Steganography Using Genetic Algorithm for Robust Cryptographic Encryption in Computer Forensics

MOHD.ABDUL.KHADER .KHAN[1], Dr.SYED ABDUL SATTAR[2]

[1]Research Scholar, CMJ University, Meghalaya, India

[2]Professor & Dean of Academics, Royal Institute of Technology & Science, Andhrapradesh, India

E-Mail: khader_all@yahoo.co.in

Abstract: Steganography will be the science about "invisible" correspondence. The reason for Steganography will be to keep up secret correspondence among 2 gatherings. The secret data could be hiding in content like image, audio, or video. This manuscript contributes a new picture steganography strategy to conceal numerous secret pictures & keys in color cover picture utilizing "Integer Wavelet Transform (IWT)". There will be no visual change among the cover & stego picture. The extracted secret pictures are also comparable to real secret pictures. Better "PSNR (Peak signal to noise ratio) values" are acquired for both extracted &stego secret pictures. The outcomes are compared with outcomes of other strategies, whereas single picture will be concealed and it will be discovered that the suggested method is straightforward & provides good values of PSNR than others.

Keywords: MSE, Steganography, RGB, IWT, PSNR, Chrominance, Luminance

1. INTRODUCTION

Majority of the data security will be fundamental for private information exchange. Steganography will be utilized to secure transmission of secret data. It holds 2 primary divisions: steganography & digital watermarking. The previous will be basically utilized for copyright security of electronic items. Evading correspondence through famous channels incredibly lessens hazard of data continuously spilled in transit. The concealing data in a photo of agency picnic will be less suspicious than collaborating an encrypted record.

In this manuscript the color picture will be taken as cover & 2 gray scale pictures would acknowledge as secret data. The secret pictures & stego keys would installed in cover picture to become stego picture. The significant goal of steganography will be to prevent few unplanned viewer from damaging secret data. There are few elements to be deliberated when outlining a steganography framework [1]. Invisibility: The invisibility will be capability to be undetected by people
Security: Even whether attacker understands the data presence in stego object it must be in tolerable for attacker to notice the data. It will be calculated in terms of PSNR.

$$PSNR = 10\log\left(\frac{L^2}{\sqrt{MSE}}\right) dB \qquad (1)$$

Where MSE =Mean Square Error and L = maximum value

$$MSE = \frac{1}{N}\sum_{i=1}^{N}\left|X_i - X_i^{|}\right|^2 \qquad (2)$$

Where N = number of samples, X = original value, and $X^{|}$ = stego value".

High value of PSNR shows high safety due to it displays minimum variance among stego& real values. So no one might suspect concealed data.

- Capacity: The number of data, which might be conceal relative to cover object size without declining cover object quality.
- Robustness: It will be capability of stego to withstand operations like filtering, cropping, rotation, compression and so on.

The outline of steganographic framework might be sorted under "spatial domain strategies & transform domain strategies" [1]. In "spatial domain methods", the procedure will be connected on pixel values of picture specifically. The merit of these systems will be effortlessness. The drawback is low capability to tolerate signal processing operations. The "Pallet based methods, Least Significant Bit Insertion methods" come under this group. In "transform domain methods", the 1st stage is to change cover picture into separate domain. Then changed factors are managed to conceal the secret data. The transformed factors are converted back into "spatial domain to get stego picture". The merit of transform domain strategies will be high capability to face "signal processing operations". Nevertheless, these type strategies are computationally difficult. Steganography strategies utilizing "DCT (Discrete Cosine Transforms), DWT (Discrete Wavelet Transforms), IWT, DFT fallen under this class.

In this manuscript, secret pictures are embedded utilizing IWT. The wavelet transform gives a time-frequency demonstration of signal. The IWT will be a more productive methodology to lossless compression. The finite precision numbers are used to represent the coefficients in this transform that permits for lossless encoding. In the event of "discrete wavelet transform", whether input comprises of integers, then output never again comprises of integers. Consequently the real picture faultless rebuilding turns into critical. Though, with the Wavelet transforms introduction, which map integers to integers the yield could be totally categorized with the integers. The "LL sub-band"[2] in instance of IWT shows to be a close duplicate with minor scale of real picture same time in instance of DWT coming about "LL sub-band" may be bended slightly, as demonstrated in figure 1.

