International Journal on Future Revolution in Computer Science & Communication Engineering
Volume: 3 Issue: 8
ISSN: 2454-4248
187 – 196

An Effective Bit Plane X-ORing Algorithm for Irretrievable Image Steganography

Mr. A. Balasubramani
Research Scholar, Faculty of Computer science & Engineering,
Siddharth Institute of Engg. & Tech., Puttur, AP, India.

Dr. Chdv. Subba Rao
Professor, SVU College of Engineering,
S. V. University, Tirupathi, A. P, India.
Email: balunbkr@yahoo. co. in

Abstract: The technical data of concealing secret info in side verbal exchange is known as Steganography; as a result the attending of skulking info is cloaked. it is the method of concealment noesis in same or a distinct media to limit awareness via the intruders. This paper introduces new system whereby irreversible steganography is employed to hide an image inside the equal medium in order that the key info is cloaked. The key image is usually referred to as payload and therefore the supplier is usually referred to as cover image. X-OR operation is employed amongst mid-level bit planes of supplier image and excessive level bit planes of knowledge image to come up with new low level bit planes of the stego photograph. recovery method involves the X-ORing of low stage bit planes and middle degree bit planes of the stego shot. targeted on the result of the recovery, ulterior data shot is generated. A RGB color image is employed as carrier and therefore the info photograph could be a grayscale image of dimensions but or adequate the dimensions of the carrier snapshot. The planned procedure extensively will increase the embedding capability without drastically reducing the PSNR value

Keywords— *Irretrievable Steganography, Payload, Carrier image, High level bit plane, Mid level bit plane, excessive level bit plane.*

*****

I Introduction

Ultra-modern day's speech needs excessive stage of protection in transmission. There area unit 2 approaches of achieving this: one by mistreatment securing the channel and therefore the alternative is by securing the message. Steganography could be a sensible illustrious and ordinarily used technique that manipulates experience (messages) so as to hide their existence. This method has several applications in laptop computer science and alternative associated fields: it's accustomed defend navy messages, company data, personal records, then forth.

Steganography is that the art and science of communication that hides the presence of power (Clair at al., 2001). It conceals the terribly existence of the message by mistreatment engrafting it within a carrier file of some kind. A snoop will intercept AN encrypted message; but he may not even perceive whether or not a steganographic message exists. Steganography, makes a trial to forestall AN interloper from suspecting that the data is there (Westfeld et al., 1998).The intention of steganography is to avert drawing awareness to the transmission of the key message.

Alternatively, steganalysis could be a means of detection potential secret communication mistreatment steganography. That is, steganalysis tries to beat steganography strategies. It depends on the very fact that activity power in digital media amends the carrier and introduces wonderful signatures or some kind of debasement that may be exploited. Hence, it's necessary that a steganography technique create such that hidden messages are not detectable (Lin et al., 2004; Rabah, 2004; Morkel et al., 2005). Steganography entails the activity of quite ton of media like text, photo, audio, video records in another media of identical kind or of specific vogue, before the message hidden within the hand-picked media is transmitted to recipient. At the receiver's end, reverse system is administrated to urge well the customary understanding (Krenn, R.).

 ISSN: 2454-4248
187 – 196

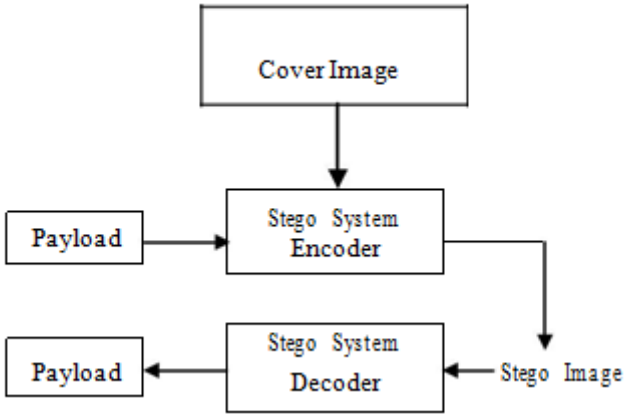


Figure 1: Steganographic Flow

The general technique of steganography is shown in figure one. 2 essential expectations that a steganography algorithmic program should live the maximum amount as are: (1) mammoth amount of secret bits may additionally be embedded within the host exposure, therefore the algorithmic program should with success enforce it, (2) the visual noise conferred thanks to embedding of the key information can got to be at tokenish degree. invisible stego-snapshot excellent is that the foremost feature of any steganography algorithmic program. There square measure variety of procedures that may be utilised to cover secret data inside a picture like LSB approach, injection, substitution, and new unharness (Krenn, R.). several the present algorithms do not discover the 3 dimensional characteristics of a RGB image for information concealment. Our quest is to implant secret information throughout distinct dimensions of a RGB image. within the planned technique we have got used the thought of injection wherever payload is substituted in parts of the supplier.

