International Journal of Information Science and Computing
Citation: *IJISC*: **6**(1): 01-08, June 2019

INFORMATION SCIENCE AND TECHNOLOGY FOUNDATION

An Application of Image Morphing Technique for Secure Data Transmission through Virtual Data Hiding

Sonali Lavangale and M.U. Karande

Dr. V. B. Kolte College of Engineering, Malkapur, Maharashtra, India

ABSTRACT

Data Hiding is the study of concealing information into harmless questions to such a degree, to the point that the nearness of the shrouded information stays intangible to an enemy. Hiding the data into cover image have differed procedures of usage created after some time. Insurance of the concealed data from an enemy is the most imperative objective of Data hiding and henceforth clearly the security of a steganography framework will increment if the image quality stays unintelligible to an assailant regardless of whether he holds information about the implanting technique. It is likewise clear that specific zones in a picture are more productive for concealing information than alternate parts of the picture.

Keywords: Virtual Key Replacement, Data Hiding, Security, PSNR, MSE etc.

Considering the scaling based on Web is champion among divine basic components based on information development and furthermore analogy has been affecting insurance of detail information. Cryptography need system as anchoring the riddle of analogy along with extensive variety based on systems made into jumble along with unriddle the data in order to preserve effective information secrecy. Lamentably it's now and again unsatisfactory to grip the concreteness about a message puzzle, it may in like manner be vital to preserve the potentiality data secrecy. The entity acclimated to do here, abidly labelled as steganography.

Data hiding holds skill as well as art of microscopic coherence. Already stated achieved over camouflage data in farther type of data, therefore mask latency based on conveyed data. The conversation steganography continue in distinction to Greek argument "*stegos*" manifest "cover" and "*grafia*" imply "stating" symbolize in the act of "guarantee composing". Latest picture steganography the info is shrouded only in image. The term Steganography alludes via craft based on undercover correspondences. Aside executing steganography, it's workable as long as Person A to relay a mystery memo towards Person B in alike route, that nobody will realize the reality of message. Ordinarily, the message is installed inside

addition question admitted in the act of mask production, by pinching its equity. The coming about yield is admitted as a stegoimage. It is built with the end goal close to indistinguishable intuitive model of the mask production, and in the meantime it likewise contains the covered up message. It is this stegoimage that is sent amongst Person A and Person B.

In the event that anyone captures the correspondence, they will get the stegoimage, similar to mask image, it acts as troublesome undertaking considering authority to disclose that the stegoimage is definitely not guiltless. In this manner obligation of steganography provide guarantee that the foe respects stegoimage. Hence, the correspondence in the act of harmless. Information concealing system is a non specific term of outlining a wide arrangement of uses, for example, the term steganography, as talked about above, is received against Greek dialect aid secret written work. The method of conceal mystery data in a correspondence direct in such a way, that the specific presence of the data is disguised.

The Steganography calculations are help to perform mystery correspondence. The most mainstream information groups utilized are .bmp, .jpeg, .mp3, .txt, .doc, .gif. Data deposit without end is the approach in the direction of camouflage a secrecy data inside mask medium, for example, picture, video, content, sound. Concealed picture has numerous applications, particularly in the present current, innovative world. Preservation together along with mystery does misery as frequent society beside network. The shrouded information requisite guarded amid change as it may be gained by two different approach: Encryption and Data Hiding. Combination of this approach is utilized to expand information security.

Afterwards, inventing data camouflage innovations, peculiarly as steganography are admit to symbolize a jeopardy towards character safety, trade what's more, nationalized safekeeping activity. The antidote advancement to steganography preservation is constantly suggested as steganalysis, which conceivably portrayed into different division: Passive and dynamic. The fundamental endeavour about idle steganalysis will pick closeness otherwise hooky of covered data within specified media items. Dynamic steganalysis (or else labelled criminology steganalysis) advert towards physical exertion by involuntary heir in the direction of extricate/evacuate/change the genuine concealed information. During previously mentioned peculiar circumstances, dynamic steganalysis is not either similar to invasion to watermarking[27].

