A New Rule for Cost Reassignment in Adaptive Steganography

SYEDA ASMA FATIMA[1], K. MANOJ KUMAR[2]
[1]PG Scholar, Dept of CSE, Shadan Women's College of Engineering and Technology, Hyderabad, TS, India,
[2]Professor & HOD, Dept of CSE, Shadan Women's College of Engineering and Technology, Hyderabad, TS, India.

Abstract: In steganography plans, the twisting feature is used to chart alteration costs on cover segments that are exceedingly key to the security of contemporary adaptable steganography. There are a couple of productive standards at reassigning the costs depicted by utilizing a given mutilation incorporate, which could propel the redemption period of the looking at steganographic count. On this paper, a novel regard reassignment conclude that is realized to no longer one yet a bundle of present mutilation limits the expenses alloted on a few pixels by techniques for different steganographic philosophies mayhap incredibly specific regardless of the method that those methodology display close security levels. This pixels are named "questionable pixel". Exploratory effects demonstrate that steganalys is capacities are not fragile to dicey pixels; in this manner these picture element are legitimate to keep extra payloads This administer the questionable Pixels earlier (CPP) sprint the show. Following the tried and true rule, that present an esteemre assignment plot. Through sizeable examinations on a duo of sorts of stegocounts, steganalys is features and cowl databases ;That show a certain CPP run can improve the bond of best in class steganographic estimations for spatial photographs.

Keywords*:* CPP, MAC, MF, CSI.

I. INTRODUCTION

Steganography is a framework for stealthy communication, which plans to disguise riddle messages into basic digital media without drawing question [1], [2],Designing steganographic figurings for various cover sources is challenging due to the pivotal nonattendance of exact models. Currently, the best approach for laying out content adaptive steganography relies upon constraining the distortion between the cover and the relating stego dissent. The distortion is procured by selecting a cost to each modified cover segment (e.g., pixel in the spatial territory picture), and the messages are embedded while restricting the total distortion which is the aggregate of costs of all changed elements. The first procedure in perspective of the structure of minimal distortion is HUGO (particularly indistinct stego) [3]. HUGO defines the pixel's cost by the changing plentifulness of the steganalyzer's features caused by modifying the present pixel, and pixels that make the component vectors more veered off will have higher costs. The features of steganalyzer SPAM (subtractive pixel proximity organize) [4] is used as a piece of HUGO. A steganalyzer's features are for the most part delivered by abusing correlations between the foreseen residuals of neighboring pixels [4].Because the pixels in smooth areas can be correctly predicted, the modifications in such locales will be easily recognized by steganalyzers. In this way the embedding changes of HUGO will be collected inside completed regions. Regardless, HUGO can be distinguished by a steganalyzer with a higher dimension of features, for instance, SRM (spatial rich models) [6].

In SRM, the foreseen residuals are created in various directions and conduct, so the connections between's pixels can be also mishandled. Therefore, one pixel, to be in a smooth area or a textural zone, should be unobtrusively portrayed for steganography. In case the pixel can be unequivocally exhibited in any direction, it should be considered as a smooth call attention to doled out greater cost. With this learning, Hulob et al. proposed the computation WOW [5] which doles out high costs to pixels thatare additionally obvious by a bank of directional channels. WOW improves the security of HUGO under the area of SRM[6]. UNIWARD (general wavelet relative contorting) [10]generalizes the cost limit of WOW to make it less troublesome and more fitting for embedding in a self-confident region, including the spatial space and DCT region. Consequently UNIWARD has a similar execution appeared differently in relation to WOW in spatial territory. Liet al. proposed the procedure HILL [11], which improves WOW by spreading the costs with a low-pass channel. In HILL [11],the close-by modification probabilities are leveled out and thus the changes group in the confounding regions (compressed as cost spreading (CS) keep running in Sec. III).The above methods design cost work in a commercial hocor trial way. Sedighi et al. proposed indicate driven approaches [12],in which Multivariate Gaussian (MG)or Multivariate Generalized Gaussian (MVG) scattering was used to show the uproar residuals of pixels by expecting them to be free yet with contrasting changes.

The models are established by surveying the progressions and after that the costs are computed by restricting the force of a perfect statistical test. As a matter of fact, little costs will be consigned to residuals modeled with extensive vacillations, which are just the significantly completed regions. Another redesigned show driven approach MiPOD is also proposed by Sedighi et al. In MiPOD the interactive effects of adjoining pixels have been taken into consideration. MiPOD achieves a predominant security by working the power of the most exceptional marker instead of the KL divergence, and accepting cost spreading depicted in by smoothing the Fisher Information of showed pixels. Apparently, the bleeding edge flexible steganographic methods consider much concerning the cost assignment which can be particularly related to the modification probabilities and the embedding zones. In the interim, steganalys is follows up. The best high-dimensional steganalytic features are thought to be flexible since they

see the adaptive steganography as a kind of assurance zone steganography. MaxSRM [7] outlines the co-occasion systems considering the most extraordinary assessed modification probability of a group of pixels as a weight coefficient, for which the steganalytic feature is inclined to isolate features from the surface region. The same idea is associated in [8], in which the mean estimated modification probability of a social occasion of pixels is used as a weight coefficient.

