ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 8, Issue 7, July 2019

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

Ms. Sonali Lavangale, Prof. M.U. Karande

M.E Scholar, Dept. Computer Science and Engineering, Padmashri Dr.V. B. Kolte College of Engineering Malkapur, M.H, India

Professor, Dept. Computer Science and Engineering, Padmashri Dr.V. B. Kolte College of Engineering Malkapur, M.H, India

ABSTRACT: Data Hiding is the art 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.

I. INTRODUCTION

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.

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 8, Issue 7, July 2019

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].

II. RELATED RESEARCH

A black and 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 the filing expansive measure of day by day records whose substance are ordinarily high contrasts 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, the 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 shows a concealing plan in view of the regular key stream generator [2]. Data covering up for security records (e.g., money) are examined by D. Gruhl [3].

Wang et.al. A 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]. It is important to maintain balance in between high installing limit and high picture quality. Impressive endeavors 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 an 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 neighboring pixels are utilized and to calculate how many numbers 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 elements is utilized in the direction of installing 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 center on accomplishing a high implanting limit. While endeavoring to accomplish high picture quality, proposed by Wang et al. [4], the picture quality is enhanced by utilizing the modulus capacity to diminish the inconsistency that is caused by using the PVD approach.

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 8, Issue 7, July 2019

Picture steganography strategies that recommend an immense installing limit along with conveying a reduced amount of contortion towards the stage picture anticipated Chang et.al [11]. The inserting procedure installs stream of mystery bits on the stage 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 compared to soft regions towards keeping up great perceptual magnificence. Different piece inserting techniques are taken over; 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 the base of 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 conspirators 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). The Less number of pixel bits are included, yet on to say picture element that enhances 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 the 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 picking which utilize a hamming code lattice. In the projected endeavor, rather than hamming code a simple Exclusive OR task is operated lying in 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 endeavors 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 has anticipated an immense safe watermarking method in recurrence space. The geometrical confused watermarked picture tends 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
[13].

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 entering 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 subgroups of Discrete Wavelet Transform, which help to recoup the first picture from misshapes 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 endeavoring in both domains. 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 a 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 its yield better outcomes. This approach is endeavored in the proposed look into. Strength

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 8, Issue 7, July 2019

is dependably an auxiliary in steganography and essential in watermarking. In any case, it is balanced to outline the steganography framework to withstand a 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 connotation 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 endeavor 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.

III. PROPOSED METHODOLOGY

A. Architecture Diagram

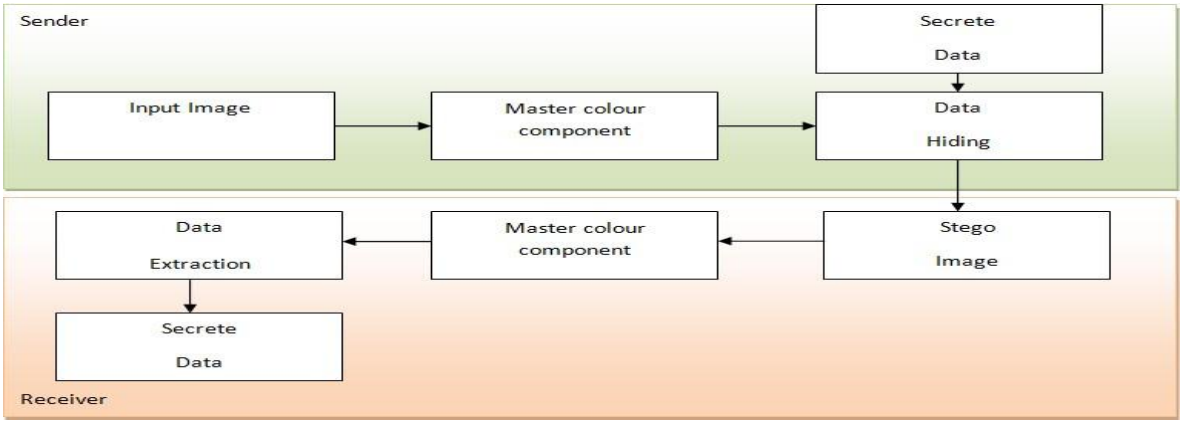


Fig. 1. Architecture Diagram

B. 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.

Step1: Select Input Image.