Related Research

A black & white picture requires just 1 bit for every pixel as contrasted and 8 bits for every dark pixel or 24 bits for each shading pixel. The little memory or capacity prerequisite makes a paired picture a perfect configuration for digitizing, preparing, transmitting and filing expansive measure of day by day records whose substance are ordinarily high contrast in nature. These reports incorporate different content and realistic archives.

Information stowing away is regularly accomplished by modifying some unimportant data in the host message. For instance, given a shading picture, Least Significant Bit based on every picture element conceivably reversal towards inserting concealed mystery is proposed by Van *et al.*[1]. E. Franz *et al.* show a concealing plan in view of the regular key stream generator[2]. Data covering up for security records (e.g., money) is examined by D. Gruhl[3].

Wang *et al.* Proposed Data hiding method that conceals information for different purposes, including security assurance and confirmation. Data Hiding installs messages into important pictures, alluded to as cover pictures, without making consideration pernicious people[4]. Information hiding on vast inserting

limit and maintaining high picture quality after messages are covered up input image. Be that as it may, vast installing limit and high picture quality make an exchange off circumstance, since a substantial implanting limit dependably acquires a significant measure of picture mutilation. It is important to maintain balance in between high installing limit and high picture quality. Impressive endeavours have concentrated on high installing limit or high picture quality in information concealing proposed by Wu *et al.*[5].

A basic and old steganography strategy LSB substitution, implants 'n' mystery bits within a wrap picture element by supplanting n Least Significant Bits substitution implement by Yang[6]. In spite of performing superior to different methodologies[7], this way is effectively identified by means of various pernicious plans moreover not think about revelation of individual. The attainability of accomplishing a high inserting limit against a individual revelation viewpoint acquire significant consideration. To accomplish elevated inserting limit, D.C. Wu *et al.* built up a pixel value differencing (PVD) method[8]. In this method pixel distinction stuck between 2 neighbouring pixels are utilized and to calculate how many number of bits are put up. A multi-pixel differencing and Least Significant Bit substitution approach projected by Jung *et al.* In this technique a square by means of 4 picture element is utilized in the direction of install information[9].

An information concealing plan in view of the modulus work, a variation Cartesian item be worked consequent to modulus capacity in the direction of shroud the message proposed by Lee *et al.*[10]. The above methodologies centre on accomplishing a high implanting limit. While endeavouring to accomplish high picture quality, proposed by Wang *et al.*[4], the picture quality is enhancing by utilizing the modulus capacity to diminish the inconsistency that is caused by using the PVD approach.

Picture steganography strategies that recommend immense installing limit along with convey a reduced amount of contortion towards the stego picture anticipated Chang *et al.*[11]. The inserting procedure install stream of mystery bits on the stego picture pixels. Rather than supplanting the Least Significant Bit of every picture element, already stated technique reinstate the picture element power through comparative esteem. The scope of adaptable pixel esteem is superior in border regions as compare to soft regions towards keep up great perceptual magnificence. Different piece inserting techniques are taken after; that chosen by the connection among genuine picture element along with the adjoining picture element. The adjoining picture element might be a pixel left, right, best or base to the real picture element[28]. The distinctive plans are two, three and four sided one. Double sided plot take higher along with left pixels, three side plans take higher, left and right while four sided take higher, left, right and base pixels. The installing limit and PSNR are contrarily relative to the sides considered.

Picture steganography conspire that settles the restriction of steganography system proposed in Chang *et al.*[11]. This technique is falling of limit issue i.e. the pixel decided for inserting end up unacceptable; since it surpasses the most extreme force level which is more noteworthy than 255 (greatest dark scale power). Less number of pixel bits are included, yet on said picture element that enhance the installing limit exclusive of trading off Peak Signal Noise Ratio[12].

