposed a mix of two Steganography areas combined with Cryptography which expected to make secret data more secure and difficult to reach to unapproved people. Messages are scrambled utilizing the 3-DES technique. On the opposite side of the cover picture is disintegrated into four subbands by utilizing DWT. LH, HL, and HH subbands are implanted encoded message utilizing LSB strategy. The last advance, done Inverse DWT (IDWT) to get the stego picture recreation. From the proposed technique is then estimated its quality with PSNR and MSE. With respect to message encryption comes about are estimated utilizing entropy. From the trial comes about acquired PSNR comes about with an estimation of 55.30 dB for picture messages measure 64 * 64 and 49.23 dB for messages estimate 128 * 128. The extraction procedure should likewise be possible splendidly with NC 1 and the normal of Entropy of encoded messages are 7.95754 for 64*64 and 7.98904 for 128*128.

Khodaei, M et al. [3] set forward a strategy for information concealing utilizing pixel esteem differencing and LSB substitution. Here a picture is part into squares of two progressive pixels .The distinction of two pixels is computed, and according to the contrast, it will gauge the quantity of installing bits into LSBs of two pixels.

Karthikeyan.B. et al. [4] proposed an approach of cryptography and steganography by sending rotor figure for guaranteed movement of information in an interfered with correspondence channel utilizing 2-bit LSB steganography which helps secluded from everything the data from the gatecrasher. They have likewise advanced [5] a progressed steganographic strategy by LSB substitution on a filtered picture which expands the security level of the message. Notwithstanding this they have displayed [6] a LSB subordinate steganography with multi-layered encryption by utilizing caeser figure system to cover the content in the

picture and encoding it in light of the confusion hypothesis. Additionally they have advanced [7] a composite strategy for concealing data through arbitrary hypothesis and reversible whole number portrayal in which DCT is connected to the picture and is covered up by LSB substitution.

AchmadSolichin et al.[9]The security and protection of the information transmitted is a critical part of the trading of data on the Internet arrange. Cryptography and Steganography are two of the most generally utilized computerized information security procedures. In this exploration, we proposed the mix of the cryptographic strategy with Data Encryption Standard (DES) calculation and the steganographic technique with Discrete Cosine Transform (DCT) to build up an advanced information security application. The application can be utilized to secure archive information in Word, Excel, Powerpoint or PDF organize. Information scrambled with DES calculation and further covered up in picture cover utilizing DCT calculation. The outcomes demonstrated that the nature of the picture that has been embedded (stego-picture) is still in a decent classification with a normal PSNR estimation of 46.9 dB. Additionally, the trial comes about demonstrate that the normal computational time of 0.75 millisecond/byte, a normal size increment of 4.79 times and a win rate of 58%. This exploration can help tackle the issue of information and data security that will be sent through an open system like the web.

B. Karthikeyan et al. [10] Steganography has turned out to be one of the broadly utilized instruments in this day and age for concealing data inside another information or a picture. It is a procedure that takes cryptography to the following level by disguising the nearness of a message itself. Information Encryption Standard calculation is such a cryptographic key which is connected to a square of plain content to change over it into a figure content and the other way around. This paper exhibits an inventive plan to shroud a message inside a picture of any measurement by scrambling the message through Data Encryption Standard calculation and covering the message by applying LSB encoding strategy in a winding way consequently improving the trouble of the decoder. The primary target is that, securing of information turns out to be more strong and shrouded than the past ones.

***KanikaAnand and Er.Rekha*Sharma** [11] thinks about the LSB and MSB based steganography with each other as indicated by the MSE (Mean square blunder) and PSNR (Peak flag to clamor proportion) values. LSB works by supplanting the minimum noteworthy piece of the pixel estimation of the cover picture (in the greater part of the cases eighth piece is supplanted). In MSB most huge piece of the pixel esteem is changed in the cover picture. Procedures are examined in detail in this paper. In this paper the outcomes demonstrate that LSB Based Steganography is superior to anything MSB construct steganography in light of the premise of MSE and PSNR esteems.

