A Novel Image Hiding Algorithm using Optimal Band Selection

Ali Baig Mohammad, Tummala Ranga Babu

***Abstract:** In the present era of transmission of data over internet requires a very high level of security. In order to transmit personal data or confidential data over internet, data privacy and secrecy are very crucial. Different security measures like cryptography and steganography are developed for provisioning security in many applications.In the process of enhancing image security, images are transformed to a format, which cannot be determined by an intermediate user, and can be retrieved back by the authorized user only.Though different approaches were defined, the need of provisioning security still observe various limitations to reach to the demands of evolving generation services and resource utilization. In this paper, a novel approach of embedding secret information in a cover image using optimal band selection is proposed. Instead of embedding the secret image in LL band, an optimal band is selected based on minimum energy constraint and is used as a room for hiding secret image in it. The proposed algorithm is applied on several images and a very less distorted cover image is obtained.The results of these experiments show better performance metrics like PSNR, MSE and NCC when compared to conventional LL band coding.*

***Index Terms**: Discrete Wavelet Transform, Image Cryptography, MSE, NCC, PSNR*

I. INTRODUCTION

In today's era, we transmit our personal images to our friends or dear ones over internet. In some cases, we may need to transmit the most confidential information over internet. In all such cases, the crucial information to be transmitted is vulnerable to several attacks by hackers. Therefore, it is very much essential to develop approaches that ensure a very high level of security to achieve attack resilience in the transmission of crucial information.

Several approaches like cryptography and steganography are proposed and being implemented. In the process of image security, images are transformed to a format, undetermined by an intermediate user, and can be retrieved back by the authorized user only.In cryptography, the information to be transmitted is converted to a format that is not understandable. In steganography, the secret information is concealed in a cover image and transmitted. Several other approaches like visual cryptography and reversible data hiding are also proposed and being implemented. Though different approaches were developed, the need of provisioning security still observe various limitations. Towards providing the security coding, in recent method, a reversible datahiding approach is suggested in [1]. Thisapproachdevelops a cryptography approach based on dataencryption using visual cryptography approach.To achieve attack resilience, bit rotation is suggested.In this approach, the authentication is developed basedon color plane coding and a key-lesscoding wassuggested, this method, however, the basicobservations of image pixelcorrelation and itsdistribution was not observed.The embedding, thoughresults in effective security coding, the coding withoutconsidering the pixel correlation and energy variationeffects the overall cryptography application.In [2] for considering an efficient embedding, binary coding was suggested. Binary level coding, where least significant bits (LSB) based coding was suggested for information hiding and security provisioning. However, in this approach as well the pixel distribution over the image is not considered. The secret image is embedded in all other components of second level Discrete Wavelet Transform except its LL component. The spectral domain gives the process of time/frequency domain coding. In spectral domain wavelet transforms are used for transformation, and almost in all past literature, LL band is selected for security coding, considering a lower information density in this band as it is derived from a set of low pass filters. However, it is observed that, all the residual information is concentrated on this band, which could be further filtered to given more finer details. Secondly, in many images, among the 3 details bands (LH, HL, HH), there would be less density in some band.An advanced technique for encrypting datausing Advanced Encryption System (AES) and hiding the data is proposed in [3]. Here cipher text is hidden at most two Least Significant Bits (LSB) positions in theless detailed regions of the carrier imageusing Haar Discreet Wavelet Transform (HDWT). The secret data is embedded in HH band of the cover image. An improved LSB information hidingalgorithm of color image using secret key is proposed in [4],combining information hiding and cryptography, increasing thehuman eye visual features, and the identity authentication basedon digital signature and encryption technology to improve thesecurity of information hiding.A new secure secret sharing based visual cryptography scheme has been proposed in [5]. This method converts secret image into number of shares as per the user needs. This process helps in increasing image security. A random selection of embedding band improves therobustness as well increase the accuracy. In the approach for provisioning of image security, the primal requirements are the image quality, transmission or storage resources and computational overhead for security provision.