II Related work

In the field of hidden ability extraction from a stego exposure severe study work is occurring around steganalysis. to urge the easier of steganalysis schemes several steganography schemes are projected, that explore the multiple dimensions of canopy image. several ideas and strategies were projected to relaxed data i.E., typically concealing of text in footage. the straightforward procedure to try and do constant is Least large Bit (LSB) different technique. However, it's its possess obstacles (Anderson et al., 2001).Steganalysis will be quite merely performed on LSB different method (Dumitrescu et al., 2002).

Cheeldod et al. (2008) projected Associate in Nursing adjustive steganographic method that selects the distinctive neighborhood of curiosity (ROI) inside the quilt image. data will be embedded in these areas. These square measureas are chosen supported human cuticle tone detection. adjustive steganography are not Associate in Nursing handy goal for assaults primarily once the hidden message is little (Chang et al., 2008). Embedding capability and fantastic physical property for the stego-graphics square measure with success equipped by suggests that of the tri-approach component worth differencing procedure (Chang et al., 2008). the best PSNR that this theme can do is thirty eight.89dB with approximate embedding capability of two bpp. The influence analysis suggests that the projected method achieves higher PSNR and higher embedding potential as examine to the theme projected with the help of river et al. (2008).

Babu et al. (2008) projected steganographic mannequin authentication of secret ability in photograph steganography which will be wont to verify the integrity of the key message from the stego-photograph. The payload during this technique is remodeled into spatial space creating use of separate ripple remodel. The permutation of DWT coefficients square measure then embedded within the spatial space of the quilt image. This permutation is finished with the verification code. DWT coefficients square measure wont to generate the verification code. For this reason the system will verify every and each row that has been changed through wrongdoer.

Moon et al. (2007) projected a hard and fast 4LSB approach to imbed an appropriate quantity of data. It might probably effectively be applied and also the degradation within the ensuing exposure simply is not visually recognizable. nonetheless, the predominant difficulty of this theme is that the encoded message can also be with ease recovered and even altered with the help of zero.33 party. Lie et al. (1999) projected Associate in Nursing adjustive system of variable size bit substitution rather than constant size to regulate the activity potential. though these approaches (Chang et al., 2008; baboo et al., 2008; Moon et al., 2007; Lie et al., 1999) develop the embedding capability moreover as stage of security, the visible distortion offered could be a motive of state of affairs. The projected theme enhances the embedding capability at the same time as reduces the visible distortion given.

 ISSN: 2454-4248
187 – 196

III Issues in steganography

Any steganography algorithmic rule can ought to call back 2 predominant issues steganographic security live and steganalysis. Steganographic protection live that any steganographic system includes must be smart outlined. the tactic can ought to satisfy any sure standards relevant for steganographic security. Steganalysis offers with varied analysis approaches used on any algorithmic rule to reason the vulnerabilities associated with the algorithmic rule.

There area unit specific steganographic security measures as special in (Cachin, 1998; Zollner et al., 1998). If you'll distinguish between duvet-snapshot and stego-picture, assumptive one has unlimited computing power then the approach is liable to attacks. Let pc denote the prospect distribution of cover-picture and note denote the prospect distribution of stego-photo. Cachin (1998) defines a steganographic algorithmic rule to be secure if the relative entropy between the quilt-object and also the stego object probability distributions (pc and note, respectively) is at the most.

$$D(P_C \| P_S) = \int P_C \cdot \log \frac{P_C}{P_S} \leq \varepsilon \quad (1)$$

From this equation we note that detectability D(.) increases with the ratio P_C P_S which in Flip means the chance of steganalysis detection may additionally increase. A steganographic method is presupposed to be cleanly relaxed if e = zero (i.E. pc = PS). On this case the likelihood distributions of the quilt and stego-objects ar indistinguishable. cleanly secure steganography algorithms ar known to exist. In our planned rule, we tend to shall acquire cleanly relaxed steganography with larger embedding capability. The detectability perform is further compatible for inspecting image steganography schemes the place the embedding potential may well be terribly low. additional applicable live for visual distortion in photograph steganography with excessive embedding potential is peak sign to Noise quantitative relation (PSNR).