3. Proposed methodology

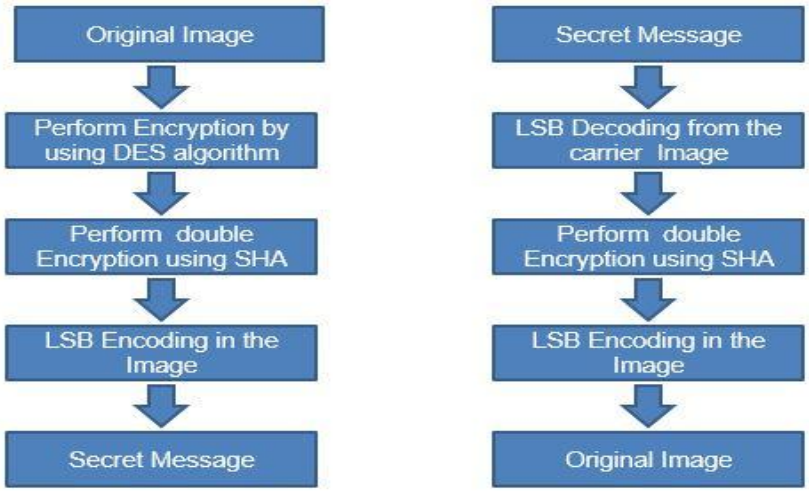


Figure 1: Flow Diagram of Proposed Approach

In our proposed hybrid approach are two most popular algorithms and Encryption and Decryption Technique**:**

(A) Data Encryption Standard Algorithm

(B) Secure Hash Algorithm

(C) LSB Based Steganography

A. DES Algorithm Based Steganography Encryption and Decryption

The DES (Data Encryption Standard) calculation is the most generally utilized encryption calculation on the planet. For a long time, and among numerous individuals, "mystery code making" and DES have been synonymous. What's more,

regardless of the current upset by the Electronic Frontier Foundation in making a $220,000 machine to split DES-scrambled messages, DES will live on in government and managing an account for quite a long time to get through an existence expanding rendition called "triple-DES."

DES is an execution of a Feistel Cipher. It utilizes 16 round Feistel structure. The piece estimate is 64-bit. However, key length is 64-bit, DES has a successful key length of 56 bits, since 8 of the 64 bits of the key are not utilized by the encryption calculation (work as check bits as it were). General Structure of DES is delineated in the following figure

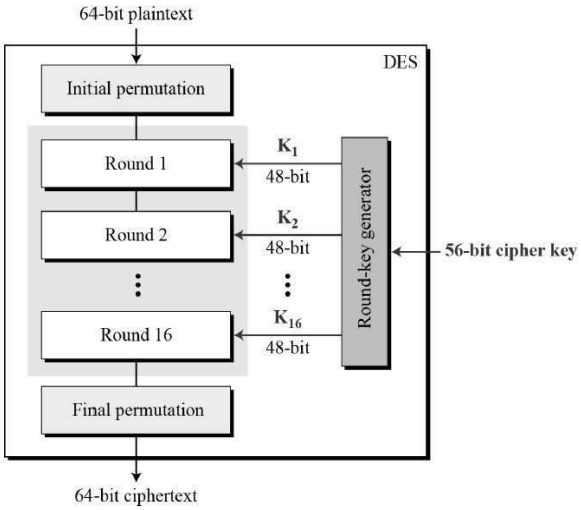


Figure 2: Data Encryption Standard (DES) to generate the Cipher Key

Since DES is based on the Feistel Cipher, DES is having the following step:

- Round function
- Key schedule
- Any additional processing − Initial and final permutation

