International Journal of Scientific Research in Engineering and Management (IJSREM)
Volume: 06 Issue: 05 | May - 2022 Impact Factor: 7.185 ISSN: 2582-3930

Implementing Steganography Techniques using Distortion Method

Shruti, Tulluri Hima Sameera, Tumpala Yuvateja, Bharath Kumar R

School of Computer Science and Engineering,

Lovely Professional University,

Phagwara-144411, Punjab, India.

***Abstract*— Steganography is the artwork of hiding the sender messages through encryption and supply to the receiver. In today's world as the internet takes on the entirety in everyone's existence privacy of sending the information to different individual has come to be the largest task and to be able to solve this mythological trouble steganography comes forward [1, 2]. The word 'STEGANOGRAPHY' is originated from the Greek language which mixes the phrases steganos, meaning "protected or concealed", and graphic meaning "writing" if we positioned it collectively it says hiding the message inside any other message. The current image steganography represents the challenge of shifting the encrypted or embedded secure records to the destination give up without being detected through any third party individual or hacker. In beyond many unique methods have been used to send the encrypted image, however in today's international digital images are the maximum popular as they their frequency run at the internet. To send the steganography image, first we want to hide the information this will be with the assist of numerous steganography techniques via way of means of encrypting the sender image and the usage of some secret lock keys. At the receiver end the user can decrypt the image and use the data. Every steganography technique has its own strong and weak points that reflect the performance of the task [3, 4, 5]. This paper is mainly focus on the comparison of different steganography techniques like LSB, JPG, SCD and many more.**

Keywords—Steganography, Image, Encryption, Decryption, Techniques, Hiding data, Secret keys

Steganography may be divided into 5 sorts text Steganography, Image Steganography, Video steganography, Audio Steganography, Network Steganography. Hiding the information through taking cowl throughout a floor because the photo is called photo steganography, Images are broadly used as floor due to the fact there are a big variety of bits gift within side the virtual illustration of a photo [9]. Distortion Involves the splitting of the floor (in our paper its miles a photo) into blocks, after which embedding one message a bit in every block. The floor block will simplest be changed while the scale of the photo is one bit otherwise it does now no longer do any amendment or no amendment is required [6, 7, 8]. The distortion approach will keep the name of the game statistics through distorting the signal. An encoder applies a series of changes to the floor, and the decoder section decodes the encrypted information to the unique information with the name of the game information through the use of mystery key. In the latest years, there is numerous information hiding strategies were advanced for images. However, those strategies forget about the security against steganalyzers. The excessive undetectability of the name of the game message method in photo steganography way it complements the Safety [10, 11, 12]. In this paper, we targeted on designing a JPEG. Photo information hiding scheme (steganographic scheme) through enhancing the undetectability whilst shielding the stego photo excellent and embedding capacity. In the evaluation we've got took diverse parameters like embedding capacity, involvement of mystery keys, Detection of escaped message, Robust, Integrity, Best appropriate distortion dimension, Message Capacity, of various distortion strategies and as compared every and each parameter [19, 20, 21]. And concluded that that's high-satisfactory and why it's miles the high-satisfactory distortion approach as compared to closing of the strategies. In the distortion dimension segment a proposed steganographic scheme is represented and comparisons of various photo steganographic schemes are represented.

INTRODUCTION

Steganography, works through hiding mystery statistics or information hiding below a virtual media in any such manner that no manner should come across count on the sender and receiver. Only the sender and receiver should come across the lifestyles of the statistics within side the virtual media.