An unusual picture steganography system examined by Amitava Nag *et al.* The mask picture spatial esteem is changed into Discrete Cosine Transformation (DCT); its lowest bit in a series is adjusted towards mystery message[13]. The mystery information used Huffman coding technique to preset preceding the inserting plan that accomplishes a noteworthy pressure rate. A superior inserting limit as well as PSNR is gotten utilizing indicated method. The said procedure is superior to the LSBs method proposed in Chang[11].

The inserting productivity is enhanced by receiving Matrix Embedding method, the plan proposed by Sarkar *et al.* ME-RA (matrix embedding repeat accumulate) is an information concealing calculation

used to shroud the mystery information. During the time spent inserting mystery information bits; it is important to alleviate the contortion jumping out at a cover picture[14]. To achieve this, grid installing is picked which utilize a hamming code lattice. In the projected endeavour, rather than hamming code a simple Exclusive OR task is operate lying on the input picture bits on the way to ensure its fortuitous event aligned with the mystery bits. The input bits are balanced in like manner to suit the mystery bits.

A watermarking procedure which is versatile to any geometrical twisting, for example, interpretation, turn, scaling and trimming presented on the watermarked picture proposed by Lin *et al.* It is intended to oppose any picture control endeavour both in spatial and recurrence space[15]. The most difficult issue in factor length watermarking is watermark synchronization. Watermark synchronization is where watermark arrangement and watermark length does not coordinate which is understood by unique programming.

Lingfang Zhang *et al.* have anticipated an immense safe watermarking method in recurrence space. The geometrical confused watermarked picture is tended to by format installing, since it has low processing intricacy. The watermark is installed adaptively in the low band utilizing Discrete Wavelet Transform which get darkened in human visual framework[16].

Lee *et al.* built up a plan to oppose geometric mutilation presented if any in the picture deliberately or inadvertently. This plan tends to both nearby and worldwide bending issues. To achieve this, unique information installing is facilitated in such picture preceding transmission[17]. These extraordinary bits are helpful in recuperating a geometrically mutilated picture; since enter data are implanted ahead of time. In their plan, a format based approach is received for information implanting. A predefined format is embedded into the three sub groups of Discrete Wavelet Transform, which help to recoup the first picture from misshaped picture.

The writing discoveries pass on that the steganography calculation is produced and tried in both spatial and frequency. Different installing philosophy, for example, versatile, settled piece and variable piece inserting strategy are endeavoured in both domain. To accomplish high payload limit, even the mystery information can be compacted through factor bit encoding procedure.

Applying Huffman compression alone won't result in higher implanting limit. Alongside Huffman method; if the other coding procedure, for example, Gray coding, Run length and Bit plane coding system are coordinated then it yield better outcomes. This approach is endeavoured in the proposed look into. Strength is dependably an auxiliary in steganography and essential in watermarking. In any case, it is balanced to outline the steganography framework to withstand straightforward picture control task, for example, turn, scaling and pressure. Despite the fact that it is obligatory in watermarking it turns into the optional objective for steganography. Geometrical contortion is tended to in the proposed inquire about. Turn/Flipping happened if any unintentionally in travel or manufactured unexpectedly by the interloper can be resolved and amended.

In any spatial area implanting strategy there will be an endeavour to change the cover picture pixel force incompletely, insignificantly or totally without trading off picture ancient rarities. A calculation named crossover inserting is tested and confirmed that there is no change or least change to the pixel force. This mitigates the bending striking the cover picture by proficient inserting strategy.

Proposed Methodology

Algorithm for the selection of Pixel component

In our proposed work we have to select the component of pixel. The following algorithm shows the working of selection of components present in a pixel. Pixel is also represented as picture element.

- Step 1: Select Input Image.
- Step 2: Select Picture element from input image.
- Step 3: Select Master colour component of image consist of Red, Green & Blue ingredients.
- Step 4: Select any components out of three.
- Step 5: if ((R + 32)>255) OR (R-32) <0), ((G + 32)>255) OR (G-32) <0), ((B + 32)>255) OR (B-32) <0), then cast off picture ingredients else replace its 5 LSB side bits with data bits.
- Step 6: Repeat step 4 to 5 until all sentinel pixel region not scanned.
- Step 5: Stop

Algorithm for the identification & Conversion of Key into Binary for the creation of Key File

In our work we have to convert our data in the form of Binary and saved the data behind Master colour components. Once the Component is identified we have to generate the key mapping table.