B. Secure Hash Algorithm Based Steganography Encryption and Decryption

The Secure Hash Algorithms are a group of cryptographic hash capacities distributed by the National Institute of Standards and Technology (NIST) as a U.S. Government Information Processing Standard (FIPS), including:
SHA-0: A retronym connected to the first form of the 160-piece hash work distributed in 1993 under the name "SHA". It was pulled back soon after production due to an undisclosed "huge defect" and supplanted by the marginally reexamined rendition SHA-1.
SHA-1: A 160-piece hash work which takes after the prior MD5 calculation. This was planned by the National Security Agency (NSA) to be a piece of the Digital Signature Algorithm. Cryptographic shortcomings were found in SHA-1, and the standard was never again affirmed for most cryptographic uses after 2010.
SHA-2: A group of two comparable hash capacities, with various piece sizes, known as SHA-256 and SHA-512. They vary in the word estimate; SHA-256 utilizations 32-bit words where SHA-512 utilizations 64-bit words. There are likewise truncated forms of every standard, known as SHA-224, SHA-384, SHA-512/224 and SHA-512/256. These were likewise planned by the NSA.
SHA-3: A hash work in the past called Keccak, picked in 2012 after an open rivalry among non-NSA fashioners. It bolsters similar hash lengths as SHA-2, and it's inside structure contrasts essentially from whatever is left of the SHA family.

C. LSB BASED STEGANOGRAPHY

LSB works by replacing the least significant bit of the Pixel value of the cover image (in most of the cases 8th bit is replaced).

Embedding the text inside the image:

- Calculate the Pixels of the image.
- Make a loop through the pixels.
- In each pass get the red, green and blue value of pixels.
- Make the LSB of each RGB pixel to zero.
- Get the character to be hidden in binary form and hide the 8-bit binary code in the lsb of pixels.
- Repeat the process until all the characters of the image are hidden inside the image.

Extracting the embed message from the image:

- Calculate the pixels of the image.
- Loop through the pixels of the Image until one find the 8 consecutive zero.
- Pick LSB from each pixel element and then convert it into the character.

4. Experimental Details and Results

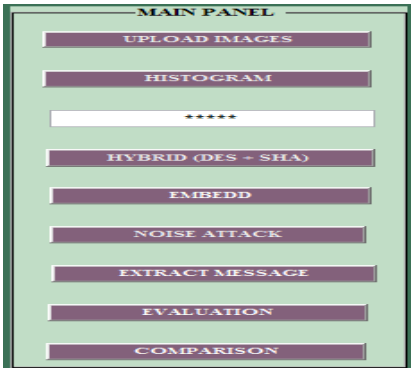


Figure 3: Main Pane of GUI

The proposed approach deals with the hybrid approach of encryption and cryptography using DES which is popularly known as Data Encryption Scheme and also the SHA-512 algorithm which will be the robust approach to perform the steganography process. For evaluate purpose of proposed hybrid approach, we take statistical technique Mean Square Error (MSE) and Peak Signal to Noise Ratio (PSNR). We take 6 sample images for steganography andapplying DES and SHA for encrypting and decrypting the message:

The figure 2 shows the main panel which deals with the GUI toolbox for the proposed work implementation. It also deals with the pushbuttons, edit texts and static texts.

