Enhancement of Image Stegnography Technique for Improvement of Security

Hemant R. Deshmukh, Mahip M. Bartere

Abstract: ***Steganography will pick up its significance because of the exponential development and mystery correspondence of potential PC clients over the web. It can likewise be characterized as the investigation of undetectable correspondence that ordinarily deals with the techniques for disguising the nearness of the bestowed message. For the most part information implanting is accomplished in correspondence, picture, content, voice or interactive media content for copyright, military correspondence, confirmation and numerous different purposes. In picture Steganography, riddle correspondence is expert to introduce a message into cover picture (used as the transporter to embed message into) and deliver a stego picture (created picture which is passing on a covered message). In this paper we have on a very basic level researched diverse steganographic strategies. For hiding data we used virtual key replacement technique which provides high data security in terms of payload, Image Quality etc.***

Keywords: Data Hiding, Security, Payload capacity.

I. INTRODUCTION

Advanced data installing in computerized media could be a records improvement ground of rapidly mounting company. The transmission of mechanized media things by ways for internet is obtaining increasingly clear. Since the electronic medium are often supportively transmitted and reproduced lossless, it conjointly incite a development of leading edge theft [1]-[4]. To handle this issue varied data concealment strategies are used. The meaning of Image steganography is came from "secured expressing" in Greek; this method is used to hide the data behind image, audio or video. So that intruder not conceals our data. That is the fundamental purpose of data contents away is to pass on carefully specified the real information that is introduced in the form of media isn't clear to the observer. It means disagreeable social occasions shouldn't enclose the flexibility to understand in between original input image and stego-picture. The stego image shouldn't stray abundant from the most cover image [5].As of late, making data hiding innovations, particularly as steganography, are believed to represent a jeopardy to personage defense, trade and also in additional, nationwide safety welfare. The measure advancement to data hiding safety is consistently advised as steganalysis. The basic endeavor of idle reverse steganography is to select the closeness or else nonattendance of coated data in specified media. Dynamic steganalysis (otherwise referred to as criminology steganalysis) eludes to the travail by unmotivated beneficiaries to extricate/evacuate/change the real concealed data.

Revised Manuscript Received on 8 February 2019.

Dr. Hemant R. Deshmukh, Professor, Dr. Ragendra Gode Institute of Technology & Research, Amravati (Maharashtra), India.

Mr. Mahip M. Bartere, Research Scholar, Sant Gadge Baba Amravati University, Amravati (Maharashtra), India.

During this specific scenario, dynamic steganalysis isn't in any respect like assaults to watermarking security. Steganography is in an exceedingly one in every security where information be cowltly planted in an input image. Where important message that is delivered is entirely modified into different ways, shrouded information underneath an input image is send to the receiver. Simply the individual who is aware of the tactic will do without a lot of stretch unscrambles the message. The execution of Steganography ways will be evaluated by 3 Parameters: limit, security and blurriness. Hence steganography entails obscured one bit of data within another.

The Steganography calculations are facilitating to perform mystery correspondence. Data storage away is that the approach toward concealing a mystery message within cover medium, for instance, picture, video, content, sound. Concealed image has varied applications, notably within the gift current, innovative world. Protection and mystery may be a worry for a good many of us on the net. hid image takes under consideration 2 gatherings to convey on the sly and on the QT. The hidden information should be secure throughout transformation are often noninheritable by 2 ways: cryptography and data hiding. a combination of the 2 methods are often utilized to expand the data security.

II. RELATED WORK

Edge locale based mostly implanting falls below the category of object based steganography and a few fascinating exploration works has been completed in making edge based image steganography strategies. In the meantime, techniques for mistreatment the scrambled projection for image encryption have in addition been projected. The larger a part of the edge place along plans underline with reference to PVD [6] to acknowledge smooth and edge picture element. The elegant province picture element is leave untouched. Least Significant Bit data hiding technique exploitation, Pixel value differencing provides superior data hiding capacity and unperceivable stego pictures that is projected by cheng & his team [9]. Wu and his group allege that the projected technique is finer to Shanghai dialect and his co [6].Then again, chaotic map based based plans have used an assortment of confused maps like Henon's Map, logistic Map, etc. perhaps a handful of the essential research works significant to the ebb and flow setting are displayed straightaway. In PVD primarily based data hiding method is projected [7]. The projected strategy is an enhancement of Least Significant Bit Matching Revisited procedure.