3.2 Steganalysis

There area unit 2 systems to the downside of steganalysis; one is to provide you a steganalysis methodology explicit to a close steganographic formula. the opposite is developing techniques which could be impartial of the steganographic formula to be analyzed. every and each of the 2 techniques has its own benefits and drawbacks. A steganalysis methodology precise to associate degree embedding system would provide glorious outcome once verified best thereon embedding system, and will fail on all totally different steganographic algorithms. we tend to detain mind these components to be extraneous and handiest center of attention on the capability to get the presence of a message. In our projected formula we tend to shall foil innumerable the steganalysis methodologies if not all cowl Image

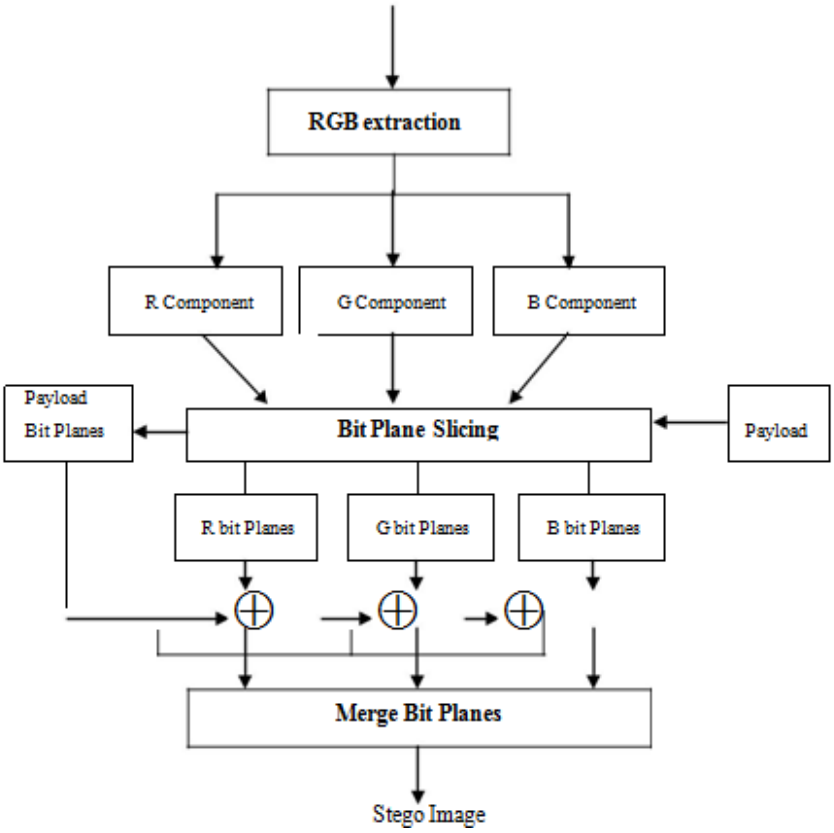


Figure 2: Bit plane X-ORing algorithm

 ISSN: 2454-4248
187 – 196

IV Proposed Scheme

The larger embedding potential is that the pay attention of the projected theme. The projected theme additionally eliminates the requirement of the quilt image to urge well the payload. Stego photograph is employed to urge well the payload. It reduces the requirement for a snug channel to share the quilt pics prior the begin of any secret dispatch. confirm two illustrates the operational escort the flow of the projected technique. The projected formula has 3 phases. 1st section includes bit plane chopping of the quilt snap nearly as good because the payload into eight bit planes. This formula takes any RGB color photograph as a cover snap, therefore RGB add-ons area unit separated before the bit plane slicing. 2d section performs X-OR operation amongst one in all the foremost middle stage bit planes of the quilt image and excessive degree bit planes of the payload and therefore the result's injected into the remaining curb level bit planes of the quilt image. The 0.33 section recovers the payload from the stego snap by means that of X-ORing the middle degree bit planes of the stego image with low stage bit planes of the stego image. The ensuing bit planes area unit the bit plane of the grayscale payload. 1st larger order 2 or 3 bit planes area unit thought to be excessive stage bit planes, next 2 or 3 higher bit planes area unit thought-about to be mid-level bit planes.

First phase

Different components of the RGB cover image are separated in this phase. The major task of bit plane extraction of cover as well as payload image is done for further processing. This phase is operational at transmission end of any communication.