Manuscript published on 30 March 2019.
***Correspondence Author(s)**

Ali Baig Mohammad, Research Scholar, ECE Dept., ANU College of Engg. & Tech., ANU, Assistant Professor, ECE Dept., Koneru Lakshmaiah Education Foudation,Vaddeswaram, AP, India,
Prof. Tummala. Ranga Babu, Professor & Head, ECE Dept., R.V.R & J.C College of Engineering, Guntur, Andhra Pradesh, India,

II. PROPOSED WORK

The experimental work is performed in two steps. In the first step, we implement conventional method where a host image is decomposed into four bands (LL, LH, HL, HH) using DWT. The secret data is embedded into the LL band of the host image considering it to be least informative as it is derived from Low Pass-Low Pass filtration. After embedding operation, image inverse coding is applied using IDWT and the secret data is recovered and various performance metrics like PSNR, MSE and NCC are computed to assess the performance of this conventional method. However, in practical scenario various image samples will have low varying elements and it may be dominative in particular direction. On selecting only, the LL band blindly for any image for security provisioning, pose the issue of data accuracy and security robustness.If always LL band is used attacker can easily detect the data, as the embedding is always in LL band attacker will directly focus on LL band to retrieve the information.In various images one detail information would be dominating with other having less impact, and LL band are observed to be a residual component, image with low varying components will have more information in such case. Hence it would not be optimal to always need LL band for coding. Here taking this limitation under consideration, we implement the second step called proposed method. In this proposed method, host image is decomposed into four sub-bands (LL, LH, HL, HH) using DWT. An optimal band selection for secret data embedding is done using minimum energy condition as shown below:

Consider the Host Image (H_I) and Embedding Image (E_I) to be encoded for transmission as shown below figure 1 below:

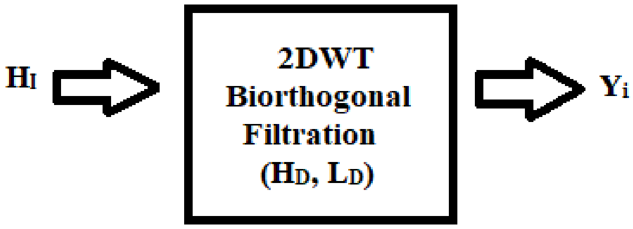

Fig. 1

The decomposed band for each resolution is obtained using the equation (1) shown below:

$$Y_i = (H_i \otimes H_D) \otimes x\, L_D \qquad (1)$$

where H_D and L_D are decomposing filter coefficients and Y_i is the decomposed band for each resolution. After obtaining the four spectral bands, the spectral energy of each band is computed using the equation (2) shown below:

$$E_i = \left|Y_i\right|^2 \quad (2)$$

Then selection of optimal band for embedding is carried out by minimal constraint shown in equation (3) below:

$$S_B = \min(E_i) \qquad (3)$$

where SB is the selected band. The secret image E_I is embedded into the selected band of the host image using the equation (4) shown below:

$$E_{si} = E_I \text{ x } (1 + \alpha E_i) \qquad (4)$$

where α is embedding weight factor. The modified data is applied for reconstruction as the updated band as shown in the equation (5) shown below:

$$\hat{Y}_i = E_{si} \qquad (5)$$

here $\hat{Y}_i$ is the updated band for inverse coding. The recovered image Ri is represented as

$$R_i = (\hat{Y}_i \otimes H_R) \otimes x\, L_R \qquad (6)$$

The objective of minimizing the processing error due to encoding of two images is minimized by processing on the lowest energy band. The performance is derived by measuring MSE, PSNR and NCC for the recovered image.

The steps of the proposed algorithm are summarized as shown below:

1. The host image and secret image are preprocessed where they are converted to gray scale and resized to 256 x 256.
2. Spectral decomposition of the preprocessed host image is carried out using DWT and four spectral bands are obtained.
3. Optimal Band Selection based on minimum energy constraint is performed on these spectral bands of host image and the optimal spectral band is chosen as a room for embedding the secret image.
4. The preprocessed secret image is embedded into the optimal selected band of the host image using the embedding equation shown in (4).
5. The embedded image along with the other spectral bands of host image are applied to image inverse coding and the reconstructed cover image is obtained.
6. The performance metrics like MSE, PSNR and NCC are computed for both conventional and proposed method.

