A Brief Survey on Steganography Techniques in Digital Image Processing

Poonam Sen[1], Prof. Sangeeta Shukla[2]
Department of Electronics & Communication Engineering
Sagar Institute of Research & Technology, Bhopal

Abstract - ***Steganography is the science that includes conveying mystery information in a suitable sight and sound transporter, e.g., picture, sound and feature documents. It goes under the suspicion that if the characteristic is obvious, the purpose of strike is clear, subsequently the objective here is dependably to hide the exact presence of the installed information. The development of fast workstation systems and that of the Internet, specifically, has expanded the simplicity of Information Communication. Unexpectedly, the reason for the advancement is likewise of the dread - utilization of computerized arranged information. In examination with Analog media, Digital media offers a few notable focal points, for example, brilliant, simple altering, high constancy duplicating, pressure and so forth. Anyhow this sort progression in the field of information correspondence in other sense has trekked the dread of getting the information snooped at the time of sending it from the sender to the collector. In this way, Information Security is turning into an entwined some piece of Data Communication. With a specific end goal to address this Information Security Steganography assumes a paramount part. Steganography is the workmanship and art of composing concealed messages in such a path, to the point that nobody separated from the sender and expected beneficiary even acknowledges there is a shrouded message. This paper is an exercise audit of the steganography systems showed up in the literary works. Different picture steganography procedures have been proposed. In this paper, we examine steganography strategies and steganalysis systems.***

Keywords- Steganography, JPEG image, capacity, stego image, security and information hiding

I INTRODUCTION

Steganography is a sort of shrouded correspondence that truly signifies "secured written work" (from the Greek words stegano or "secured" and graphos or "to compose"). The objective of steganography is to shroud a data message inside safe spread medium in such a path, to the point that it is not conceivable even to recognize that there is a mystery message [1, 2]. Intermittently all around history, scrambled messages have been caught however have not been decoded. While this ensures the data covered up in the figure, the block attempt of the message could be as harming in light of the fact that it tells an adversary or foe that somebody is speaking with another person. Steganography takes the inverse approach and endeavors to conceal all confirmation that correspondence is occurring. Basically, the data concealing process in a Steganographic framework begins by recognizing a blanket medium's excess bits (those that could be adjusted without annihilating that medium's trustworthiness). The implanting methodology makes a stego medium by trading these repetitive bits with information from the concealed message. Present day steganography objective is to keep its negligible vicinity imperceptible, however steganographic frameworks, as a result of their obtrusive nature, abandon perceivable follow in the spread medium through adjusting its factual properties, so spies can identify the mutilations in the ensuing stego medium's measurable properties. The procedure of discovering these bends is called Statistical Steganalysis. For the most part talking, data concealing identifies with both watermarking and steganography. A watermarking framework's essential objective is to accomplish an abnormal amount of strength that is, it ought to be difficult to evacuate a watermark without corrupting the information object's quality. Steganography, then again, strives for high security and limit, which regularly involves that the shrouded data is delicate. Indeed trifling adjustments to the stego medium can crush it.

Relational abilities have dependably been the sign of human intelligence. The primitive methods that incorporate hollow drawings, smoke sign, and drums and so on find out that through the years has been the usual way of doing things (mode of operation) of social & business intercourse. The mechanical multiplication in this electronic age has stretched skylines and has enabled associations, countries or partnerships to impart savvy data and be commonly profited by it. Anyway with the rats race to get power, ethics have reverted and has made electronic listening in a prime issue. Any famous arrangement of legislation running from the keeping money segment to the authoritative part of a nation must be behind the floods of

strong security frameworks to ensure it from emotionless and flippant individuals who associate to haul out any significant data they can snatch. Information encryption [3] and Data concealing [4, 5] strategies are potential devices for securing touchy data and thus is generally used to secure the information over an obvious channel from malevolent assailants.