Let C be the RGB cover image. The R, G, and B components of the cover image C are separated. Let us denote these components as C_R, C_G and C_B respectively. Each component is sliced into eight bit planes.

$$\left(C_R|C_G|C_B\right) = \text{split\_comp}(C)$$

$$\left(C_R(1)|C_R(2)|C_R(3)|.....|C_R(7)|C_R(8)\right) = \text{dec2binp}(C_R, 8)$$
$$\left(C_G(1)|C_G(2)|C_G(3)|.....|C_G(7)|C_G(8)\right) = \text{dec2binp}(C_G, 8)$$
$$\left(C_B(1)|C_B(2)|C_B(3)|.....|C_B(7)|C_B(8)\right) = \text{dec2binp}(C_B, 8)$$

The function *split_comp()* separates three components of an RGB image. Equations (2)- (4) slices each component into eight bit planes, where $C_R(1)$, $C_G(1)$ and $C_B(1)$ are the highest level bit planes of C_R, C_G, and C_B respectively and $C_R(8)$, $C_G(8)$ and $C_B(8)$are the lowest level bit planes of C_R, C_G, and C_B respectively. Similarly, payload P is sliced as in equation (5).

$$\left(P(1)|P(2)|P(3)|P(4)|P(5)|P(6)|P(7)|P(8)\right) = \text{dec2binp}(P, 8)$$

Second phase

This phase performs Bit plane X-ORing on different bit planes of cover and payload images. First three bit planes of payload P; P(1), P(2), and P(3) are X-ORed with mid level three bit planes of C_R and the result is stored in the low level three bit planes of C_R. The basic idea behind X-ORing the mid level bit planes of cover image with the high level bit planes of the payload is that some of the characteristics of mid level bit planes remain intact in the resulting bit planes due to the nature of the X-OR operation. When we insert these planes in the lower level bit planes of the cover image, we are essentially transforming the bit patterns of the lower level bit planes into the bit patterns of the mid level bit planes of the cover image. This diminishes the expected distortion in the resulting stego image.

$$C_{RM}(6) = \text{XOR}\left(C_R(5), P(1)\right)$$
$$C_{RM}(7) = \text{XOR}\left(C_R(4), P(2)\right)$$
$$C_{RM}(8) = \text{XOR}\left(C_R(3), P(3)\right)$$

$$C_{BM}(7) = \text{XOR}\left(C_B(6), P(7)\right)$$
$$C_{BM}(8) = \text{XOR}\left(C_B(5), P(8)\right)$$

$$C_{RM} = \text{bin2decp}\left(C_R(1)|C_R(2)|C_R(3)|.....|C_{RM}(7)|C_{RM}(8)\right)$$
$$C_{GM} = \text{bin2decp}\left(C_G(1)|C_G(2)|C_G(3)|.....|C_{GM}(7)|C_{GM}(8)\right)$$
$$C_{BM} = \text{bin2decp}\left(C_B(1)|C_B(2)|C_B(3)|.....|C_{BM}(7)|C_{BM}(8)\right)$$

The function *bin2decp()* converts an array of binary planes into a decimal plane. Stego image S is formed by merging these three modified components.

$$S = \text{Merge\_Comp}\left(C_{RM}, C_{GM}, C_{BM}\right)$$

Merge_Comp() merges three components to form a RGB image. So, S is the stego image obtained after phase three.

Third phase

This phase is the recovery phase. Payload is recovered from the stego image at the receiving end. Recovery process is just the reverse of phase two. Stego image is split into the equivalent red, green and blue component.

$$\left(C_{RM}|C_{GM}|C_{BM}\right) = \text{split\_comp}(S)$$

The function *split_comp()* separates three components of an RGB image. Now, individual color components are sliced into bit planes.

$$\left(C_{RM}(1)|C_{RM}(2)|.....|C_{RM}(7)|C_{RM}(8)\right) = \text{dec2binp}(C_{RM}, 8)$$
$$\left(C_{GM}(1)|C_{GM}(2)|.....|C_{GM}(7)|C_{GM}(8)\right) = \text{dec2binp}(C_{GM}, 8)$$
$$\left(C_{BM}(1)|C_{BM}(2)|.....|C_{BM}(7)|C_{BM}(8)\right) = \text{dec2binp}(C_{BM}, 8)$$

 ISSN: 2454-4248
187 – 196

The payload bit planes are recovered by X-ORing the respective bit planes of each component.