Beginning late, an enhancing confirmation channel aware steganalysis join was proposed by Denemarket al.[9], in which the weight coefficient of co-event matrices is supplanted by the residuals in SRM. These adaptive steganalysis can accomplish better shows in detecting steganography since they concentrate more on the finished region instead of treating finished locales and smooth ones equally. In this case, changing pixels basically considering the texture complexity will never again drive the security of steganography. Denemarket al. and Li et al. take the interaction between contiguous pixels into thought, and power the modifications to be amassed a relative way (thick as synchronizing change heading (SMD) lead in Sec. III).This technique may cheat versatile steganalys is to assess an incorrect change likelihood for pixels, thusly potentially weakening the shows of adaptable steganalys is and promoting the security of steganography. The design of adaptable steganography is more right in the latest works. By virtue of changing in finished zone, spreading costs to neighbors utilizing the CS control or pressing modification directions with the SMD oversee, they are away to locate a more suitable procedure for installing. By and by, these gainful rules are essentially used to update one existing turning limit for steganography.

In this paper, I consider how to make anadvanced contorting limit from a heap of existing ones. I propose a security improved direct by joining several comparable systems, following our past work. Note that some inconsequential bending steganographic strategies exhibit comparable security introductions in repudiating detection, but they depict mutilation works in completely different manners. Along these lines, they may dispatch all around different expenses to the same pixel. We call such pixels questionable pixels, and consider that these defective pixels have the potential to accommodate more payloads. I can overhaul un detect ability by giving need of changes to such sketchy pixels. This novel lead the Controversial Pixels Prior (CPP)rule. Showed up distinctively in connection to our past work, by utilize a redirection in Sec. IV of this paper to give a starter demonstrate that the CPP rule is persuading, and consolidate trades of the refreshing function and the metric of faulty degree. In Sec. VI, two groups of cases, CPP (UNI chose) and CPP (HILL derived),are added to demonstrate that the measure of crucial methods for the CPP lead can be no under three, and the improvements are still indispensable. For impel examination, we entwined the CPP rule with the CS direct and the SMD provoke accomplish a further improvement.

Whatever is left of this paper is managed as takes after. After introducing the structure of unimportant mutilation steganography in Sec. II, we accumulate two or three existing rules for adaptive steganography in Sec. III. In Sec. IV, proposed CPP rule and familiarize an engendering with demonstrate the benefits of the CPP rule instinctually. In Sec. V, I give a full depiction of the framework of CPP-based steganographic plot and discuss the streamlining limit and the metric for sketchy degree. In Sec. VI, basic parameters are settled through experiments and a few social events of steganalyls is experiments have been done to avow the upsides of the CPPrule. Besides demonstrate joining the CPP continue running with other effective measures in Sec. VI, and two remarkable databases are used for propel confirmation here. I make conclusions in Sec. VII.

II. PREVIOUS WORKS ON COST ASSIGNMENT FOR ADAPTIVESTEGANOGRAPHY

In past steganographic plans, one essential control for cost task is Complexity Prior. Unpredictability earlier means that the steganographer should give need for modification to the mind boggling zones, as it were, flighty parts in a picture ought to have high needs. The philosophy of unpredictability earlier is that non-intermittent surfaces and noisy regions are hard to show, subsequently making adjustments in such regions frequently prompts minor deviation in steganalytic feature space and to be less perceptible. Indeed, all of the methods itemized in [3], [5], [10] – [12], and take after this rule unequivocally, and characterize contortion works by investigating how to sensibly characterize the perplexing degrees of pixels in the sense of opposing discovery. In addition, in view of the center idea of Complexity Prior, a few compelling tenets for positioning priority of pixels have been proposed by past works. These rules for cost task in versatile steganographic plans can be abridged as takes after.

A. Cost Spreading (CS) Rule

This manage is likewise called clustering guideline. It requires that the expenses of altering two neighboring components ought not to contrast enormously. In other words, a component with high alteration need should spread its high-rank to its neighborhood, and the other way around for an element with low need. This decides recommends that it is better to make changes in a bunched way as opposed to in a scattered one. By applying this run, a pixel that is close to a high-rank complex area ought to have a higher priority than another pixel in less unpredictable locale, despite the fact that these two pixels have same expenses in the meaning of distortion function. Correspondingly, the inserting changes are clustered. This control was first effectively utilized as a part of HILL [11] to enhance WOW [5], and after that utilized as a part of to enhance MVG. Experiments have shown that the cost spreading rule can make less deviation in a steganalytic include space.