The characterization of the picture element decides the live of data that may exist coated up contained by that pixel. The graceful district pixels embrace less important measure of the data as compare to the edge pixels grip increasingly inserted information. In addition [8], a footing primarily based inserting arrange projected a Laplacian locator to locate edge picture element & implants addicted to the additional honed edges utilizing the LSB Replacement (LSBR).R.L Tataru et al., [10] have anticipated a spatial domain chaotic plan supported steganography scheme that makes the use of PVD for pixel combine separation in addition to a clamorous transformation map to pick the two pixel amass for implanting extraction. In [11], a picture scrambling system utilizing turbulent feline mapping has been proposed. The picture is at first mutilated utilizing the feline confused mapping and afterward XOR function is executed between certain pixel estimation of the superior picture and a turbulent esteem. For rebuilding of the picture, a converse change is achieved. In [12, 13, and 14] author discussed the image techniques by using different methods.

III. METHODOLOGY

3.1 Carrier Image

Let a carrier image I represented with combinations of basic color that is Red, Green & Blue. These are the natural colors and any other colors can be formed with the combinations of RGB Color. An image can be represented with the functions

F(x1) = $\int_{i=1,j=1}^{i=w,j=h}(r,g,b)$

Where w= width of image.
H= height of an image.
A pixel P (I,j) is a basic entity of image which is a combination of RGB color components. If an image I with height h & width w contain
h*w= number of pixels

$$n = h * w$$

If p(c) is total number of components of an image then p(c) is represented as

$$p(c) = n * 3$$

$$p(c) = h * w * 3$$

3.2 Feature Extraction & Master Color pixel Selection

Master Pixels m(p) is a basic component of proposed methodology for virtual data hiding.RGB components are extracted from an image I and are combined with its position, binary value.
Let f (x2) is a function for extraction of RGB components which can be represented as

$$f(x2) = \int i, j, p(cr), B(r), p(cg), B(g), p(cb), B(b)$$

Where
I = width coordinator
J = height coordinator
P(cr) = pixels red components
P(cg)= pixels green component
P(cb)= pixels blue component
B(r)= Binary Red component.
B(g) Binary Green Component
B(b)= Binary Blue component.

In order to create complexity throughout the process, of virtual Data hiding & extraction, It should be necessary that data hiding & extraction should not be depend on single master pixel. The complexity C is directly proportional to numbers of master pixel components.

$$C \propto f(x2)$$

Complexity of proposed algorithm is achieved by selecting master pixels component through Fibonacci series. Where based on single master pixel selections, future (upcoming) master pixels are chosen automatically.
In Fibonacci series, initially one master component is selected from the position
F(p)= F(I,j)
F(p+1)= F(I,j+1)
F(p+2)= F(p) + F(p+1)
F(p+3)= F(p+2) +F(p+1)…….F(p+m)=F(p+m-1)+F(p+m-2)+……..F(p).

3.3 Data Hiding

Proposed methodology is based on complete virtual data hiding & extraction mechanism where a carrier object is untouched with secret data. An illusion will be created for outsider (Intruder) about the existence of data. Let F(h) is functions that hide the secret data s(d) into carrier image I.
Let B(Sd) is secret binary data and B(Pc) is a binary master pixel component.

F(h)= { If B(Sd) ==0 then find (position (B(Pc),0))
If B(Sd) ==1 then find (position (B(Pc),1))

F(h)= Add Position(B(Pc))

Output of virtual data hiding process is F(h) is a key consisting of positions of Zeros & one of secret data B(Sd).
Length of F(h) is directly proportional to length of B(Sd).

$$F(h) \propto Length(B(Sd))$$

3.4 Key Compression

One of the major step of proposed methodology is to reduced the burden of positions key F(h) generated by Virtual data hiding mechanism. A subsequent clusters from F(h) is chosen & its frequency should be located IF frequency of occurrence of cluster within F(h) is Greater than or equal to 2, then we replace it with the single ASCCII character.
F(hc)= cluster (F(h), Lc)
Where Lc is cluster length.
If Frequency (F(hc)>=2 then F'(h) = Replace (h(c),F(hc) , ASCII_Char)
With the proposed key compression mechanism, almost 90% reductions in key length h(c) is possible to achieve.
100 >F'(h) > = (10/ F(h))*100.
An output of key compression is compressed key F'(h) and key replacement table. Number of touples (T(h'c)) is directly proportional to the iterations required for key compressions.
T(F'(c))α iteration (F(c))

3.5 Data Extraction

An accuracy of data extraction is depends on exact decompression mechanism. Let a function F''(h'(hc)) is key decompression functions that decode compressed key F'(hc) with the help of key mapping table.