II SYSTEM MODEL

A traditional steganographic framework's security depends on the encoding framework's mystery. Despite the fact that such a framework may work for a period, once it is known, it is basic enough to uncover the whole gained media (e.g., pictures) passing by to check for concealed messages at last, such a steganographic framework comes up short. Current steganographic framework, as demonstrated in Figure 1 endeavors to be discernible just if mystery data is known in particular, a mystery key. Hence, cryptography ought to be included, which holds that a cryptographic framework's security ought to depend singularly on the key material. For the steganography to remain undetected the unmodified spread medium must be kept mystery, in light of the fact that assuming that it is uncovered, an examination between the spread and stego media promptly uncovers the progressions [6, 7]. Steganography has characteristic qualities, for example, identification of little and gigantic honesty, which might be further fortified by presenting regulated varieties in the example of inserting of mystery information.

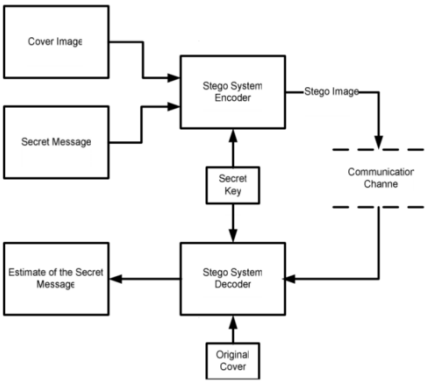

Figure 1. A modern steganography system

The point when these regulated varieties are as distinction in encoding of the mystery information and a pseudo-arbitrary decision of traversal way [8, 9], the discovery gets to be truly lesser than that which might be acquired utilizing numerous created Steganographic calculations. The encryption of mystery information before installing builds the security, as it was, [4].

Three essential sorts of stego frameworks are accessible:

- Pure stego frameworks - no key is utilized.
- Secret-key stego systems - mystery key is utilized.
- Public-key stego systems - open key is utilized.

The method that is followed in this paper will utilize mystery key to encode the shrouded message that will be embodied inside a spread media.

LSB Substitution Method [10]

The most well-known steganographic method in the information concealing field is slightest noteworthy bits substitution. This strategy inserts the altered length mystery bits in the same settled length of pixels. Despite the fact that this system is straightforward, it for the most part causes perceptible mutilation when the amount of implanted bits for every pixel surpasses three. A few versatile systems for steganography have been proposed to decrease the contortion created by LSBS substitution. For instance, versatile techniques fluctuate the amount of implanted bits in every pixel, and they have preferred picture quality over different systems utilizing just straightforward LSBS substitution. Notwithstanding, this is accomplished at the expense of a lessening in the installing limit.

Optimum Pixel Adjustment Procedure [10]

The proposed Optimal Pixel modification Procedure (OPAP) lessens the twisting brought on by the LSB substitution strategy. In OPAP system the pixel quality is balanced after the covering up of the mystery information is carried out to enhance the nature of the stego picture without exasperating the information stowed.

A. Procedure for hiding:

- To begin with a couple of slightest critical bits are substituted with the information to be covered up.
- At that point in the pixel, the bits before the concealed bits are balanced suitably if important to give fewer mistakes.
- Let n LSBs be substituted in each pixel.

- Let d= decimal value of the pixel after the substitution.
- d1 = decimal value of last n bits of the pixel.
- d2 = decimal value of n bits hidden in that pixel.

If(d1~d2)<=(2^n)/2

There after no adjustment is made in that pixel.

Else

If(d1<d2)
d = d – 2^n .
If(d1>d2)
d = d + 2^n .

This d has been converted to binary and written back to pixel.

B. Retrieval:

The recovery takes after the extraction of the slightest huge bits (LSB) as concealing is carried out utilizing straightforward LSB substitution.