$$RP(1) = XOR(C_{RM}(5), C_{RM}(6))$$
$$RP(2) = XOR(C_{RM}(4), C_{RM}(7))$$
$$RP(3) = XOR(C_{RM}(3), C_{RM}(8))$$
$$RP(4) = XOR(C_{GM}(5), C_{GM}(6))$$
$$RP(5) = XOR(C_{GM}(4), C_{GM}(7))$$
$$RP(6) = XOR(C_{GM}(3), C_{GM}(8))$$
$$RP(7) = XOR(C_{BM}(6), C_{BM}(7))$$
$$RP(8) = XOR(C_{BM}(5), C_{BM}(8))$$

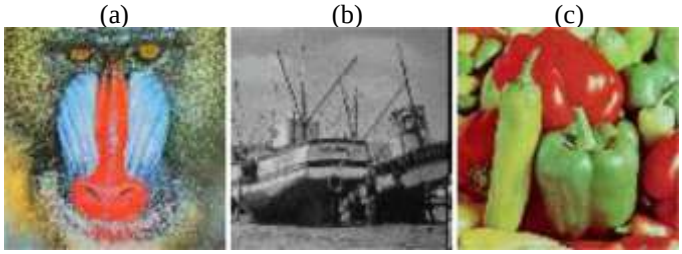
These recovered bit planes are combined to recover the payload.

$$RP = bin2decp(RP(1)|RP(2)|RP(3)|.....|RP(7)|RP(8))$$

V Experimental results

To investigate the potency of the projected procedure we have a tendency to embedded the equal payload in six one-of-a-kind quilt pics Lena River, Barbara, Boat, vegetables, Pepper, and catarrhine of extraordinary complexness. All of the cover pictures are chosen from typical exposure set utilised in several state-of-artwork. The quilt pictures and also the payload ar shown in figure three(a)-(f) and figure three(g) severally. In every example the scale of the quilt exposure (M x N)) and also the dimensions of the payload (m x n) convinced succeeding constraints m $m \leq M$ & $n \leq N$ ..

(a) (b) (c)



(d) (e) (f)

(g)

Figure 3: Test images (a)-(f) and Payload (g). (a) Lena; (b) Barbara; (c) Greens; (d) Baboon; (e) Boat; (f) Pepper; (g) Cameraman.

By method of taking a canopy image of size comparatively larger than the size of payload the noise within the sego photograph may also be diminished extra. The key bit planes ar made by suggests that of playacting X-OR operation amongst the bit planes of the quilt photo and therefore the bit planes of the payload. the general payload is same and impartial of the quality of the cover photograph.

With our theme eight bits of the key data ar inserted in each pel of the duvet photo, which implies there by victimisation eight bit pel understanding of the payload is embedded in twenty four bit pel data of the quilt photo. the most important obstacle in growing the embedding capability is that the rise in visible distortion within the stego image. It's largely known that the distortion of the stego image is tough to note by suggests that of the human eyes as long because the PSNR price is more than or up to thirty sound unit (Lee et al., 2008).

The amount of knowledge inserted in every and each illustration of the experiments is saved constant to analyze the distortion offered within the stego photo, whereas the quilt image in every and each example is changed. despite the fact that, the distortion is visually unrecognisable the introduction of noise is inevitable. Illustration of the experiment has constant payload (Cameraman). though eight pel data of the payload is distributed over distinctive bit planes of the cover image, the visual distortion is just about unrecognisable.

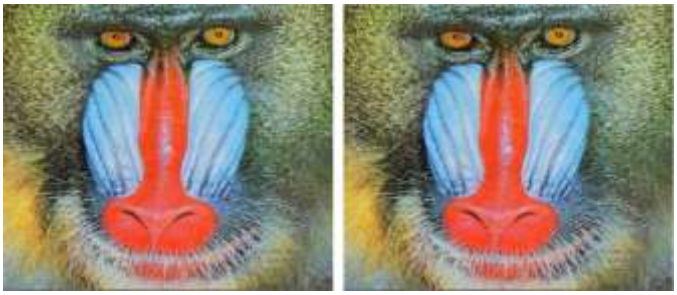
The fundamental methodology wont to verify the noise in stego image is peak-signal-to-noise-ratio (PSNR). potency of any image steganography algorithmic rule depends on activity capability and embedding potency. So, we have a tendency to take into account each aspects to research the results. PSNR is associate objective live for subjective analysis of degree of similarity between an inspired image and a stego image (Baekl et al., 2010). PSNR is outlined as;