Literature Review

S.No	Title	Method Proposed	Advantages	Disadvantages
1	Digital Image steganography using Universal Distortion Method.	Image processing and computer vision using distortion function and side informed embedding	This distortion method distorts the signal and stores the secret data.	The cover block of message can only be modified when the message bit is one otherwise no.
2	Secure Binary image steganography based on fused distortion measurement.	A fused a distortion measure is developed to better measure the distortions bought by flipping pixels. Next, flipping position optimization is designed to find better flipping positions for flipping pixels to embed secret message.	It combine the merits of FDM and two data-carrying pixel location methods including EAG and CPC, a flipping position optimization (FPO) to find better positions for flipping to further improve the steganographic performance.	Improving steganographic performance in binary images is still in progress visual quality and statistical security is not enough.
3	Binary image steganography based on joint distortion measurement.	Proposed a kind of distortion measurement that is not only based on the discrimination effects after flipping the pixels but also depends on the visual effects of corresponding pixels, which is called joint distortion measurement	It divides images into small blocks and select appropriate pixels to embed secret message thus it increases the compilation speed.	Capacity of the image size if very less does not useful for high resolution pixel images.
4	A novel minimum distortion-based edge adaptive image steganography scheme using local complexity.	Focuses on introducing a novel, minimal, distortion, edge image steganography, scheme called Block-wise edge adaptive steganography scheme (BEASS) , that adaptively adjusts itself according to message payload by choosing regions with the highest local complexity to embed data.	The capacity to embed high payloads of data can be done by directly modifying image pixels.	Steganalysis was deemed unsuccessful in discovering the hidden message and blind steganalysis attack.
5	Secure halftone image steganography based on density preserving and distortion fusion.	Proposed optimization strategy of pixel density distribution preserving and distortion fusion that further improves statistical security.	It measures the flipping distortion according to the statistics of the image database but neglect the characteristic of a single image.	The distortions of halftone images are mainly in the form of “salt-and-pepper” artifacts due to local clusters of pixels.
6	Distortion function based on residual blocks for JPEG steganography.	RBVs of residual blocks that are to inspect the embedding risk in spatial domain and the quantization steps that are to inspect the embedding risk in embedding domain.	We can able to obtain the very less statistical detect-ability since it hides the message in blocks with secret keys.	Implementing the distortion function based steganography is very much complex time taking process.
7	Zero distortion Technique: An approach to Image steganography Using strength of indexed based chaotic Sequence.	ZDT(Zero Distortion technique) is proposed to overcome the limitations as no changes are reflected in the histogram and PSNR value of the cover and stego image.	This is the most common technique uses to hide the data with help of LSB technique.	Major drawback is it can be easily detected by histogram and PSNR value.
8	Defining Joint distortion for JPEG.	Proposed a principle of Block boundary Continuity (BBC) for defining JPEG joint distortion which aims to restrain blocking	Main aim is to restrain the blocking artifacts which caused by inter-block adjacent modifications to achieve the	Joining the images is the complicated process cannot be used for faster compilation.

		artifacts caused by inter block adjacent modifications.	joint distortion.	
9	Side informed steganography with additive distortion.	Described a general principle for incorporating the side information in any steganographic scheme designed to minimize embedding distortion.	The embedding of secret messages utilizes a higher quality form of the cover object which helps in image processing faster.	The embedding algorithm has much quantization errors while converting from precover to low quality image.
10	Distortion function Designing for JPEG Steganography with uncompressed Side-Image.	Framework for designing distortion function of Joint Photographic experts group with uncompressed side image. Frameworks are discrete cosine transform coefficient including all direct current (DC) and alternating current (AC).	The number of embedding changes and the number of distortion functions which are used to identify individual elements to cover could be modified during embedding process of the image.	It is constrained to the aforementioned for dividing the scenarios or frameworks to obtain the distortion.
11	Steganography for BTC compressed images using no distortion technique.	Improved data hiding scheme to embed secret data in the compressed bit streams where the quality of the image is maintained even after embedment	This is the technique which uses the embedded sensitive information in the cover image later which could be used to recover the original form of the image	Finding of missing data is not possible because it does not have any technique.
12	Distortion function for Emoji Image steganography.	Proposes the profile of image content, the intra and inter frame co-relation are taken into account in the distortion function to fit the unique properties of the emoji image.	We can integrate the data embedding impacts for the intra frames and to the inter frames which helps in obtain better security.	Conversion of the embed framework to the animated GIF is a major security challenge.