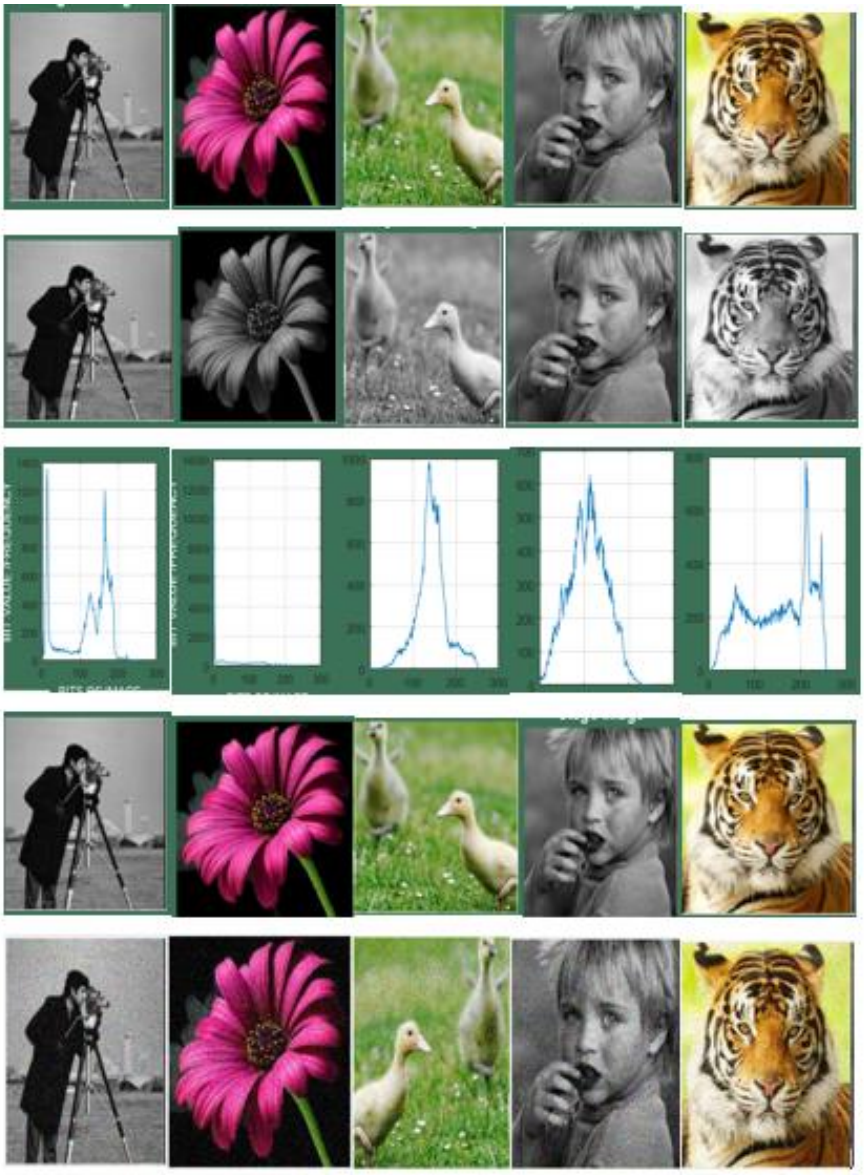


Figure 4: In first row Original Image, In second row are Gray Scale Image, In third row are histogram of cover Image, In forth row are Steganography image after Encryption and the last row showing Noise attacked Image

1)Output of DES and SHA

Fig 5: Output of DES and SHA

In the above figure shows the output in the encrypted form for the evaluation of steganography approach. The left part shows the DES output and Right part shows the SHA output and then noisy attacked image which is done for the evaluation of the performance of the proposed work in the presence of the attack which shows that our proposed approach will help to evaluate and handle the embedding and extraction process

(1) MSE and PSNR

MSE and PSNR of the proposed approach and shows that the system is able to achieve high peak signal to noise ratio and less mean square error rate for the high authentication and performance of the system to achieve high steganography approach.

Base Approach:

A) Without noise

For the base approach the below table shows the values of PSNR and MSE for 50, 100 and 200 characters for five different figures without noise attack.

50 characters			100 characters		200 characters	
Figure	**PSNR**	**MSE**	**PSNR**	**MSE**	**PSNR**	**MSE**
1.	50.1872	0.018014	48.3909	0.04154	42.5599	0.03389
2.	51.8412	0.08978	50.4658	0.03942	45.2788	0.029032
3.	53.1693	0.014588	48.9877	0.016151	41.8139	0.038475
4.	51.9621	0.011751	48.3152	0.025759	42.5906	0.078553
5.	54.3218	0.020948	48.3104	0.040967	41.1003	0.053627

Table 1

Proposed Approach:

A) Without noise

For the proposed approach the below table shows the values of PSNR and MSE for 50, 100 and 200 characters for five different figures without noise attack.

For 50 characters			For 100 characters		For 200 characters	
Figure	**PSNR**	**MSE**	**PSNR**	**MSE**	**PSNR**	**MSE**
1.	60.4535	0.011375	56.7535	0.01602	54.9041	0.029247

2.	61.7855	0.021801	58.8158	0.017881	57.8168	0.015299
3.	61.2577	0.012203	55.2211	0.018967	58.0418	0.015438
4.	59.5259	0.010552	56.6234	0.016186	54.2449	0.025319
5.	60.3035	0.010395	57.3303	0.020313	55.054	0.031533

Table 2

B) GAUSSIAN NOISE ATTACK:

For the proposed approach the below table shows the values of PSNR and MSE for 50, 100 and 200 characters for five different figures with Gaussian noise attack.