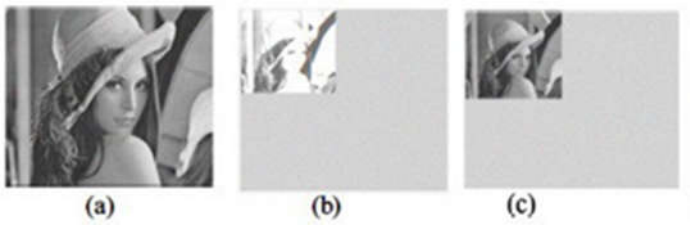


Figure 1. (a) Original image Lena. (b) One level DWT in sub band LL (c) One level IWT in sub-band LL.

Whether the real picture (I)will be"X pixels high and Y pixels wide", the level of each pixel at(i,j)is denoted by$I_{i,j}$.[3]

The IWT factors are given by

$$LL_{i,j} = \lfloor (I_{2i,2j} + I_{2i+1,\ 2j})/2 \rfloor \quad (1)$$

$$HL_{i,j} = I_{2i+1,\ 2j} - I_{2i,2j} \quad (2)$$

$$LH_{i,j} = I_{2i,\ 2j+1} - I_{2i,2j} \quad (3)$$

$$HH_{i,j} = I_{2i+1,\ 2j+1} - I_{2i,\ 2j} \quad (4)$$

The inverse transform is specified by

$$I_{2i,2j} = LL_{i,j} - \lfloor HL_{i,j}/2 \rfloor \quad (5)$$

$$I_{2i,2j+1}=LL_{i,j}+\lfloor(HL_{i,j+1})/2\rfloor \quad (6)$$

$$I_{2i+1,\,2j} = I_{2i,\,2j\,+1} + LH_{i,j}\text{-}HL_{i,j} \quad (7)$$

$$I_{2i+1,\,2j+1} = I_{2i+1,2j} + HH_{i,j}\text{-}LH_{i,j} \quad (8)$$

Where $1 \le i \le X/2$, $1 \le j \le Y/2$ and $\lfloor\ \rfloor$ denotes floor value.

II. Proposed Method

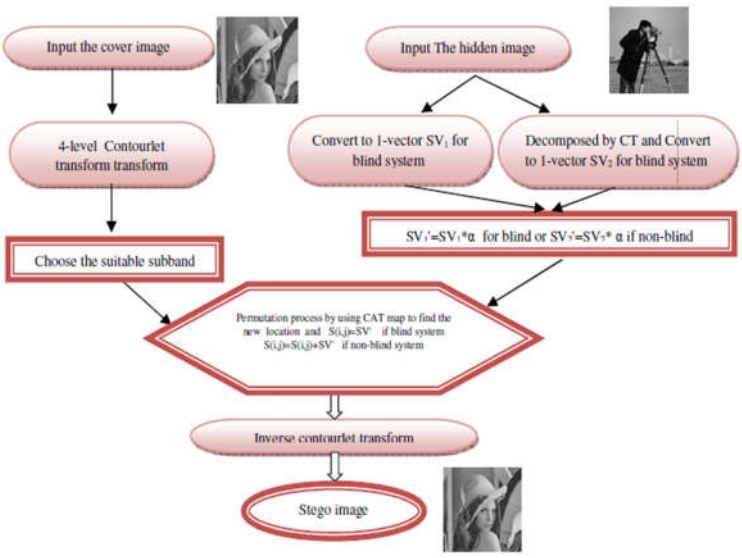
In the suggested technique, the cover will be"256x256 color image, 2 grey scale images of size 128 x128" are utilized as secret pictures. In this method, subsequent stages are executed for encoding:

- Signify cover picture C in color space of YCbCr
- Attain single level IWT of secret-imagesS1,S2 and Cb, Cr component of C.
- Thesubsequenttransformedmatrixcontainsof4sub-bandsequivalentto"LL, LH, HL and HH sub bands".
- The LL sub band of Cb is utilized to conceal one secret picture & LL sub band of Cr will be utilized to conceal another secret picture. Then the 2 keys K1 and K2 consistent to 2 secret pictures are gained utilizing the similar process utilized in past work [16] as defined in sec 2.
- The 2 keys are then encrypted utilizing simple exclusive or operation with a key and run length encoded & then hidden in the cover picture utilizing IWT as follows:

Discover the integer wave let transform of Cb component of cover picture. Exchange the "least significant bit planes of the higher frequency components" of transformed picture by bits of keyK1. Attain inverse IWT of subsequent picture to become stego Cb component. Likewise hide K2 in Cr component. Signify the subsequent picture in RGB color space to attain stego picture G.
Secret pictures might be extracted from Cb& Cr components of the stego picture as follows:

Signify the stego picture G in YCbCr color space". Let it be GyGcbGcr Attain IWT of Gc band Gcr" &a ttain the K1 & K2 keys. Then secret pictures are attained with support of K1 & K2 following the similar steps mentioned before for our past work [12] in section2.

Figure.1. Block diagram of Hidden image in image



The algorithm is tested in MATLAB. The "wavelet tool box" is utilized. The lifting wave *cdf 2.2* is utilized to discover the "integer wavelet transform". The outcomes with diverse secret pictures & cover pictures are shown. Figure 3 represents the Real secret & cover pictures. Two cover images "baboon" and "peppers" (Figure 3(a) and 3(b)), each of size 256X256, are considered for testing the algorithm. The secret pictures considered are "earth, football and moon" (Figure 3(c), 3(d), and 3(e)),eachofsize128X128.The"footballandearth"areembeddedin"peppers".Figure 4(a) displays the resultant stego picture. The "earth and moon" are embedded in "baboon". Figure 4(b) displays the resultant stego picture. Extracted secret pictures from "peppers" are represented in Figure 4(c) & 4(d). Extracted secret pictures from "baboon" are represented inFigure4 (e)&4(f).In all instances, the average PSNR value of stego pictures will be44.7dB.ThePSNR values of the extracted secret images are also nearly 44.7 dB. The PSNR values in dB in all cases for stego & extracted secret pictures are shown in Table 1, 2.Table 3 compares the PSNR value of the stego picture in recommended technique and that in other 4 methods. In all these cover image considered is "peppers" and secret images utilized are of comparable sizes. The average PSNR value in the suggested technique will be much higher than that in other approaches.

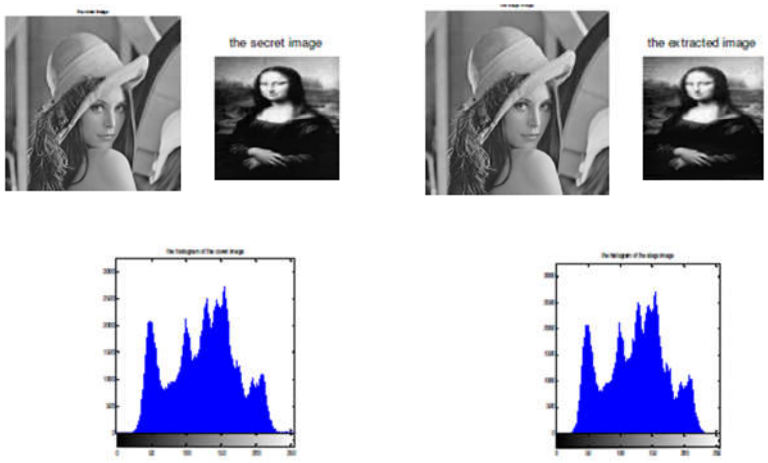


Figure.2. Histogram results

Table 1. PSNR (in dB) of the stego picture

COVER IMAGE (256x256)	SECRET IMAGES (128x128)	PSNR
baboon	earth and moon	44.8
peppers	football and earth	44.7

Table 2. PSNR (in dB) of the extracted secret picture

COVER IMAGE (256x256)	SECRET IMAGES (128x128)		
	football	earth	moon
baboon		44.8	44.8
peppers	44.6	44.7	