Ⅲ. Comparison of different steganography techniques

Method Name	**Parameters**							
	Embedding	**Involve-ment of secret keys**	***Detection of escaped message***	***Robust***	**Best Suitable Distortion *Measurement***	***Distortion***	***Integrity***	**Message Capacity**
Least Significant Bit(LSB) (2017)	Technique in which least significant bit of the image is replaced with data bit	1	5%	Mostly low	DRD	35%	24%	256 bits
Hash-LSB and RSA algorithm (2018)	Uses a hash function to generate a pattern for hiding data bits into LSB of RGB pixel values of the cover image	1	14%	High	ELD	38%	32%	448 bits
Blow-fish Encryption-LSB Steganography (2019)	This process gives Stego image in which secret data is hidden into cover image that select pixel randomly and store this key in the stego image	1	21%	High	DRD	46%	38%	512 bits
Transform domain method (2020)	The techniques used for hidden exchange of information in frequency domain	1	36%	High	ELD	54%	56%	800 bits
JPEG Image Steganography Technique (2021)	The steganography operation is applied on the image after its transformation from time into the frequency space after the discretisation of transformed data	1	44%	HIgh	SCD	67%	74%	1024 bits
Quantization Based Steganography (2021)	This technique is used because of its efficiency and simplicity which divide the image into small portions and performs the hiding operation	2	68%	High	ELD	78%	80%	1600 bits
File and Pallet Embedding Steganography Technique (2022)	This new technique embeds one message bit into one pixel. The pixels for message embedding are chosen randomly using a pseudo-random number generator seeded with a secret key.	2	78%	High	SCD	86%	88%	2048 bits

Spread Spectrum Image Steganography Technique (2022)	A value can be added to the cover-object by transmitting under the added noise value	2	90%	High than rest of all.	SCD	92%	90%	4096 bits

Ⅳ. Comparision of different steganography distortion measurments techniques

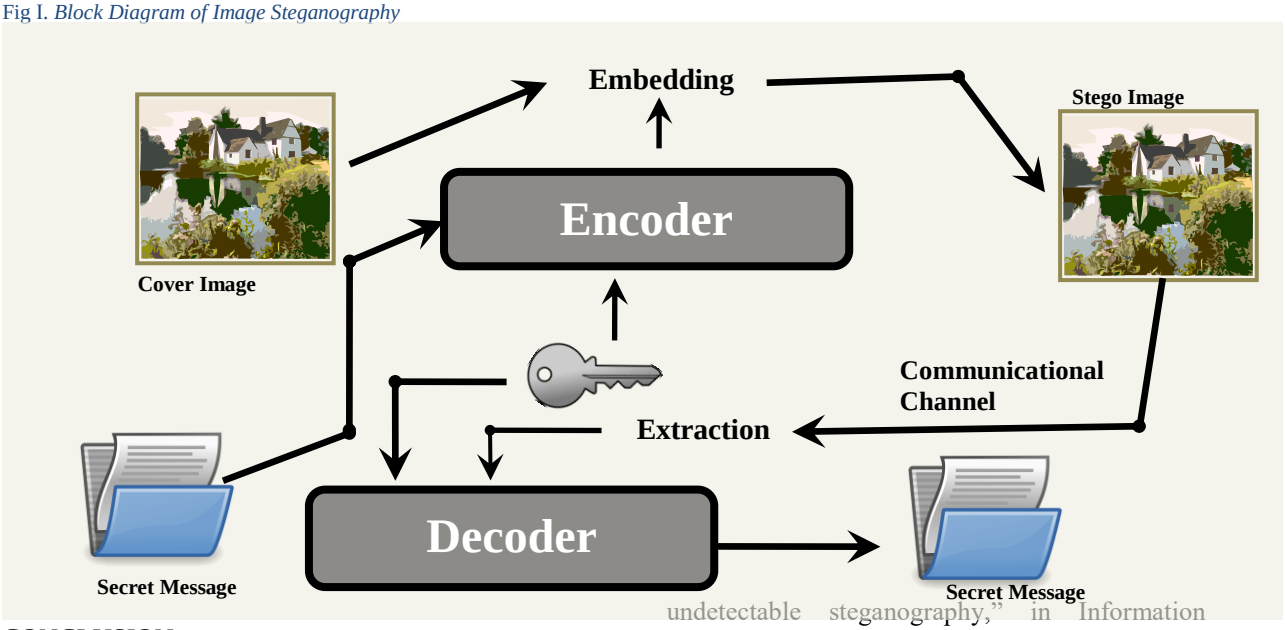
Distortion Measurement	**Parameters**					
	Embedding	***Involvement of Secret Keys***	***Robust***	***Detection of Escaped Message***	***Integrity***	***Message Capacity***
Distance Reciprocal Distortion(DRD)	The message is delivered by the distance metric and according the reciprocal graph is drawn simultaneously	Yes	Mostly low	Considerably low	65%	1024 bits
Edge Line Distortion-based measurement(ELD)	In this technique the distance is measured from the distance from the edge points to the regression line	Yes	Compared to DRD the ELD has better robustness.	Moderate detectable	78%	2056 bits
Smoothness and Connectivity Distortion(SCD)	In this technique the a line is drawn from the slant edges around the image and the distance is measured.	Yes	The SCD has the highest among the all.	Fully detectable	92%	4096 bits
Proposed	Considering all the three the SCD is the best proposed method as it measures the based on the edges of the image.	All are applicable.	SCD	SCD is best because it can fully detect the missing information	SCD	SCD.