Step 2: Select Picture element from input image.

Step 3: Select Master colour component of image consist of Red, Green and 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 7: Stop

C. Algorithm for the identification and 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

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 8, Issue 7, July 2019

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 if Bi ==Mp(i) Add i to Key File end
end
Step 9: Save Key

D. 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
Replace c with Single character that is A-Z, a-z etc
i = i - 1
End
Step 6: Save Key Mapping Table.

IV. RESULT ANALYSIS

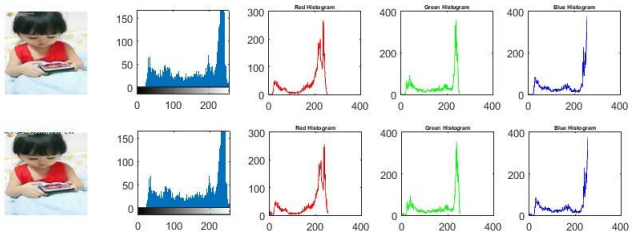


Fig. 2. Plot between Original and Resultant Image

Above figure shows comparision between Original Image (Image before data hiding) and Resultant Image (Image after data hiding). it shows that both images are same which are the indication of virtual data hiding.

TABLE I
PARAMETER WISE COMPARISON OF IMAGES

Parameters	Original Image	Result Image
Entropy	7.4613	7.4748
Mean	170.4939	170.6701
Standard deviation	77.8474	78.2165
Pure Height	100	100
Pure Width	300	300

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

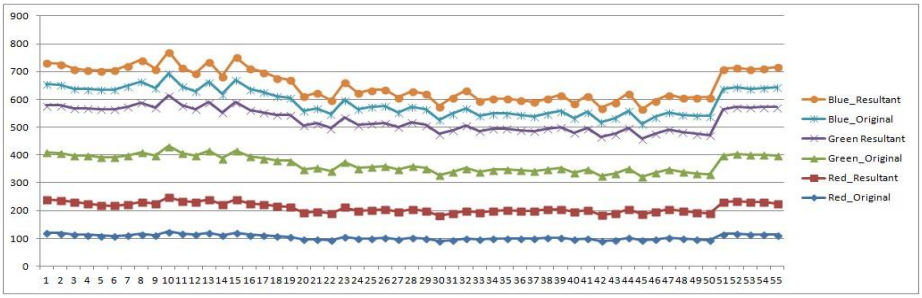
International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 8, Issue 7, July 2019

Fig. 3. Plot between Original and Resultant Image



V. CONCLUSION

For some innovative recommended steganographic calculation, individual needs to assess its execution based on Image quality, PSNR and MSE. Performance of proposed algorithm can be tested with various parameters like Mean Sqaure Error, PSNR, Entropy, Standard Deviation, Max Error etc. Result shows that, input image and image after data concealing are exactly same and not afetced by amount of data hidden.