C. Advantages:

1. Simple methodology.
2. Easy retrieval.
3.Improved stego-image quality than LSB substitution.

Inverted Pattern Approach (IP) [11]

This altered example LSB substitution methodology utilizes the thought of handling mystery messages before inserting. In this strategy each one segment of mystery pictures is dead set to be upset or not altered before it is implanted. Furthermore, the bits which are utilized to record the change are dealt with as mystery keys or additional information to be re-inserted.

A. The embedding procedure is:

The embedded string is S, the replaced string is R, and the embedded bit string to divided to P parts. Let us consider n-bit LSB substitution to be made. Then S and R are of n-bits length. For P part in i = 1 to P

If MSE (Si, RI) ≤ MSE (Si, Ri)
Choose Si for the embedding
Mark key (i) as logic _0‘
If MSE (Si, RI) ≥ MSE (Si, RI)
Choose S‘i for the embedding
Mark key (i) as logic ‘1‘
MSE – Mean Square Error.
End
Where,
S is the data to be hidden
S‘is the data which is to be hidden in inverted form.

B. Procedure for retrieval is:

The stego-image and the key file are required at the retrieval side.

- First corresponding numbers of LSB bits are retrieved from the stego-image.
- If the key is _0‘, then the retrieved bits are kept as such.
- Else if the key is _1‘, then the bits are inverted.
- The bits are retrieved in this manner from every pixel of the stego-image gives the data hidden.

IP Method Using Relative Entropy [11]

Relative entropy measures the data disparity between two separate sources with an ideal limit got by minimizing relative entropy. In this strategy as opposed to discovering the mean square blunder for modified example approach, the relative entropy is figured to choose whether S or S' suites the pixel. In likelihood hypothesis and data hypothesis, the Kullback– Leibler disparity (likewise data dissimilarity, data addition, or relative entropy) is a non-symmetric measure of the contrast between two likelihood circulations P and Q. It is given by,

$$D(p \parallel q) = \sum_{x \in \chi} p(x) \log \frac{p(x)}{q(x)} = E_p \log \frac{p(X)}{q(X)}$$

A. Embedding procedure is:

Divide the cover image into P blocks of same size, the embedding string is S, and the replaced string is R. For P part in i =1 to P

If rel.entropy (Si, RI) ≤ rel.entropy (Si, RI)
Choose Si for the embedding
Mark key (i) as logic _0‘
If rel.entropy (Si, Ri) ≥ rel.entropy (Si, Ri)
Choose S‘i for the embedding
Mark key (i) as logic _1‘
End
Where,
S is the data to which is to be hidden
S‘is the data to be hidden in inverted form.

B. Procedure for retrieval is:

The stego-image and the key file are required at the retrieval side.

- First consequent numbers of LSB bits are retrieved from the stego-image.

- If the key is ‗0', then the retrieved bits are kept as such.
- Else if the key is ‗1', then the bits are inverted.
- The bits retrieved in this manner from every pixel of the stego-image gives the data hidden

III LITERATURE REVIEW

"Image steganography using discrete fractional fourier transform", 2013, The Fractional Fourier change, as a generalization of the established Fourier convert, was presented numerous years back in math writing. For the upgraded reckoning of fragmentary Fourier change, discrete adaptation of Frft started to be i.e. Dfrft. This paper represents the playing point of discrete fragmentary Fourier convert (Dfrft) as contrasted with different changes for steganography in picture transforming. The reenactment consequence shows same PSNR in both space (time and recurrence) yet Dfrft gives preference of extra stego key i.e. request parameter of this convert.