B. Synchronizing Modification Direction (SMD) Rule

The previously mentioned CS manages depends on the idea of minimizing the whole of expenses of every single changed pixel, which is called added substance twisting model. In added substance bending model, the alterations of pixels are thought to be independent. Actually, the neighboring installing changes will interact with each other, and in this manner a non-added substance contortion model

will be more appropriate for versatile steganography intuitively. Recently, the main viable standard on the most proficient method to misuse the power of non-added substance mutilation was discovered freely by Denemark et al. and by Li et al.; the proposed thought is based on a supposition that the steganalytic classifier cannot distinguish a picture with all pixels changed by +1 or - 1 at the same time from a unique cover picture. Tests imply that synchronizing the change bearings of neighboring pixels can altogether enhance the security performance. This thought can be condensed as the control of synchronizing modification course, which implies that neighboring in similar ways, i.e., +1 or - 1 at the same time, will present littler expenses. This govern is likewise called clustering modification.

III. A NEW RULE FOR RANKING PRIORITY OF PIXELS

The previously mentioned CS administer and SMD run are proposed to improve a solitary existing bending capacity, however by comparing different calculations, I found a fascinating phenomenon. Namely, that some steganographic techniques have an extremely similar security execution while characterizing mutilations in exceptionally different ways. Among these techniques, there is recognition on the costs task for a few pixels, as it were, the costs assigned on a few pixels are huge in one strategy however small in another. I characterize these pixels as "Disputable Pixels" because they are alloted with altogether different expenses in different algorithms. Indeed, even with such an inconsistency, some of these algorithms can in any case give a similar level of security. This phenomenon suggests that changes on such controversial pixels have little effect on highlights of staganalysis. Based on these examinations, I propose another lead for adaptive steganography. I take points of interest of the differences among amount steganographic techniques and center on those disputable pixels. Our proposed control is designated the questionable pixels earlier (CPP) run, and is portrayed as follows:

A. Questionable Pixels Prior (CPP) Rule

This administer endeavors to discover disputable pixels by looking at a few comparable steganographic strategies, and the CPP decide recommends that it is better to give these dubious pixels need of modification rather than considering the many-sided quality of take care of components only. Since costs speak to the need of a pixel, and the costs have an immediate association with the adjustment probabilities as expressed in Eq. (7), I center around the change probabilities (abbreviated as MPs). As appeared in Fig. 1, assuming that the pixels in the blue squares are standard pixels, the costs of those pixels are little and equivalent to each other, which means they have a similarly high need of modification when simply considering many-sided quality earlier. The pixels in thered squares are some dubious ones. In current adaptive steganography, it is ordinary to change pixels in the blue blocks first as a result of their high needs, while the CPP rule expects us to alter the needs of questionable pixels in the red squares to be higher.

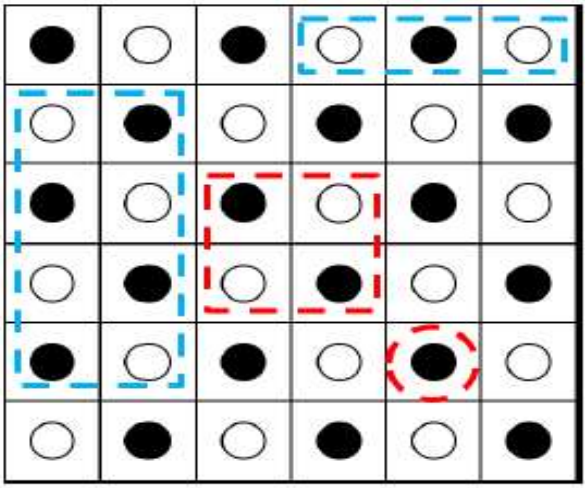

Fig.1.Illustration of the location of controversial pixels for the CPP rule.

Along these lines, modifications are more prone to be grouped in the red squares, which are involved by disputable pixels. I guess that this distinctive method for change will present less deviation in a steganalytic space than customary ways do. To legitimize our claim, we execute a recreation with the accompanying advances.