For 50 characters			**For 100 characters**		**For 200 characters**	
Figure	**PSNR**	**MSE**	**PSNR**	**MSE**	**PSNR**	**MSE**
1.	59.6758	0.078509	58.1026	0.016007	55.6141	0.029483
2.	61.7004	0.042918	58.9711	0.091071	57.9325	0.015098
3.	59.4697	0.077641	56.7272	0.018975	58.274	0.015098
4.	59.584	0.072545	57.2682	0.016138	55.125	0.025523
5.	59.1283	0.089937	56.9352	0.020432	53.5447	0.031674

Table 3

C) SALT &PEPPER NOISE ATTACK:

For the proposed approach the below table shows the values of PSNR and MSE for 50, 100 and 200 characters for five different figures with salt and pepper noise attack.

For 50 characters			**For 100 characters**		**For 200 characters**	
Figure	**PSNR**	**MSE**	**PSNR**	**MSE**	**PSNR**	**MSE**
1.	60.2724	0.078401	57.5394	0.016104	53.8306	0.029245
2.	63.4473	0.046166	58.3605	0.086764	55.3932	0.01527
3.	61.6349	0.075832	57.7897	0.018986	56.6559	0.015332
4.	60.992	0.070111	56.6076	0.016081	54.0682	0.025342
5.	60.5853	0.090453	56.4552	0.020248	55.5418	0.031755

Table 4

D) POISSON NOISE ATTACK:

For the proposed approach the below table shows the values of PSNR and MSE for 50, 100 and 200 characters for five different figures with poisson noise attack.

For 50 characters			For 100 characters		For 200 characters	
Figure	PSNR	MSE	PSNR	MSE	PSNR	MSE
1.	60.189	0.07965	57.0735	0.016211	53.7049	0.029204
2.	61.5602	0.044328	59.0138	0.087863	56.9651	0.015382
3.	61.5293	0.07975	56.338	0.019259	57.1003	0.015329
4.	61.2361	0.072216	56.6935	0.016426	55.0247	0.025353
5.	60.9814	0.089269	57.7275	0.020248	54.3876	0.031508

Table 5

Calculation of Execution time:

A) Without noise attack

For the proposed approach the below table shows the execution time in seconds for 50, 100 and 200 characters for five different figures without noise attack.

	50 Character	**100 character**	**200 character**
1.	0.1263 sec	0.10965 sec	0.16311 sec
2.	0.11704 sec	0.14663 sec	0.1496 sec
3.	0.11702 sec	0.058277 sec	0.11778 sec
4.	0.1071 sec	0.11259 sec	0.112 sec
5.	0.1183 sec	0.1065 sec	0.13471 sec

Table 6

B) With Gaussian noise attack :

For the proposed approach the below table shows the execution time in seconds for 50, 100 and 200 characters for five different figures with Gaussian noise attack.

	50 Character	**100 character**	**200 character**
1.	0.13266 sec	0.29288 sec	0.13661 sec
2.	0.13456 sec	0.12976 sec	0.1337 sec

3.	0.13103 sec	0.096061 sec	0.14362 sec
4.	0.12096 sec	0.1057 sec	0.13594 sec
5.	0.12056 sec	0.121955 sec	0.15406 sec

Table 7

C) With Salt & Pepper noise attack :

For the proposed approach the below table shows the execution time in seconds for 50, 100 and 200 characters for five different figures with salt and pepper noise attack

	50 Character	**100 character**	**200 character**
1.	0.14187sec	0.11876 sec	0.1428 sec
2.	0.14991 sec	0.14329 sec	0.14698 sec
3.	0.14527 sec	0.13643 sec	0.113592 sec
4.	0.12957 sec	0.053142 sec	0.113911 sec
5.	0.113764 sec	0.1185 sec	0.18215 sec