- Step 1: Select Input Image (I)
- Step 2: Input Secret Data
- Step 3: Convert Secret Data to Binary (SD)
- Step 4: Select Master Pixel (Mp)
- Step 5: Convert Master Pixel to Binary
- Step 6: For i=1 to Length (SD Binary)
- Step 7: Bit Bi = SD Binary (i)
- Step 8: For i=0 to 8
- Step 7: if Bi ==Mp(i)
- Step 8: Add i to Key File
- Step 9: Save Key

Algorithm for Data Compression of Key File

- Step 1: Input Key File
- Step 2: for I = 1 to 2

- Step 3: Cluster key file with Length (c) = i
- Step 4: Find c into the Key
- Step 5: If Frequency (c) >= 2
- Step 6: replace c with Single character that is A-Z, a-z etc
- Step 7: End
- Step 8: i = i - 1
- Step 7: Save Key Mapping Table.

Result Analysis

Payload Size	PSNR dB			
	Baboon	**Tiffany**	**Peppers**	**F16**
32 × 32	99	99	99	99
60 × 60	99	99	99	99
64 × 64	99	99	99	99
80 × 80	99	99	99	99
100 × 100	99	99	99	99
Average		99		

CONCLUSION

For some innovative recommended steganographic calculation, individual needs to assess its execution based on Image quality, PSNR & MSE.

REFERENCES

1. van Schyndel, R.G., Tirkel, A.Z. and Osborne, C.F. 1994. "A digital watermark," in Proc. *IEEE Int. Conf. Image Processing,* **2**: 86–90.
2. Franz E. *et al.,* 1996. "Computer-based steganography," in Information Hiding, *Springer Lecture Notes in Computer Science,* **1174**: 7–21.
3. Gruhl, D. and Bender, W. 1998. "Information hiding to foil the casual counterfeiter," in Proc. *Workshop Information Hiding*, IH'98, Portland, Apr. 1998.
4. Wang, R.Z., Lin, C.F. and Lin, J.C. 2000. "Image Hiding by Optimal LSB Substitution and Genetic Algorithm," *Pattern Recognition,* **34**(3): 671-683.
5. Wu, H.C., Wu, N.I., Tsai, C.S. and Hwang, M.S. 2005. "Image Steganographic Scheme Based on Pixel-Value Differencing and LSB Replacement Methods," IEE Proc.-Vis. *Images Signal Process.,* **152**(5): 611-615.

6. Yang, C.H. 2008. "Inverted Pattern Approach to Improve Image Quality of The Information Hiding by LSB Substitution," *Pattern Recognition,* **9**(1): 153-164.

7. Lee, L.S. and Tsai, W.H. 2009. "Data Hiding in Greyscale Images by Dynamic Program Based on A Human Visual Mode," *Pattern Recognition,* **42**(7): 1604-1611.

8. Wu, D.C. and Tsai, W.H. 2003. "A Steganographic Method for Images by Pixel-Value Differencing," *Pattern Recognition Letters,* **24**(9-10): 1613-1626.

9. Jung, K.H., Ha, K.J. and Yoo, K.Y. 2008. "*Image Data Hiding Method Based on Multi-Pixel Differencing and LSB Substitution Methods*," in Proc. International Conf. Convergence and Hybrid Information Technology, pp. 353-358.

10. Lee, C.F. and Chen, H.L. 2010. "A Novel Data Hiding Scheme Based on Modulus Function," *Journal of Systems and Software*, **83**(5): 832-843.

11. Chan, CK. and Cheng, L.M. 2004. "Hiding data in images by simple LSB substitution", *Pattern Recogn.,* **37**(3): 469 - 474.

12. Chen, P.Y and Wu, 2006. "A DWT Based Approach for Image Stegnography" *International Journal of Applied Science & Engineering,* **4**(3): 275-290.