F'' (F'(hc))= Decode F'(hc),key mapping table.
Again number of iterations required for F''(F'(hc)) is directly proportional to touples present in Key mapping table. Iteration (F'' (F'(hc)= T (key mapping table)

3.6 Virtual Data Extraction

Ones key F'' (F'(hc)) is decoded, a master pixel component are chosen from carrier image.
The extraction of secret accurate data is depending on accurate master pixel selection.
B(Sd) = F(Extract (F''(F'(h(c)), B(Pc))
The extracted Secret Binary data B(Sd) uis grouped into an equal length of 8 bits so as to generate its equivalent ASCII char. An accuracy of Extracted ASCII char data Sd is compared with Secret data used on sender side. If Extracted and hidden data are same it means accuracy of entire proposed methodology is 100 %.

IV. RESULT ANALYSIS AND DISCUSSION.

Table 1: Original Image Entropy & Encrypted Image Entropy

Input Image	X-OR Method		Virtual Key Replacement Method	
	Original Image Entropy	Encrypted Image Entropy	Original Image Entropy	Encrypted Image Entropy
Image 1	17.67083	17.9837	8.5678	8.5678
Image 1	17.8021	17.9946	7.7657	7.7657
Image 1	16.7554	17.9822	5.4229	5.4229
Image 1	17.4179	17.8623	12.2847	12.2847
Image 1	17.8945	17.9901	13.4876	13.4876

Table 2: Comparison of Our approach with other methods

Cover Image	Entropy		
	Image encryption using Chaos Method	Image Encryption using X-OR Method	Virtual Key Replacement Method
Picture	7.009716	17.67083	8.5678
Lena	7.439721	17.8021	7.7657
Peppers	7.460669	16.7554	5.4229

From Table 1 it is observed that the Original Image entropy & Encrypted Image entropy using X-OR method can affect the quality of Image, which results into data may be get extracted by the third party. By using our approach the quality of image is maintained. Table 2 represents the superiority of image after data hiding [15].

Table 3: Mean Intensity of original Image & Encrypted Image [15]

Input Image	X-OR Method		Virtual Key Replacement Method	
	Mean Intensity Of Input	Mean Intensity of Encrypted Image	Mean Intensity Of Input	Mean Intensity Of Encrypted Image
Image 1	0.6	0.50196	175.373	175.373
Image 2	0.4582	0.49412	128.271	128.271
Image 3	0.7333	0.49412	157.243	157.243
Image 4	0.56471	0.53333	197.281	197.281
Image 5	0.4667	0.47451	189.246	189.246

Table 3 shows the evaluation of mean intensity of Original & Encrypted image using different Approach.

Table 4: Standard Deviation (SD) of Input Image & Stego Image

Input Image	Separable reversible Scheme		Virtual Key Replacement Method	
	SD of Input Image	SD of Stego Image	SD of Input Image	SD of Stego Image
Image 1	69.4146	69.3133	58.7554	58.7554
Image 1	67.9175	67.6684	67.6785	67.6785
Image 1	86.8575	86.1076	76.2014	76.2014
Image 1	62.8087	62.5733	65.3251	65.3251
Image 1	58.7619	58.7058	61.2035	61.2035

Table 5: Comparison of Proposed method with PVD & PVD with LSB replacement.

Cover Image 512 X 512	PVD		PVD & LSB Replacement(Wu-Tsai-Wang)		Virtual Key Replacement Method	
	Capacity (Bytes)	PSNR (dB)	Capacity (Bytes)	PSNR (dB)	Capacity (Bytes)	PSNR (dB)
Peppers	50907	37.07	96281	35.34	96781	99
Tank	50499	41.99	96089	37.38	96389	99
Jet	51224	37.42	96320	35.01	96620	99
Baboon	57146	33.43	89731	32.63	89931	99
Lena	51219	38.94	95755	36.16	95800	99
Elaine	49739	40.13	97790	36.60	97990	99

So to demonstrate the attainability of our strategy to lift the limit of covering up with an adequate nature of the stego-picture, we tend to utilised the MATLAB program dialect device [16, 17] and achieve the elevated PSNR value. We are able to additionally observe that wu and Tsai's scheme uses the smallest amount little bit of the cover image to implant the most secret information. As compare to our projected methodology we tend to accomplish higher PSNR value as compare to PVD & PVD with LSB Replacement technique. that's to mention, the standard of the stego-image when embedding secret information will still possess a high PSNR value.