ISSN: 2454-4248
187 – 196

a g

b h

c i



d j

e k

 ISSN: 2454-4248
187 – 196

f l

Alternate in cowl photograph will no longer have a sway on the visible aspects of the payload once extraction. Visible istortion within the stego image is minimal , if we alter the quilt image for the identical payload. complexness of the photograph "Barbara" is one-of-a-kind in several respects even then the distortion within the stego image for the identical payload (Cameraman) is negligible. The predominant demand of any image steganography algorithmic rule is minimal visible distortion within the ensuing stego photograph and it should be same for specific cowl pics. The results illustrate that the projected algorithmic rule conforms to those specifications

Table 1 Mean Square Error for different components of the cover image and Payload

Images	Mean Square Error (decimal)		
	Red	**Green**	**Blue**
Barbara	8970	8190	9330
Lena	6070	6130	7210
Green	10100	9480	11300
Baboon	8350	6420	8740
Boat	6164	6164	6164
Pepper	6522	10525	9092

VI Performance and Comparisons

Outcome evidenced in table two illustrate analysis of planned theme with (Lin et al., 2004) and (Lee et al., 2008). The planned theme achieves or so equal PSNR (dB) for distinctive cover pics, for a similar payload. For this reason, the choice of cover image should not be a imperative thought for the planned rule. one image is up to carry the whole payload and one needn't take under consideration a sequence of pictures for information embedding. For special sized payload, the alternate in PSNR for special cover pictures is shown in table three. Outcome evidenced in table 3 apparently illustrate the reality that for a given quilt exposure the PSNR is stable for distinct sized payloads. most embedding ability and also the highest PSNR achieved in state of design and planned theme has been represented in table four. The planned system attains higher embedding potential whereas protective the well-liked PSNR. The planned rule is economical enough in achieving higher and steady PSNR as compared to (Lin et al., 2004) and (Lee et al., 2008) as evidenced in figure five.The exchange in PSNR for exceptional payload is evidenced in verify half-dozen. For increasing payload the planned rule confer minimum trade PSNR. Despite the very fact that the size of the payload is augmented, the PSNR price by no suggests that goes to a lower place the minimum needed value of 30dB.

 ISSN: 2454-4248
187 – 196

Table 2 Comparison results (Lin et al., 2004), (Lee et al., 2008), and proposed scheme

Images	Embedded Data	PSNR(dB) (Lin et al., 2004)	PSNR(dB) (Lee et al., 2008)	Average PSNR(dB) Proposed Scheme
Barbara	4,60,800 bits	38.12	34.74	40.08
Lena		38.52	34.32	39.94
Greens		38.38	34.27	40
Baboon		38.26	34.84	40.04
Boat		38.40	34.41	40.07
Pepper		38.45	34.24	40.04

Table 3 Comparison of PSNR for different cover images and different size payload using proposed scheme

Payload (Bits)	Barbara PSNR(dB)	Lena PSNR(dB)	Greens PSNR(dB)	Baboon PSNR(dB)	Boat PSNR(dB)	Pepper PSNR(dB)
20,000	40.05	39.97	39.94	39.89	40.07	40.05
80,000	40.09	39.95	39.93	40	39.99	40.02
3,20,000	40.05	39.96	39.99	40.04	40.01	40.06
4,60,800	40.08	39.94	40	40.04	40.07	40.04

Table 4 Comparison of Embedding Capacity and PSNR for state of art and the proposed scheme

Steganography Schemes	Maximum Embedding Capacity (bpp)	Maximum PSNR (dB)
(Lin et al., 2004)	1	38.52
(Chang et al., 2008)	1	38.89
(Babu et al., 2008)	0.99	50.13
4 LSB	4	36.67
(Lie et al., 1999)	0.45	40
(Baekl et al., 2010)	1	58.42
(Lee et al., 2008)	1	34.84
Proposed Scheme	8	40

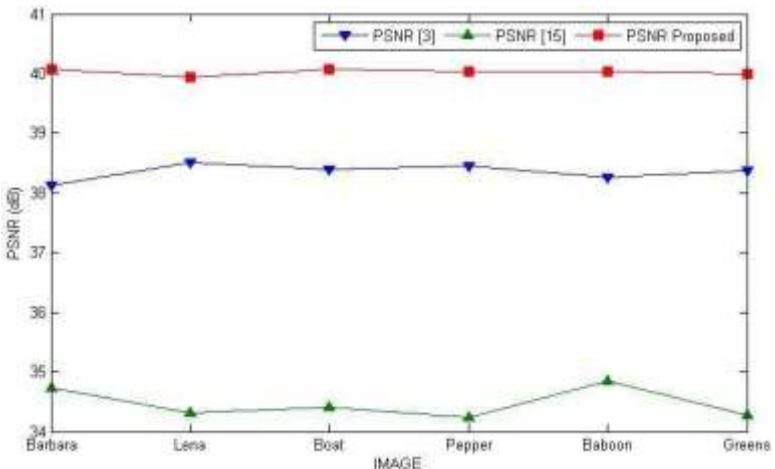


Figure 5: Comparison results (Lin et al., 2004), (Lee et al., 2008), and the proposed scheme