13. Amitava Nag, Biswas, S. and Sarkar, D. 2010. "A Novel Technique for Image Steganography Based on Block-DCT and Huffman Coding", *International Journal of Computer Science & Information Technology,* **2**(3): 103-112.

14. Sarkar, A., Madhow, U. and Manjunath, B.S. 2010. "Matrix Embedding With Pseudorandom Coefficient Selection and Error Correction for Robust & Secure Stegnography ", *IEEE Trans. Inf. Foren Sec.,* **5**(2): 225-239.

15. Lin, Y.T, Huang 2011. "Rotation, Scaling, and translation Resilient Watermarking for Images", *IET Image Processing,* **5**(4): 328-340.

16. Lingfang Zhang, Xine You & Yuping Hu 2010. "A robust Watermarking algorithm against Geometric Distortions", Paper Presented at 3rd International Symposium on Information Processing, Qingdao, China, pp. 389-392.

17. Lee, M.S. and Chiu, 2010. "Image Recovery of Geometric Distorations with Multi-Bit Data Embedding", Paper presented at International Conference on Multimedia and Expo, pp. 382-387, Singapore.

18. Swain, G. and Lenka, S.K. 2014. "Classification of spatial domain image steganography techniques: a study" *International Journal of Computer Science & Engineering Technology,* **5**(3): 219-232.

19. Wang, Z. and Bovic, 2002. "Universal Image Quality Index", *IEEE Signal Processing Letters,* **9**(3): 81-84.

20. Khodai and Faez, 2012. "New Adaptive Stegnographic method using least-significant-bit substitution and PVD", *IET Image Processing,* **6**: 677-686.

21. Wu, D.C. and Tsai, W.H. 2003. "A steganographic method for images by pixel-value differencing", *Pattern Recognition Letters,* **24**(9-10): 1613–1626.

22. Ratnakirti Roya, Anirban Sarkara and Suvamoy Changdera, 2013. "*Chaos based Edge Adaptive Image Steganography*", International Conference on Computational Intelligence: Modeling Techniques and Applications (CIMTA) 2013.

23. Amrita Khamruia and Mandalb, J.K. 2013. "*A Genetic Algorithm based Steganography using Discrete Cosine Transformation (GASDCT)"*, International Conference on Computational Intelligence: Modelling Techniques and Applications (CIMTA).

24. Chang Chin Chen *et al.* 2007. "Reversible hiding in DCT based compressed images", Science Direct, *Information Sciences,* **177**(13): 2768–2786.

25. Anita Pradhan, Aditya Kumar Sahu, Gandharba Swain, K. Raja Sekhar, "*Performance Evaluation Parameters of Image Steganography Techniques*", International Conference on Research Advances in Integrated Navigation Systems (RAINS - 2016), April 06-07, 2016.

26. Allan G. Weber, 2011. The USC-SIPI Image Database: Version 5, Original release: October 1997, Signal and Image Processing Institute, University of Southern California, Department of Electrical Engineering. http://sipi.usc.edu/database/(Last accessed on 20th January, 2011).

27. Mahip Bartere and Deshmukh, H.R. 2017. "*Study of Data hiding mechanism using virtual Key replacement method*", International Conference on inventive computing & Informatics (ICIC).

28. Nityanandum, Ravichandran, Priyadharshini & Santron, N.M. "An Image stegnography for colour images using lossless compression technique", *International Journal of Computational Science & Engineering.*

29. Anita Pradhan, Aditya Kumar Sahu, Gandharba swain, K. Raja Sekhar, 2016. "*Performance Evaluation parameter of Image Stegnography Techniques*", International Conference on Research Advances in Integrated Navigation Systems (RAINS).

30. Ratnakirti Roy, Anirban Sarkar and Suvamoy Changder, 2013. "*Chaos Based Edge Adaptive Image Stegnography*", International Conference on Computational Intelligence: Modeling Techniques and Applications (CIMTA) 2013.