Table 1: Summary of Literature Review

YEAR	TITLE	APPROACH	RESULT
2013	Image steganography using discrete fractional Fourier transform	Enhanced computation of fractional Fourier transform	PSNR is more and MSE is less
2013	Enhancing the security and quality of LSB based image steganography	Variation of plain LSB algorithm using bit-inversion technique	Improve robustness of steganography
2012	Data hiding in intermediate significant bit planes, a high capacity blind steganographic technique	Based on Data hiding in intermediate significant bit planes, a high capacity blind	Provide high capacity blind steganographic technique
2012	Color image steganography based on modified quantization table	JMQT Steganography method is compared with JPEG-JSteg	Capacity increases and stego size increases
2011	Steganography and steganalysis based on digital image	Analysis based on digital image	High Accuracy and performance
2011	An effective image steganalysis method based on neighborhood information of pixels	Method based on neighborhood information of pixels	Effective results based on neighborhood information of pixels
2010	Image steganography based on adaptive optimal embedding	Using adaptive optimal embedding	High Optimized Results
2009	A novel steganography method for image based on Huffman encoding	Huffman coding is performed over the secret images	High capacity and good invisibility

"Enhancing the security and quality of LSB based image steganography", 2013, This research work is concerned with executing Steganography for pictures, with a change in both security and picture quality. The particular case that is executed here is a variety of plain LSB (Least Significant Bit) calculation. The stego-picture quality is enhanced by utilizing touch reversal method. In this strategy, certain minimum noteworthy bits of spread picture are rearranged after LSB steganography that co-happen with some example of different bits and that diminishes the amount of changed LSBS. Subsequently, less number of slightest critical bits of spread picture is modified in examination to plain LSB technique, enhancing the PSNR of stegoimage. By archiving the spot designs for which LSBS are upset, message picture could be acquired effectively. To enhance the vigor of steganography, Rc4 calculation has been utilized to accomplish the randomization secluded from everything message picture bits into spread picture pixels as opposed to saving them consecutively.

"Data hiding in intermediate significant bit planes, a high capacity blind steganographic techniques", 2012, The accessibility of fairly sensible advanced items coupled with the guarantee of higher data transfer capacity and nature of administration (Qos) for both wired and remote correspondence systems have made it conceivable to make,

duplicate, transmit, and convey computerized information without any misfortune in quality. In such a situation steganography has gained gigantic consideration from the examination group adjust the globe, as it has been discovered handy for data security and under spread correspondence. Stegnography alludes to secretive correspondence for exchange of secret data over a correspondence channel. This paper introduces a high limit stegnographic strategy in which mystery information is implanted in Intermediate Significant Bit planes of the spread picture. The information to be installed is softened down up pieces of moderately diminishing lengths and each one piece is inserted in the spread media under control of an exceedingly secure key.

"Steganography and steganalysis based on digital image", 2011, with the fast improvement of steganography, steganalysis has propelled rapidly. Fight steganography and steganalysis has turned into a significant issue in data security. Pointing at a regularly utilized spread media, i.e., computerized picture, this article surveys steganography and steganalysis dependent upon advanced picture. Idea and guideline of steganography and steganalysis are delineated. Spatial area and convert space inserting strategies are summed up. Also the late developments in steganalysis are reiterated.

"An effective image steganalysis method based on neighborhood information of pixels", 2011, this paper keeps tabs on picture steganalysis. We utilize higher request picture detail dependent upon neighborhood data of pixels (NIP) to locate the stego pictures from unique ones. We utilize subtracting ash qualities of nearby pixels to catch neighborhood data, and in addition to make utilization of "revolution invariant" property to lessen the dimensionality for the entire capabilities. We tried two sorts of NIP characteristic, the test outcomes shows that our proposed capabilities are with great execution and even beat the state-of-workmanship in certain viewpoint.

"Image steganography based on adaptive optimal embedding", 2010, A genuine necessity roused this detailed analysis of secure secret correspondence. Steganography is a user system used to move shrouded data in a subtle way. We proposed a novel methodology of substitution system of image steganography. The proposed strategy is totally adaptable on size of mystery message bits and permits us to install a lot of mystery messages and also keeping up great visual nature of stego-picture. Utilizing this strategy, message bits are installed into unverifiable and higher LSB layers, bringing about expanded indistinct and heartiness of stego-picture.