 ISSN: 2454-4248
187 – 196

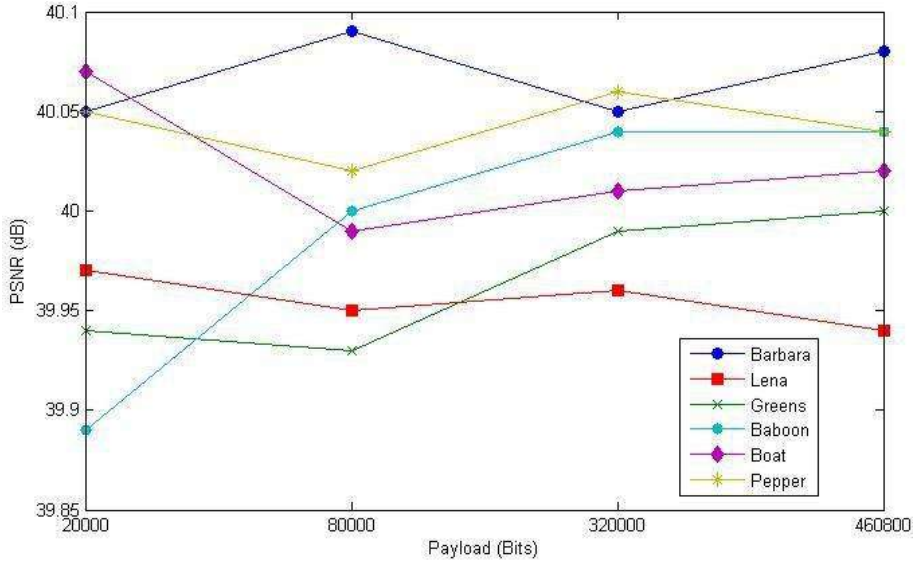


Figure 6: Comparison of PSNR for different cover images and different payload using proposed algorithm.

Table 5 Comparison of time taken for completions in non-threading, two threads, four threads

Size of array to be stored	Time Taken for completion Non-Threading (in sec.)	Time Taken for completion two threads (in sec.)	Time Taken for completion four threads (in sec.)
100	0.007	0.0009	0.00018
1000	0.0056	0.0013	0.00063
10000	0.1341	0.0038	0.00198
20000	0.26722	0.0056	0.00496
40000	0.6338	0.0112	0.00825

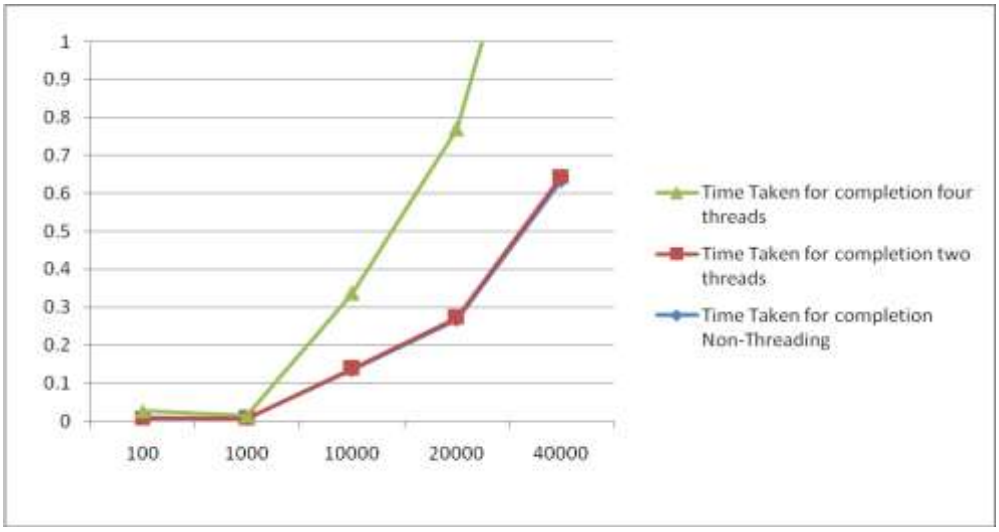


Figure 7 Comparison of time taken for completions in non-threading, two threads, four threads