- Take 1000 grayscale pictures from the BOSSBasever.1.01 database haphazardly, and trim a square of size 64 × 64 from the focal point of each picture. The new generated picture set is indicated {Cj}(j ∈ {1,… … ,1000}).
- Choose two versatile steganographic strategies as contrastive methods to find questionable pixels, here use UNIWARD [10] and WOW [5] as two fundamental methods because that they have shown a very much like security performance under the discovery of SRM [6].
- Set the change probabilities of dubious pixels to be which implies that the payload of a single pixel can achieve the greatest as indicated by information theory. What's more, set the payload to be 0.2bpp to keep the implanted message lengths predictable in several algorithms.
- Modify common components of the pictures in {Cj} in the order of need after characterized bends by UNIWARD and WOW, while just altering questionable elements after finding them utilizing the CPP run the show. The generated stego picture sets are signified as {S Aj}; {S Bj}, and {SCj}respectively.
- Calculate the 34671-D SRM steganalytic highlight vector for each picture. The got include sets are indicated by{ f (Cj)}; { f (S Aj)}; { f (S Bj)}, and { f (SCj)}.Calculate the MMD (most extreme mean disparity which measures the separation between the list of capabilities of cover pictures and that of stego pictures) between { f (Cj)}and { f (S Aj)}; { f (S Bj)}, and { f (SCj)}. Get the average valule of the MMD and standard deviation more than 10different free tests on the dataset. Signify these three outcomes as MMD(CPP), MMD(UNI), MMD(WOW),and at that point make an examination.

Fig. 2 provides an example of the modification locations described in Step(d) above. The statistical results of MMD and its standard deviation are given in Table I,

with the rightmost rows containing the total change rates. From the statistical results, the MMD(CPP) value is apparently smaller than that of the other two methods. The change rate of CPP is between that of UNIWARD and WOW, even though change rate has no nonstop relation with security. It can also be referenced data that may indicate that the CPP rule has found a better balance between the payload of a single ingredient and the whole change rate. Since MMD represents the distance in steganalytic feature space between cover set and stagiest, the simulation results prove that making modification in controversial regions is more make safe than that making them in ordinary regions. In Sec. V, I put forward a new strategy of designing distortion function by applying the CPP rule. I introduce more in Sec. VI, in which several aforementioned rules for deceitful distortion functions to achieve a prominent increase in security.

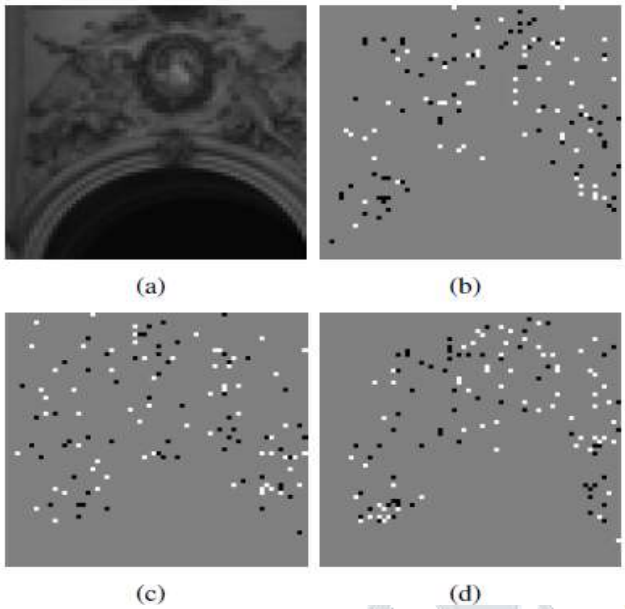

Fig.2. Illustration of modified location in an image of size 64 × 64 for the CPP rule. The black, white and gray pixels represent +1, -1 and no change, respectively. (a) Cropped 1013.pgm of BOSS base. (b) Modified location of CPP rule. (c) Modified location of UNIWARD. (d) Modified location of WOW.

TABLE I: Simulation results of MMD, Standard Deviation And Change Rates

Payload	Embedding method	MMD	Change rate
0.2	CPP	$5.3240 \times 10^{-2} \pm 0.0051$	2.93%
	UNIWARD	$9.1198 \times 10^{-2} \pm 0.0027$	2.56%
	WOW	$8.9245 \times 10^{-2} \pm 0.0047$	3.66%

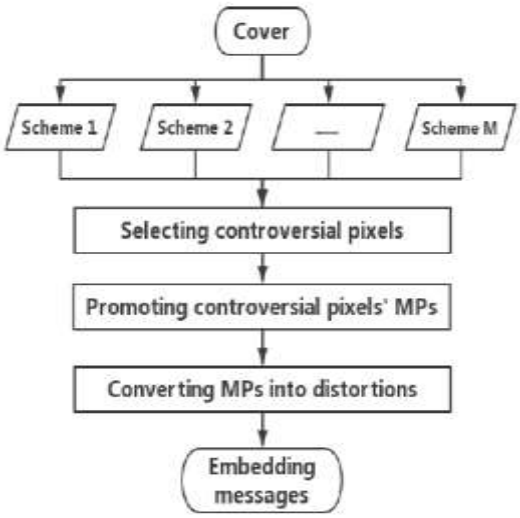

Fig.3. Flowchart of proposed CPP based method.