Table 8

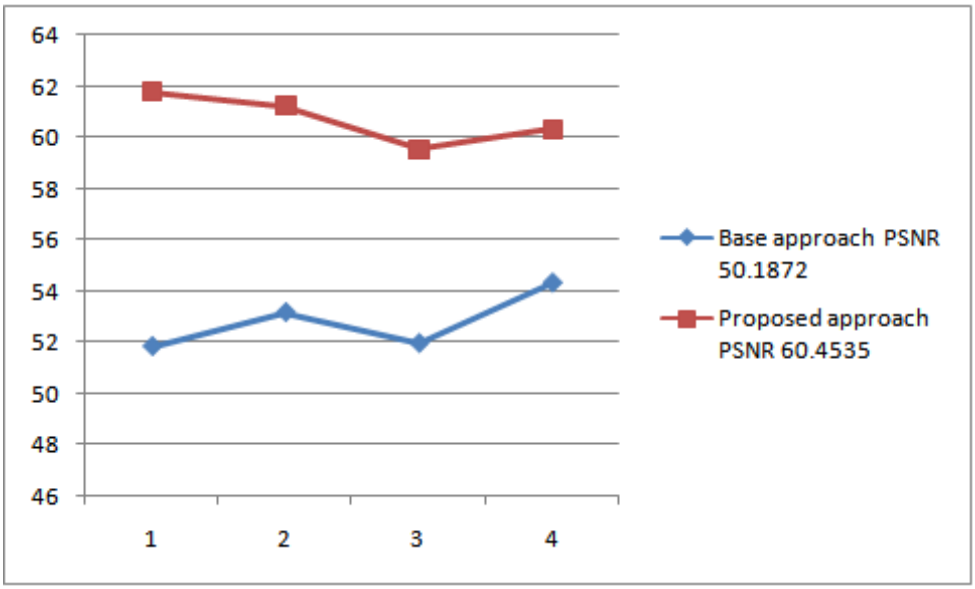
D) With Poisson noise attack:

For the proposed approach the below table shows the execution time in seconds for 50, 100 and 200 characters for five different figures with Poisson noise attack

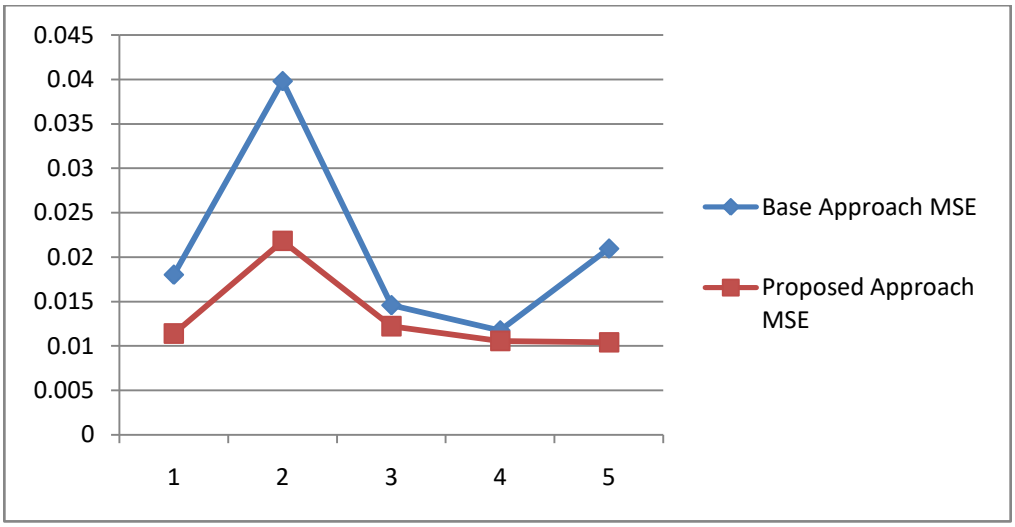
	50 Character	**100 character**	**200 character**
1.	0.12141 sec	0.12872 sec	0.15283 sec
2.	0.15861 sec	0.155 sec	0.15568 sec
3.	0.14737 sec	0.13689 sec	0.14274 sec
4.	0.13877 sec	0.056642 sec	0.17244 sec
5.	0.13829 sec	0.1516 sec	0.18213 sec