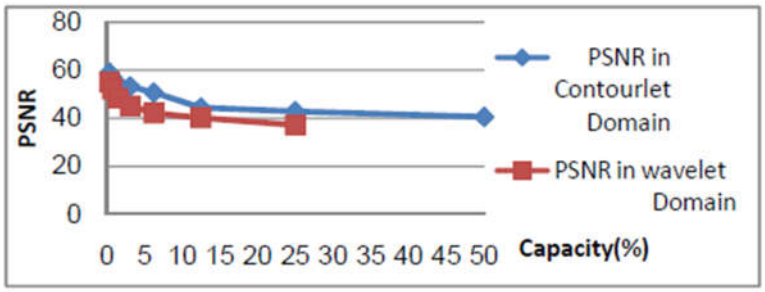


Figure.3. Cpmarision between wavelet based stego

Conclusion

In this manuscript, we watch that 2 secret pictures might be concealed in one color picture & they might be redeveloped without really storing the picture. This method outcome in high quality of stego picture having high values of PSNR contrasted with different systems. Though, the drawback of the method will be that it is vulnerable to noise whether spatial domain strategies are utilized to hide the key. The method will be extremely basic and level of security might be expanded by utilizing "standard encryption strategies" to encrypt the keys.

REFERENCES

[1] Katzenbeisser, S. and Petitcolas, F.A.P., (2000) Information Hiding Techniques for Steganography and Digital Watermarking. Artech House, Inc., Boston,London.

[2] M.F.Tolba, M.A.Ghonemy, I.A.Taha,A.S.Khalifa,(2004)"UsingIntegerWaveletTransformsin Colored Image-Stegnography", International Journal on Intelligent Cooperative Information Systems, Volume 4, pp.75-85.

[3] GuorongXuanet. al, (2002) "Distortionless Data Hiding Based on Integer Wavelet Transform", Electronics Lelters, Vol. 38, No. 25, pp.1646-1648.

[4] Shejul, A. A., Kulkarni, U.L., (2011) "A Secure Skin Tone based Steganography (SSTS) using WaveletTransform",InternationalJournalofComputerTheoryandEngineering,Vol.3,No.1,pp.16- 22.

[5] Masud, Karim S.M., Rahman, M.S., Hossain, M.I., (2011) "A New Approach for LSB Based Image Steganography using Secret Key.", Proceedings of 14th International Conference on Computer and Information Technology, IEEE Conference Publications, pp 286 –291.

[6] Xie,Qing.,Xie,Jianquan.,Xiao,Yunhua.,(2010)"AHighCapacityInformationHidingAlgorithmin Color Image.", Proceedings of 2nd International Conference on E-Business and Information System Security, IEEE Conference Publications, pp1-4.

[7] Sachdeva, S and Kumar, A., (2012) "Colour Image Steganography Based on Modified Quantization Table.",ProceedingsofSecondInternationalConferenceonAdvancedComputing&Communication Technologies , IEEE Conference Publications, pp 309 –313.

[8] Chen, R. J., Peng, Y. C., Lin, J. J., Lai, J. L., Horng, S. J. Novel Multi-bit Bitwise Adaptive Embedding Algorithms with Minimum Error for Data Hiding. In Proceedings of 2010 Fourth International Conference on Network and System Security (NSS 2010), (Melbourne, Australia, 1-3 September 2010), IEEE Conference Publications, 306 –311.

[9] Roy, S., Parekh, R., (2011) "A Secure Keyless Image Steganography Approach for Lossless RGB Images.", Proceedings of International Conference on Communication, Computing & Security, ACM Publications,573-576.

[10] Mandal, J.K., Sengupta, M., (2011) "Steganographic Technique Based on Minimum Deviation of Fidelity (STMDF).", Proceedings of Second International Conference on Emerging Applications of Information Technology, IEEE Conference Publications, pp 298 –301.

[11] Mandal, J.K., Sengupta, M., (2010) "Authentication/Secret Message Transformation Through Wavelet Transform based Subband Image Coding (WTSIC).", Proceedings of International Symposium on Electronic System Design, IEEE Conference Publications, pp 225 –229.

[12] Sarreshtedari, S., Ghaemmaghami, S. High Capacity Image Steganography in Wavelet Domain. In Proceedingsof20107thIEEEConsumerCommunicationsandNetworkingConference(CCNC)(Las Vegas, Nevada, USA, 9 – 12 January 2010), IEEE Conference Publications,1-5