IV. A NOVEL STRATEGY BASED ON THE CPP RULE

A. Description of the CPP Based Scheme

With the new perspective on cost reassignment, I propose an enhanced steganographic method based on the CPP rule, that generates a new distortion function from several existing ones. As shown in Eq. (7), the distortion can be converted into MP, which then determines the payloads assigned on each pixel. Therefore, attention on the MPs when sharp for controversial-pixels. The framework of the proposed embedding method is depicted in Fig. 3. Suppose that M comparable steganographic methods whose sanctuary performances are similar. First, we compute the MPs of pixels with these M distortion functions. Second, i label the controversial-pixels according to the MPs. Third; I adjust the MPs to promote the controversial pixels' priorities with the CPP rule. Fourth, the adjusted MPs are changed into a new deformation function. Finally, the messages are set in with STCs according to the new distortion function.

V. EXPERIMENTS

A. Setups

In this paper, four disjoint sets are utilized as the image database. In Sec. VI-B, we first take BOWS-2-OrigEP3[25](simplified as BOWS-2) which containing 10,000 512 ×512 8-bit grayscale pictures as the database with which to explore the ideal setting of the questionable limit . I that point check utilizing the other picture set, to be specific the BOSS base ver.1.01 database containing 10,000 512×5128-piece grayscale pictures. In Secs. VI-D and VI-E, all of the steg-analysis tests depend on the BOSS base ver.1.01.In Sec. VI-F, two different datasets, BOSS base C and BOSSbase-J85 are utilized for encourage check. The security of all steganographic plans are assessed utilizing a steg-analyzer that is an indicator prepared on a given cover source and its stego form implanted with a settled payload. The finder is first prepared utilizing the best in class 34,671-D SRM feature set [6] with the troupe classifiers for a few groups of illustrations. For additionally explores, we utilize the selection channel-mindful element maxSRMd2 [9]. Execution in terms of opposing recognition is assessed by the testing mistake, which is registered as the mean estimation of the false positive rate and the false negative

rate, arrived at the midpoint of more than 10 arbitrary parts of the dataset. A bigger arrangement mistake rate implies stronger security.

B. Assurance of Controversial Threshold

Initially envision the appropriation of chose controversial pixels in Fig. 4 by differing the estimation of. UNIWARD and WOW are utilized to characterize the essential twisting capacities under the payload of 0.4bpp.check the disputable pixels in the stego variant of 6.pgm of BOWS-2 by setting = 3; 5and 10. Clearly, the areas of dubious pixels spread with expanding. As specified, the aggregate change rate of pixels has a direct connection with relative payload. Considering that the message length is constrained, the quantity of chose controversial pixels ought to likewise be balanced comparing to the payload. In Fig. 5, we plot the bend of differing patterns of SRM testing mistake as for. The CPP based plan is CPP(UNI,WOW) and the database is BOWS-2. The security performances vary inside a restricted range when the controversial edge changes both on account of 0.2bppand 0.4bpp. The biggest testing mistake shows up around at = 3 for 0.2bpp and at roughly = 8 for 0.4bpp. To determine the connection between an ideal and payload, I conduct a few steganalytic analyzes under other payloads, and the picked esteems are recorded in Table IV. Steganalytic probes CPP(HILL, MiPOD), of which the two fundamental strategies are HILL [11] and MiPOD[15]. The steganalytic include is maxSRMd2, since HILL and MiPOD have comparative security exhibitions under the detection of max SRM. The ideal qualities for CPP(UNI,WOW) and CPP(HILL, MiPOD) are indicated 1 and 2, separately, in Table IV.

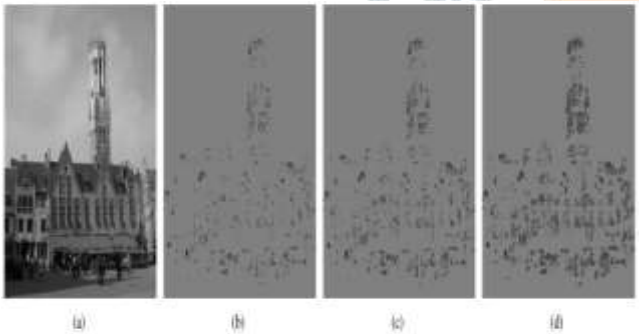

Fig.4. Location of the top α% of large controversial pixels: (a) the sample cover image 6.pgm of BOWS-2, (b) α= 3, (c) α= 5, and (d) α = 10. Where the dark-gray points represent the controversial pixels and the light-gray points represent ordinary ones.