REFERENCES

[1] R. G. van Schyndel, A. Z. Tirkel, and C. F. Osborne, "A digital watermark," in Proc. IEEE Int. Conf. Image Processing, vol. 2, 1994, pp.86–90.
[2] E. Franz et al., "Computer-based steganography," in Information Hiding, Springer Lecture Notes in Computer Science, vol. 1174, 1996,pp. 7–21.
[3] D. Gruhl and W. Bender, "Information hiding to foil the casual counterfeiter," in Proc. Workshop Information Hiding, IH'98, Portland, Apr. 1998.
[4] R. Z. Wang, C. F Lin, and J. C. Lin, "Image Hiding by Optimal LSB Substitution and Genetic Algorithm," Pattern Recognition, vol. 34, no.3, pp. 671-683, 2000.
[5] 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. Images Signal Process., Vol. 152, No.5, pp. 611-615, 2005..
[6] C. H. Yang, "Inverted Pattern Approach to Improve Image Quality of The Information Hiding by LSB Substitution," Pattern Recognition, Vol.9, No. 1, pp. 153-164, 2008.
[7] L. S. Lee and W. H. Tsai, "Data Hiding in Greyscale Images by Dynamic Program Based on A Human Visual Mode," Pattern Recognition, Vol. 42, No. 7, pp. 1604-1611, 2009.
[8] D. C. Wu and W. H. Tsai, "A Steganographic Method for Images by Pixel-Value Differencing," Pattern Recognition Letters, Vol. 24, No. 910, pp. 1613-1626, 2003.
[9] K. H. Jung, K. J. Ha, and K. Y. Yoo, "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, 2008.
[10] C. F. Lee and H. L. Chen, "A Novel Data Hiding Scheme Based on Modulus Function," Journal of Systems and Software), Vol. 83, No. 5, pp. 832-843, 2010.
[11] Chan, C-K., and Cheng, L.M. "Hiding data in images by simple LSB substitution", Pattern Recogn Vol. 37, No. 3, pp. 469 - 474, 2004.
[12] Chen, P.Y and Wu, "A DWT Based Approach for Image Stegnography" International Journal of Applied Science and Engineering, Vol 4, No.3, pp 275-290,2006
[13] Amitava Nag, Biswas S, Sarkar D "A Novel Technique for Image Steganography Based on Block-DCT and Huffman Coding" ,International Journal of Computer Science and Information Technology, Vol. 2, No. 3, pp. 103-112, 2010.
[14] Sarkar,A., Madhow, U. and Manjunath, B.S. "Matrix Embedding With Pseudorandom Coefficient Selection and Error Correction for Robust and Secure Stegnography ", IEEE Trans. Inf. Foren Sec. Vol.5 No. 2, pp. 225-239, 2010.
[15] Lin, Y.T, Huang "Rotation, Scaling, and translation Resilient Watermarking for Images", IET Image Processing, Vol. 5, No. 4, pp. 328-340, 2011.
[16] Lingfang Zhang, Xine You and Yuping Hu " A robust Watermarking algorithm against Geometric Distortions", Paper Presented at 3rd International Symposium on Information Processing, Qingdao,China, pp. 389-392, 2010.
[17] Lee, M.S and Chiu, "Image Recovery of Geometric Distorations with Multi-Bit Data Embedding", Paper presented at International Conference on Multimedia and Expo, pp. 382-387, Singapore, 2010.
[18] G.Swain, S. K. Lenka, "Classification of spatial domain image steganography techniques: a study" International Journal of Computer Science and Engineering Technology, vol.5, no.3, pp.219-232, 2014.
[19] Z.Wang and Bovic, "Universal Image Quality Index", IEEE Signal Processing Letters, vol.9, no.3, pp. 81-84, 2002.

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 8, Issue 7, July 2019

[20] Khodai and Faez, "New Adaptive Stegnographic method using leastsignificant-bit substitution and PVD", IET Image Processing Vol.6, pp.677-686, 2012.
[21] 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.
[22] Ratnakirti Roya,,AnirbanSarkara, SuvamoyChangdera ," Chaos based Edge Adaptive Image Steganography", International Conference on Computational Intelligence: Modeling Techniques and Applications (CIMTA) 2013.
[23] Amrita Khamruia, J K Mandalb," A Genetic Algorithm based Steganography using Discrete Cosine Transformation (GASDCT) ", International Conference on Computational Intelligence: Modelling Techniques and Applications (CIMTA) 2013
[24] Chang Chin Chen et al "Reversible hiding in DCT based compressed images", Science Direct, Information Sciences vol: 177, issue: 13 pages: 2768–2786 July (2007).
[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, 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] MahipBartere, Dr. H.R.Deshmukh, "study of Data hiding mechanism using virtual Key replacement method", International Conference on inventive computing and Informatics (ICIC), 2017.
[28] Nityanandum, Ravichandran, Priyadharshini and N.M.Santron, "An Image stegnography for colour images using lossless compression technique", International Journal of Computational Science and Engineering.
[29] Anita Pradhan, Aditya Kumar Sahu, Gandharba swain, K. Raja sekhar, "Performance Evaluation parameter of Image Stegnography Techniques", International Conference on Research Advances in Integrated Navigation Systems(RAINS), 2016.
[30] Ratnakirti Roy, Anirban Sarkar, Suvamoychangder, "Chaos Based Edge Adaptive Image Stegnography", International Conference on Computational Intelligence: Modeling Techniques and Applications (CIMTA) 2013.