"A novel steganography method for image based on Huffman encoding", 2009, Steganography is the art of science that includes imparting mystery information in a suitable sight and sound bearer, e.g., picture, sound and feature documents. It goes under the presumption that if the characteristic is noticeable, the purpose of assault is apparent, consequently the objective here is dependably to cover the precise presence of the installed information. This paper shows a novel strategy for picture steganography dependent upon Huffman Encoding. Two 8 cycle ash level picture of size M X N and P X Q are utilized as spread picture and mystery picture individually. Huffman Encoding is performed over the mystery image/message before inserting and every spot of Huffman code of mystery image/message is installed inside the spread picture by adjusting the minimum huge touch (LSB) of each of the pixel's intensities of spread picture.

IV CONCLUSION

The extent that information concealing utilizing steganography is concerned, two essential destinations are fascinating: the procedure that will be utilized for steganography ought to give the most extreme conceivable payload, and the implanted information must be subtle to the onlooker. It ought to be pushed on the way that steganography is not intended to be vigorous. Any adjustments to the document, for example, transformations between record sorts, standard picture preparing or geometrical altering are required to influence the concealed bits from the index. It is rising in its crest in light of the fact that it doesn't draw in anybody without anyone else's input. In this paper a similar examination of a few systems has been effectively actualized. The MSE and PSNR of every last one of strategies are additionally thought about and likewise this paper exhibited a foundation dialog and execution on the significant calculations of steganography conveyed in advanced imaging. The developing strategies, for example, LSB based, OPAP, Inverted example based LSB utilizing MSE, Inverted example based LSB utilizing Relative entropy, String of 1 and 0 based, mod based and Mod 10 Generally few of these techniques have a tendency to have an easier payload contrasted with spatial area calculations. There are diverse approaches to diminish the bits required to encode a shrouded message.

REFERENCES

[1] Lu S., Multimedia Security: Steganography and Digital Watermarking Techniques for Protection of Intellectual Property, Idea Group Publishing, 2005.

[2] Popa R., "An Analysis of Steganographic Techniques," Working Report on Steganography, Faculty of Automatics and Computers, 1998.

[3] Bruice Schneier, Applied Cryptography Protocols, Algorithm and Source Code in C. Second edition. Wiley India edition 2007.

[4] S. Katzenbeisser, F.A.P. Petitcolas, Information Hiding Techniques for Steganography and Digital Watermarking, Artech House, Norwood, MA, 2000.

[5] W. Bender, D. Gruhl, N. Morimoto, A. Lu, ―Techniques for data hiding‖ IBM Syst. J. 35 (3&4) (1996) 313–336.

[6] Johnson N. and Jajodia S., "Steganography: Seeing the Unseen," IEEE Computer Magazine , vol. 25, no. 4, pp. 26-34, 1998.

[7] Lin T. and Delp J., "A Review of Data Hiding in Digital Images," in Proceedings of the Image Processing, Image Quality, and Image Capture Conference, Georgia, pp. 274-278, 1999.

[8] R.Amirtharajan and R.John Bosco Balaguru. ―Constructive Role of SFC & RGB Fusion versus Destructive Intrusion‖.International Journal of Computer Applications 1(20):30–36

[9] R.Amirtharajan and Dr. R. John Bosco Balaguru, ―Tri-Layer Stego for Enhanced Security – A Keyless Random Approach‖ - IEEE Xplore, DOI, 10.1109/IMSAA.2009.5439438.

[10]. C.K. Chan, L.M. Chen, Hiding data in images by simple LSB substitution, Pattern Recognition 37 (3) (2004) 469–474.

[11]. C.H. Yang, Inverted pattern approach to improve image quality of information hiding by LSB substitution Pattern Recognition 41 (2008) 2674–2683.

Author's Profile

Poonam Sen is pursuing her Master of Technology in Digital Communication from Sagar Institute of Research & Technology, under Rajiv Gandhi Technical University, Bhopal. Her research interests are Digital Image Processing (DIP) with security techniques enhancements.