C. Selection of Basic Steganographic Methods for CPP

In Sec. V-A, we mentioned that an important condition in our proposed CPP rule is that several adaptive steganographic methods exist with comparable security performances. This is the essential principle for selecting candidate algorithms for the CPP rule: basic methods have comparable security performances. In theory, any pair of steganographic methods canbe used in the CPP rule as basic functions as long as they have similar security performances. Some off-the-shelf methods can be used as the basic distortion functions of CPP rule. UNIWARD and WOW are the best cases for the CPP rule. Since they characterize mutilation works in truly similar way, the security exhibitions under the identification of SRM of these two techniques are amazingly near each other on BOSS base ver.1.01. This gathering of calculations was utilized first in the accompanying experiments. HILL and MiPOD include another combine of cases in the following investigations. Slope is a versatile algorithm which uses the CS lead to characterize costs, while MiPOD is an completely display driven plan that likewise thinks about the CS rule. Slope accomplishes a more elevated amount of security than MiPOD under the discovery of SRM while MiPOD performs better than HILL under the determination station mind full steganalytic featuremaxSRMd2.

The match of previously mentioned strategies are not as similar as UNIWARD and WOW, but rather they are at present the most viable steganographic techniques; in this way i utilize them to prove the viability of our CPP run the show. For facilitate confirmation, i endeavor to include the quantity of basic methods in the CPP run the show. As of late, another thought has been proposed in, in which diversion hypothesis has been taken into consideration for planning contortion work. The primary ideas poused in is utilization of a current versatile steganographic method to characterize an essential twisting capacity, and afterward to define a predisposition work in the structure of amusement hypothesis to adjust the conveyance of alteration probabilities. In this paper, i utilize UNIWARD and HILL, separately, to characterize the basic contortion capacity and afterward recreate the experiments as itemized. I find that the security of the method generated from UNIWARD is very near the original UNIWARD under the discovery of maxSRMd2, just like that using HILL. This outcome shows that the new strategy depicted can be received by the CPP control as an essential technique. Since the inclination work is vital in this strategy, we name the new twisting capacities BIAS UNI and BIAS HILL. To make another approximative fundamental bending function for the CPP manage, we keep on making a couple of adjustments to unique UNIWARD and HILL. Chen et al. proposed a method, the fundamental thought of which is doing pre-processing on a cover picture utilizing the system of un sharp masking which can somewhat change the textural highlights of cover images.

After the preprocessing, we can reclassify distortions on the new cover with UNIWARD or HILL, and consequently obtain different mutilation works that are meant UM UNI and UM HILL, individually. I show some factual information of modification probabilities in Table VI to demonstrate the nuances among unique UNIWARD, BIAS UNI, and UM UNI, and among unique HILL, BIAS HILL, and UM HILL. The sharpening parameter for UM UNI and UM HILL is 0.8.The security exhibitions under maxSRMd2 are additionally listed, and they tried payloads extend from 0.1bpp to 0.5bpp.The three furthest left sections list factual information for the modification probabilities of the whole cover picture, including the most extreme, the interquartile run, and the change. The five furthest right sections are the trying mistakes and standard deviations opposing maxSRMd2 from 0.1bpp to 0.5bpp. Obviously, the three strategies identified with UNIWARD are quite different from each other, despite the fact that they have similar security exhibitions. Those three techniques identified with HILL are in a similar circumstance. Along these lines, we

utilize these two gatherings of algorithms as another two cases for the CPP run the show.

VI. SCREENSHOTS

Screenshots of this paper is as shown in bellow Figs.5 to 17.

Fig.5. Home Page.

Fig.6. Patient Registration Page.

Fig.7. Patient Login Page.

Fig.8. Admin Login Page.

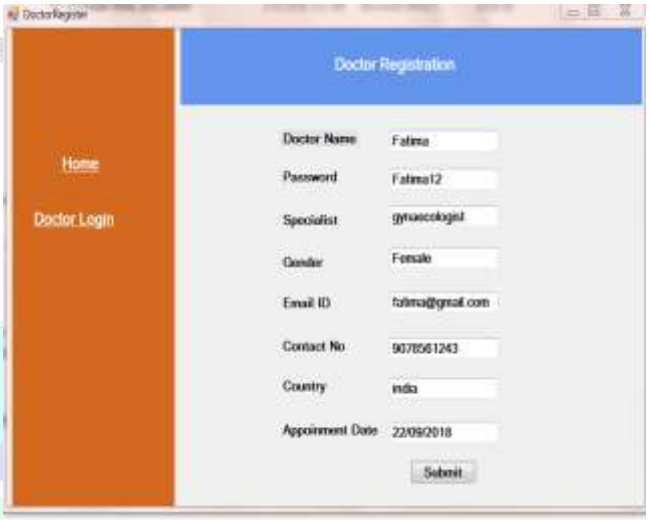

Fig.9. Doctor Registration Page.