V. PSEUDO CODE

```
SET libraries TO Import
SET start To datetime.now()
DEFINE FUNCTION decode():
    Screen.destroy()
    Set DecScreen To TK()
    DEFINE FUNCTION openFile():
        Global FileOpen
        SET FileOpen TO StringVar()
        SET FileOpen TO askopenfilename()
        Set label TO Label()
    DEFINE FUNCTION Decpder():
        SET Message TO stg.reveal(FileOpen)
        SET text_box TO Text(height,width)
        SET filesize TO os.path.getsize(FileOpen)
        SET SelectButton TO Button()
        SET end TO datetime.now()
        OUTPUT(tracemalloc.get_traced_memory())
    Tracemalloc.stop()
    OUTPUT('Excution Time')
DEFINE FUNCTION Encode():
    Screen.destroy()
    SET EncScreen TO TK()
    SET LABEL
    DEFINE FUNCTION openFile():
        Global FileOpen
        SET FileOpen TO StringVar()
        SET FileOpen TO askopenfilename()
    DEFINE FUNCTION Encoder():
        SET Response TO messagebox.askyesno('POP UP')
        IF Response EQUALS 1:
            messagebox.showinfo("Pop Up", "Successfully Encoded")
        ELSE:
            messagebox.showwarning("Pop Up", "Unsuccessful ")
        SET SelectButton TO Button()
        SET end TO datetime.now()
    OUTPUT('The time of excution of
```

```
        Encode:{}'.format(end-start))
37.     Scree=TK()
```

Fig I. *Block Diagram of Image Steganography*



CONCLUSION

Steganography can defend information through hiding it. however the usage of it on my own won't guarantee overall protection. It is viable that through the usage of a steganocryption technique, enemy detects presence of textual content message within side the photo document after which he/she might also additionally however the usage of it on my own won't guarantee overall protection. It is viable that through the usage of a steganocryption technique, enemy detects presence of textual content message within side the photo document after which he/she might also additionally achieve extracting data from the picture, which may be disastrous in actual lifestyles situations. This is identical for undeniable encryption. In this situation through seeing the meaningless acting series of bits enemy can come across that a few unlawful message is being dispatched and we might also additionally land in a elaborate situation.However, if one makes use of each methods, this could lead to 'protection in depth'. The message must first be encoded the usage of a robust encryption set of rules after which embedded right into a carrier.

REFERENCES

[1] J. Bierbrauer and J. Fridrich, "Constructing good covering codes for applications in steganography," in Transactions on Data Hiding and Multimedia Security III. Berlin, Germany: Springer-Verlag, 2008, pp. 1-22.