Table 9

Comparison of PSNR and MSE for base and proposed approach



Graph 1: Comparison of PSNR



Graph 2: Comparison of MSE

Future Scope

To cover up secret data steganography can be adequately utilized. The goal of any Steganography technique is to shroud most extreme mystery data which is invulnerable to outer assaults and furthermore ought not pass on the way that the cover medium is convey mystery data. In this work it investigates just a little piece of the study of steganography. As another train, there is significantly more innovative work to do, for example, steganography in internet, in printed media and so forth.

Conclusion

In this technique we utilized the DES and SHA with LSB steganography for covering up confidential information since it delivers less bending and picture quality is additionally kept up accordingly the adversary can't realize that secret message is covered up in the image. Alongside this we have incorporated another security level by scrambling the mystery message with a changed s-des calculation. Along these lines, regardless of whether the adversary gets secret message from the picture, he needs to decode the message utilizing adjusted DES calculation which is very troublesome on account of the utilization of table mapping. Our approach additionally gives a strategy to checking the trustworthiness of the secret message. By this the recipient can check whether the secret message has arrived altogether or not.

References

[1] Ms.G.S.Sravanthi, Mrs.B.Sunitha Devi, S.M.Riyazoddin&M.Janga Reddy “A Spatial Domain

Image Steganography Technique Based on Plane Bit Substitution Method"

[2] aek J "(N, 1) secret sharing approach based on steganography with gray digital images", IEEE International Conference on Wireless Communications, Networking and Information Security,2010, Article number 5541793,Pages 325-329.

[3] Khodaei M "Adaptive Data Hiding, Using Pixel-Value-Differencing and LSB Substitution", Institute for Advanced Studies in Basic Sciences (IASBS), Zanjan, Iran, 14 August 2016, Pages1-12.

[4] Sriram S, Karthikeyan B, Vaithiyanathan V, Raj MMA "An approach of cryptography and steganography using rotor cipher for secure transmission"2015 IEEE International Conference on Computational Intelligence and Computing Research, ICCIC 2015, 17 March 2016, Article number 7435669.

[5] Karthikeyan B, Ramakrishnan S, Vaithiyanathan V, Sruti S, Gomathymeenakshi M "An improved steganographic technique using LSB replacement on a scanned path image", International Journal of Network Security, Volume 16, Issue 1, January 2014, Pages 14-18.

[6] Charan GS, NithinKumar SSV, Vaithiyanathan V, Divya Lakshmi, Karthikeyan B "A novel LSB based image steganography with multi-level encryption", ICIIECS 2014-2015, IEEE International Conference on Innovations in Information, Embedded and Communication Systems, 12 August 2015, Article number 7192867.

[7] Nithin Kumar SSV, Charan GS, Karthikeyan B, Vaithiyanathan V, Rajasekhar Reddy M "A hybridapproach for data hiding through chaos theory and reversible integer mapping", International Conference on Computational Intelligence, Cyber Security and Computational Models, ICC3 2015; Coimbatore; India, Volume 412, 2016, Pages 483-49

[8] GiovaniArdiansyah; Christy Atika Sari; De Rosal Ignatius Moses Setiadi; EkoHari Rachmawanto2017 2nd International conferences on Information Technology, Information Systems and Electrical Engineering (ICITISEE) Year: 2017

[9] AchmadSolichin; Erwin Wahyu Ramadhan 2017 3rd International Conference on Science in Information Technology (ICSITech)

[10] B. Karthikeyan; A. Deepak; K. S. Subalakshmi; Anishin Raj M M; V. Vaithiyanathan 2017 Third International Conference on Advances in Electrical, Electronics, Information, Communication and Bio-Informatics (AEEICB)

[11] KanikaAnand, Er. Rekha Sharma, Comparison of LSBand MSB Based Image Steganography, Ijarssce, Volume 4, Issue 8, August 2014