Fig.10. Doctor Login Page.

Fig.11. Image Cropping.

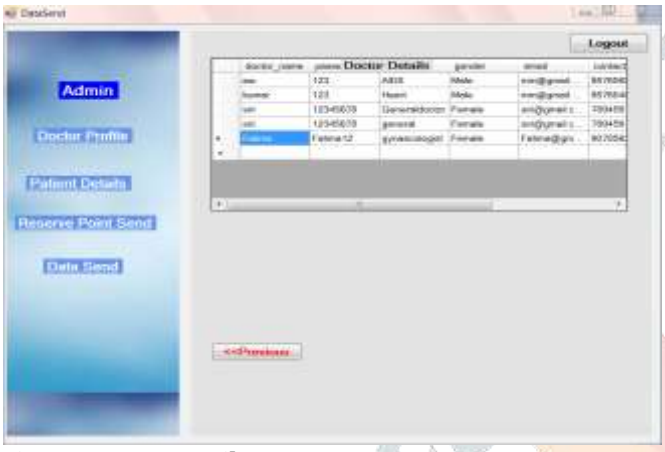

Fig.12. Doctor Details.

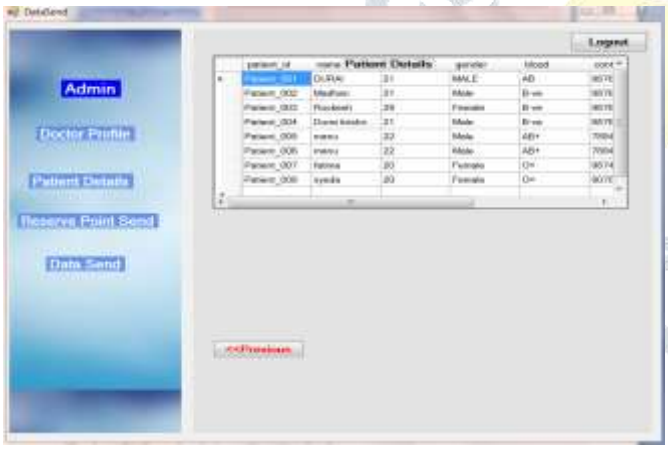

Fig.13. Patient Details.

Fig.14. Get Reserve Point.

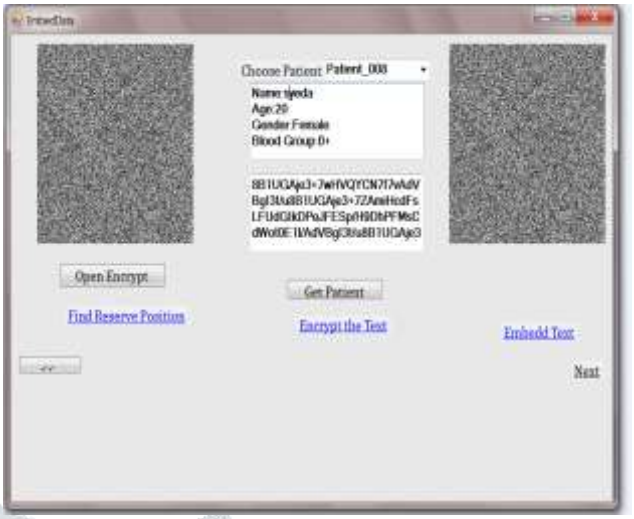

Fig.15. Embedded.

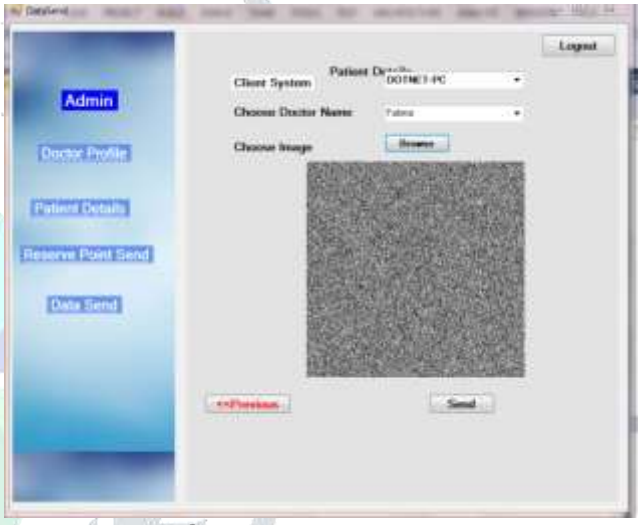

Fig.16. Data Send.