[2] T. Filler, J. Judas, and J. J. Fridrich, "Minimizing additive distortion in steganography using Syndrome-trellis codes," IEEE Trans. Inf. Forensics Security, vol. 6, no. 3, pp. 920–935, undetectable steganography," in Information Hiding (Lecture Notes in Computer Science), R. Böhme, P. W. L. Fong, and R. Safavi-Naini, Eds., vol. 6387. New York, NY, USA: Springer-Verlag,Oct. 2010, pp. 161–177.

[8] L. Chiew and J. Pieprzyk, "Binary image steganographic techniques classification based on multi-class steganalysis," in Information Security, Practice and Experience. Berlin, Germany: Springer-Verlag, 2010, pp. 341–358.

[9] K. Solanki, K. Sullivan, U. Madhow, B. S. Manjunath, and S. Chandrasekaran, "Provably secure steganography: Achieving zero K-L divergence using statistical restoration," in Proc. IEEE Int. Conf. Image Process., Oct. 2006, pp. 125–128

[10] Bashayer Falah Alatiyyat, Narmatha C, "Survey on Image Steganography Techniques", Computing and Information Technology (ICCIT) 2022 2nd International Conference on, pp. 57-64, 2022.

[11] Mustafa Takaoğlu, Adem Özyavaş, Naim Ajlouni, Ali Alshahrani, Basil Alkasasbeh, "A Novel and Robust Hybrid Blockchain and Steganography Scheme", Applied Sciences, vol. 11, pp. 10698, 2021.

[12] Nandhini Subramanian, Ismahane Cheheb, Omar Elharrouss, Somaya Al-Maadeed, Ahmed Bouridane, "End-to-End Image Steganography Using Deep Convolutional Autoencoders", Access IEEE, vol. 9, pp. 135585-135593, 2021

[13] Preksha B, Rishika Harish, Sreenivas B, Vasanthalakshmi M, "Image Steganography using RSA Algorithm for Secure Communication", Mobile Networks and Wireless Communications (ICMNWC) 2021 IEEE International Conference

Sep. 2011.

[3] Oleg Evsutin, Anna Melman, Roman Meshcheryakov, "Algorithm of error-free information embedding into the DCT domain of digital images based on the QIM method using adaptive masking of distortions", Signal Processing, vol. 179, pp. 107811, 2021

[4] Manashee Kalita, Swanirbhar Majumder, "A new steganographic method using Contourlet Transform", Signal Processing and Communication (ICSC) 2016 International Conference on, pp. 274-278, 2016

[5] Tabares-Soto Reinel, Ramos-Pollán Raúl, Isaza Gustavo, "Deep Learning Applied to Steganalysis of Digital Images: A Systematic Review", Access IEEE, vol. 7, pp. 68970-68990, 2019.

[6] Y. Kim, Z. Duric, and D. Richards, "Modified matrix encoding technique for minimal distortion steganography," in Information Hiding. Berlin, Germany: Springer-Verlag, 2007, pp. 314–327.

[7] T. Pevný, T. Filler, and P. Bas, "Using high-dimensional image models to perform highly

on, pp. 1-5, 2021.

[14] . Bayu Kumoro Yakti, Sarifuddin Madenda, Sunny Arief Sudiro, Purnamawan Musa, "Processing Speed Comparison of the Least Significant Bit (LSB) Steganography Algorithm on FPGA and Matlab", Informatics and Computing (ICIC) 2021 Sixth International Conference on, pp. 1-7, 2021.

[15] Yaofei Wang, Weiming Zhang, Weixiang Li, Nenghai Yu, "Non-Additive Cost Functions for JPEG Steganography Based on Block Boundary Maintenance", Information Forensics and Security IEEE Transactions on, vol. 16, pp. 1117-1130, 2021.

[16] Mujian Yu, Xiaolin Yin, Wanteng Liu, Wei Lu, "Secure halftone image steganography based on density preserving and distortion fusion", Signal Processing, vol. 188, pp. 108227, 2021.

[17] Cheng, Jun and Kot, Alex C and Liu, Jun and Cao, Hong, "Steganalysis of data hiding in binary text images," in IEEE International Symposium on Circuits and Systems. IEEE, 2005, pp. 4405–4408.