VII Conclusion

This paper proposes AN rule that exploits the multiple dimensions of a RGB photograph to insert a secret photograph. the method now not achieves high bit per component embedding however in addition manages diminished MSE within the succeeding stego-snapshot. Bit plane X-ORing is employed to switch the bit planes of the one in every of the parts of the quilt shot. the following stego photograph is of the identical measure because the dimensions of the cover image, that nullifies the detection of hidden ability within the carrier. convalescence method entails X-ORing of distinctive bit plains of the stego image. The projected method attains larger PSNR

 ISSN: 2454-4248
187 – 196

and embedding potential. during this theme the requirement for shared cowl pics for restoration of the payload is taken out of the shot. further enhancements area unit possible on this procedure if another correlation would be placed amongst the R, G, and B parts of the quilt-photograph and also the payload. Our future work can involve operating with color portraits as payload. A method in addition must be developed for grayscale payload pics whose component depth is over eight pixels, as is that the case in technical makes use of like scientific imaging or faraway sensing.

References

[1] Anderson, R.J. and Petitcolas, F. A. P. (2001) 'On the limits of the Steganography', IEEE Journal Selected Areas in Communications, 16(4), pp. 474-481.

[2] Babu,K. S., Raja, K. B., Kumar, K. K., Manjula Devi, T. H., Venugopal, K. R. and Pataki, L. M. (2008) 'Authentication of secret information in image steganography', IEEE Region 10 Conference, TENCON-2008, pp. 1-6.

[3] Baekl, J., Kim, C., Fisherl, P. S. and Cha, H. (2010) '(N. 1) Secret Sharing Approach Based on Steganography with Gray Digital Images'. IEEE 978-1-4244-5849-3.

[4] Cachin, C. (1998) 'An information-theoretic model for steganography', 2nd International Workshop Information Hiding, vol. LNCS 1525, pp. 306–318.

[5] Clair and Bryan. (2001) 'Steganography: How to Send a Secret Message', www.strangehorizons.com/2001/20011008/steganography.shtml.

[6] Chang, K. C., Chang, C. P., Huang, P. S. and Tu, T. M. (2008) 'A novel image steganographic method using Tri-way pixel value Differencing', Journal of multimedia, 3(2).

[7] Cheddad, A., Condell, J., Curran, K. and McKevitt, P. (2008) 'Enhancing Steganography in digital images', IEEE Canadian conference on computer and Robot vision, pp. 326-332.

[8] Dumitrescu, S., Wu W.X. and Memon, N. (2002) 'On steganalysis of random LSB embedding in continuous-tone images', Proc. International Conference on Image Processing, Rochester, NY, pp. 641-644.

[9] Krenn, R. (2004) 'Steganography and Steganalysis', http://www.Krenn.nl/univ/cry/steg/article.pdf.

[10] Lee, C. C., Wu, H. C., Tsai, C. S.and Chu, Y. P. (2008) 'Adaptive lossless steganographic scheme with centralized difference expansion', (Elsevier), Pattern Recognition 41 , pp. 2097 – 2106.

[11] Lie, W. N. and Chang, L. C. (1999) 'Data Hiding in images with adaptive numbers of least significant bits based on human visual system', IEEE international conference on image processing, vol. 1, pp. 286-290.

[12] Lin, C. C. and Tsai, W. H. (2004) 'Secret Image Sharing with Steganography and Authentication', Journal of Systems and Software, 73(3). pp. 405-414.

[13] Moon, S. K. and Kawitkar, R.S. (2007) 'Data Security using Data Hiding', IEEE International conference on computational intelligence and multimedia applications, vol. 4, pp. 247- 251.

[14] Morkel, T., Eloff, J. H. P. and Olivier, M. S. (2005) 'An Overview of Image Steganography', Information and Computer Security Architecture (ICSA) Research Group, Department of Computer Science, University of Pretoria, SA.

[15] Westfeld, A. and Wolf, G. (1998) 'Steganography in a Video conferencing system, in proceedings of the second international workshop on information hiding', vol. 1525 of lecture notes in computer science, Springer, pp. 32-47.

[16] Rabah, K. (2004) 'Steganography - The Art of Hiding Data', Information technology Journal 3 (3).

[17] Zollner, J., Federrath, H., Klimant, H., Pfitzman, A., Piotraschke, R., Westfeld, A., Wicke, G. and Wolf, G. (1998) 'Modeling the security of steganographic systems',