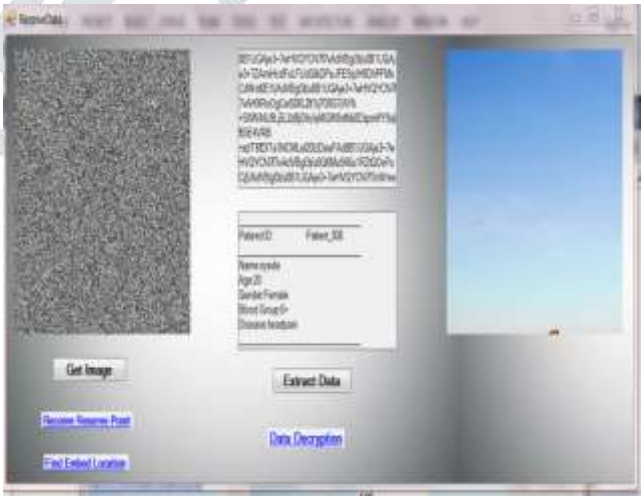

Fig.17. Receiver data.

VI. CONCLUSION

The contemporaneous framework diminishes the layout of secure steganography in trial spreads towards the trouble of finding adjacent conceivable outcomes for the twisting limit that link with authentic scrumptiousness before long. By working out the present theory in factor for a individual

mixture of the mutilation work, likely affirm the approach and look at changed options presented towards the steganographer before long.

VII. REFERENCES

[1] J. Fridrich, Steganography in Digital Media: Principles, Algorithms andApplications. CambridgeUniversity Press, 2009.
[2] B. Li, J. He, J.w. Huang, and Y. Q. Shi , "A survey on imagesteganography and steganalysis," Journal of Information Hiding andMultimedia Signal Processing, vol. 2, no. 2, pp. 142-172, 2011.
[3] T. Pevn´y, T.Filler, and T. Bas, "Using high-dimensional image modelsto perform highly undetectable steganography," Proc. of InternationalWorkshop on Information Hiding, vol. LNCS 6387, pp. 161-177, Jun.28-30, 2010.
[4] T. Pevn´y, P. Bas, and J. Fridrich, "Steganalysis by subtractive pixeladjacency matrix," IEEE Trans. on Inf. Forensics and Security , vol. 5,no. 2, pp. 215-224, Jun. 2010.
[5] V. Holub and J. Fridrich, "Designing steganographic distortion usingdirectional filters," Proc. of IEEE Workshop on Information Forensicand Security, pp. 234-239, Dec. 2-5, 2012.
[6] J. Fridrich and J. Kodovsk´y, "Rich models for steganalysis of digital images," IEEE Trans. on Inf. Forensics Security, vol. 7, pp. 868-882,Jun. 2012.
[7] T. Denemark, V. Sedighi, V. Holub, R. Cogranne, and J. Fridrich,"Selection-channel-aware rich model for steganalysis of digital images,"Proc. of 6th IEEE International Workshop on Information Forensics andSecurity, Atlanta, GA, USA, Dec. 3-5, 2014.
[8] W. X. Tang, H. D. Li, W. Q. Luo, and J. W. Huang, "AdaptiveSteganalysis Based on Embedding Probabilities of Pixels," IEEE Trans.on Inf. Forensics Security, vol. 11(4), pp. 734-745, Apr. 2016.
[9] T. Denemark and J. Fridrich, "Improving Selection-Channel-AwareSteganalysis Features," Proc. of IS&T, Electronic Imaging, Media Watermarking,Security, and Forensics 2016, San Francisco, CA, Feb. 14-18,2016.
[10] V. Houlb and J. Fridrich, "Digital image steganography using universaldistortion," Proc. of ACM Workshop on Information hiding and multimediasecurity, pp.59-68, Jun. 17-19, 2013.
[11] B. Li, M. Wang, J. W. Huang, and X. L. Li, "A new cost function forspatial image steganography," Proc. of IEEE International Conferenceon Image Processing, Oct. 27-30, 2014.
[12] J. Fridrich and J. Kodovsk´y, "Multivariate Gaussian model for designingadditive distortion for steganography," Proc. of IEEE ICASSP, Vancouver,BC, May 26-31, 2013.

Author's Details:

Ms. SYEDA ASMA FATIMA has completed B.TECH (CSE) from Shadan Women's College of Engineering And Technology, Khairthabad. JNTU University Hyderabad. Presently, she is pursuing her Masters in Computer Science and Engineering from Shadan Women's College Of Engineering And Technology, Hyderabad, TS. India.

Mr.K.MANOJ KUMAR has completed B.Tech (CSE) from K.S.R College Of Engineering And Technology, Tiruchengode, M.Tech (CSE) from K.S.R college of engineering and technology, Ph.D from Annamalai University, Chidambaram, Currently he is working as an Professor and Head of CSE Department in Shadan Womens College of Engineering And Technology, Hyderabad, TS. India.