Table 6: Comparison of Stego image & Extracted Image based on PSNR.

Cover Image	Two Way Block Matching (Ran Wang Yeh) [18]		Virtual Key Replacement Method	
	PSNR (Stego Image & Cover image)	PSNR (Extracted Image & Original Image)	PSNR (Stego Image & Cover image)	PSNR(Extracted Image & Original Image)
Jet	44.42	44.42	99	99
Lena	44.53	44.26	99	99
Milk	44.42	44.55	99	99
Scene	44.51	43.16	99	99
Tiff	44.46	44.36	99	99

We can see that the nature of the stego-picture is high, and fortuitous eyewitnesses will not realize the presence of the covered up important image. To be sure, it's troublesome to acknowledge the PSNR of stego image and cover image, utilizing the blank eye shows that the esteem and typical utilization of the essential image are safeguarded. Table 6 condenses the PSNR estimations of this check. Table 7 demonstrates that our approach contains a characteristic of imperceptibility. Besides, from MSE values, it shows that the modified value of every pixel is nearly 0[19].

Table 7: Comparison of Image based on MSE.

Cover Image	MSE (Spatial LSB Domain System)	MSE (Virtual Key Replacement Method)
Elaine	7.911	0
Lena	7.337	0
Baboon	11.543	0
Peppers	6.619	0
Toys	7.293	0
Girl	7.109	0
Gold	6.749	0
Tiffany	6.872	0

Table 8: Comparison of Proposed method with PVD & Four Pixel Differencing & LSB

Image	Image Size	PVD	Four Pixel Differencing & LSB	Virtual Key Replacement Method
Lena	255 X 255	8192	10007	Payload capacity is more as compared to other two methods mentioned in this table.
Peppers	255 X 255	8192	10211	
Baboon	255 X 255	8192	9767	
Lena	512 X 512	32768	40017	
Peppers	512 X 512	32768	40990	
Baboon	512 X 512	32768	39034	
Lena	1024 X 1024	131072	160604	
Peppers	1024 X 1024	131072	163724	
Baboon	1024 X 1024	131072	156308	

We have investigated our outcomes as indicated by PVD strategy and Four pixel Differencing and LSB for every one of the tried pictures. We likewise dissected our outcomes by registering Payload. The extent of information that could be imbedded inside the cover picture is appeared Table 8. We test our proposed calculation on the diverse pictures [20].

V. CONCLUSION:

This paper proposed a new stegnographic technique, with careful implementation of Virtual Key Replacement method. This system resulted in both Data Hiding Image & Extracted image creature of good quality. The high embedding ability enables a sender to send huge quantity of secret information following any image in any situation where dimension of image is diverse. With the proposed algorithm we also show that the quality of image is maintained with respect to various parameters like PSNR, MSE, Entropy, and Standard Deviation.

REFERENCES:

1. Hong Cao and Alex C. Kot, On Establishing Edge Adaptive Grid for Bilevel Image Data Hiding", IEEE transactions on information forensics and security, vol. 8, no. 9, September 2013.
2. Che-Wei Lee and Wen-Hsiang Tsai, A Secret-Sharing-Based Method for Authentication of Grayscale Document Images via the Use of the PNG Image With a Data Repair Capability, IEEE transactions on image processing, vol. 21, no. 1, January 2012.
3. Ming Li, Michel K. Kulhandjian, Dimitris A. Pados, Stella N. Batalama, and Michael J. Medley, Extracting Spread-Spectrum Hidden Data From Digital Media, IEEE transactions on information forensics and security, vol. 8, no. 7, July 2013.
4. Chunfang Yang, Fenlin Liu, Xiangyang Luo, and Ying Zeng, Pixel Group Trace Model-Based Quantitative Steganalysis for Multiple Least-Significant Bits Steganography, IEEE transactions on information forensics and security, vol. 8, no. 1, january 2013.
5. A. E. Mustafa, A.M.F. ElGamal, M.E. ElAlmi, Ahmed.BD, A Proposed Algorithm For Steganography In Digital Image Based on Least Significant Bit , Issue No. 21, April. 2011.
6. D. C. Wu and W. H. Tsai, "A steganographic method for images by pixel-value differencing", Pattern Recognition Letters, vol. 24, no. 9-10, pp. 1613–1626, 2003.
7. Weiqi Luo, Fangjun Huang, Jiwu Huang, "Edge Adaptive Image Steganography Based on LSB Matching Revisited", IEEE Transactions on Information Forensics and Security, Vol. 5, No. 2, June 2010, pp. 201-214.
8. G.Karthigai Seivi, Leon Mariadhasan, K. L. Shunmuganathan, "Steganography using Edge Adaptive Image", Proc. of the International Conference on Computing, Electronics and Electrical Technologies (ICCEET), pp. 1023-1027, 2012.
9. Cheng-Hsing Yang, Chi-Yao Weng, Shiuh-Jeng Wang , Hung-Min Sun, "Adaptive Data Hiding in Edge Areas of Images With Spatial LSB Domain Systems", IEEE Transactions on Information Forensics and Security, Vol. 3, No. 3, September 2008, pp.488-497.
10. R. L. Tataru, D. Battikh, S. El Assad, H. Noura, O. Deforges, "Enhanced Adaptive Data Hiding in Spatial LSB Domain by using Chaotic Sequences", Eighth International Conference on Intelligent Information Hiding and Multimedia Signal Processing, pp. 85-88, 2012.
11. Zhu Liehuang, Li Wenzhuo, Liao Lejian , Li Hong, "A Novel Algorithm for Scrambling Digital Image Based on Cat Chaotic Mapping", International Conference on Intelligent Information Hiding and Multimedia Signal Processing, pp. 601-605, 2006.
12. Sahar Mazloom, Amir-Masud Eftekhari-Moghadam, "Color Image Cryptosystem using Chaotic Maps", IEEE Symposium on Computational Intelligence for Multimedia, Signal and Vision Processing, pp. 142-147, 2011.
13. Qian-chuan Zhong, Qing-xin Zhu , Ping-Li Zhang ,"A Spatial Domain Color Watermarking Scheme based on Chaos", International Conference on Apperceiving Computing and Intelligence Analysis (ICACIA), pp. 137-142, 2008.
14. Chen Wei-bin, Zhang Xin, "Image Encryption Algorithm based on Henon Chaotic System", International Conference on Image Analysis and Signal Processing (IASP), pp. 94-97, 2009.
15. A. E. Mustafa, A.M.F. ElGamal, M.E. ElAlmi, Ahmed.BD, A Proposed Algorithm For Steganography In Digital Image Based on Least Significant Bit , Issue No. 21, April. 2011.
16. Anuja Yeole, Mahip Bartere ,"An X-Or Base Image Encryption and Data Security through Higher LSB Data Hiding Approach: Result Oriented", International Journal of Engineering Science and Computing, April 2016 Volume 6 Issue No. 4.
17. Wu, D.C., and Tsai, W.H.: 'A steganographic method for images by pixel-value differencing', Pattern Recognit. Lett., 2003, 24, (9-10), pp. 1613–1626
18. H.-C. Wu, N.-I. Wu, C.-S. Tsai and M.-S. Hwang,"Image steganographic scheme based on pixel-value differencing and LSB replacement methods"IEE Proc.-Vis. Image Signal Process., Vol. 152, No. 5, October 2005.
19. Ran-Zan Wang and Yeh-Shun Chen," High-Payload Image Steganography Using Two-Way Block Matching", IEEE Signal Processing Letters, Vol. 13, No. 3, March 2006 161.
20. Cheng-Hsing Yang, Chi-Yao Weng, Shiuh-Jeng Wang," Adaptive Data Hiding in Edge Areas of Images With Spatial LSB Domain Systems", IEEE Transactions On Information Forensics And Security, Vol. 3, No. 3, September 2008.
21. M.B. Ould Medeni," A Novel Steganographic Method for Gray-Level Images With four-pixel Differencing and LSB Substitution",978-1-61284-732-0/11/$26.00 ©2010 IEEE.