III. PERFORMANCE METRICS

A. Mean Squared Error (MSE)

The MSE tellshow much error is introduced due to security coding on the original data. Lower the MSE, higher is the efficiency of the security-coding algorithm.It is computed using the equation (7) shown below:

$$MSE = \frac{\sum_{i=1}^{N}\sum_{j=1}^{N}\left|Y_{ij} - R_{ij}\right|^2}{N \text{ x } N} \quad (7)$$

Here, Yij and Rij are original cover image and reconstructed cover image respectively. NxN is the size of the original cover image.

B. Peak Signal to Noise Ratio (PSNR)

The PSNR is the measuring parameter which tells how much the original (host) data got affected after performing security coding. The PSNR is computed using the equation (8) shown below:

$$\text{PSNR} = 10\log\left(\frac{N^2}{MSE}\right) \tag{8}$$

The higher the PSNR the better is the preservation of the cover image because of embedding.

C. Normalized Cross Correlation (NCC)

The parameter NCC is computed using the equation (9) shown below:

$$\text{NCC} = \frac{\sum_{i=1}^{N}\sum_{j=1}^{N}\left|Y_{ij}-R_{ij}\right|}{\sum_{i=1}^{N}\sum_{j=1}^{N}Y_{ij}} \tag{9}$$

The NCC value goes towards zero if the two images do not haveany difference. The lower the value of NCC the better is the embedding efficiency of the algorithm.

IV. SIMULATION RESULTS

The two methods of image cryptography conventional method and proposed method are implemented on MATLAB using multiple images and the simulation results are obtained as shown below:

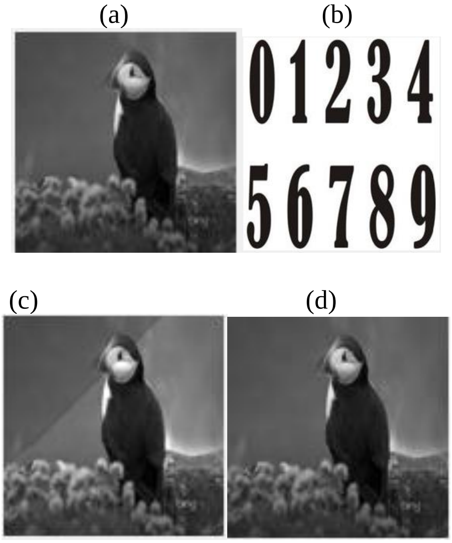

Fig. 2: S1 – (a) Original Host image, (b) Secret Image (c) Reconstructed Host image using conventional method (d) Reconstructed Host image using proposed method

(a) (b)

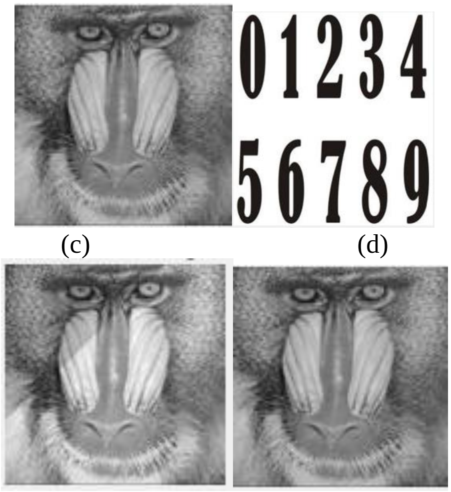

Fig. 3: Baboon – (a) Original Host image, (b) Secret Image(c) Reconstructed Host image using conventional method(d) Reconstructed Host image using proposed method

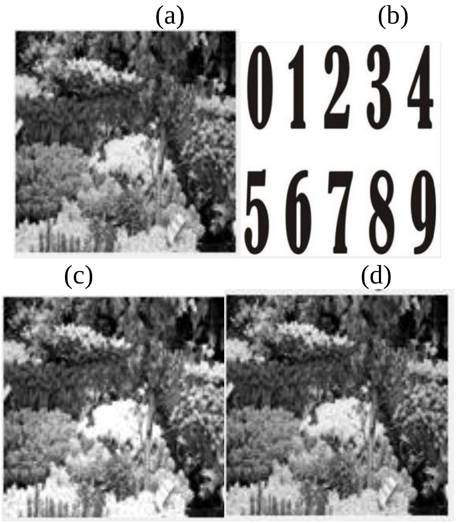

Fig. 4: Flower – (a) Original Host image, (b) Secret Image (c) Reconstructed Host image using conventional method (d) Reconstructed Host image using proposed method

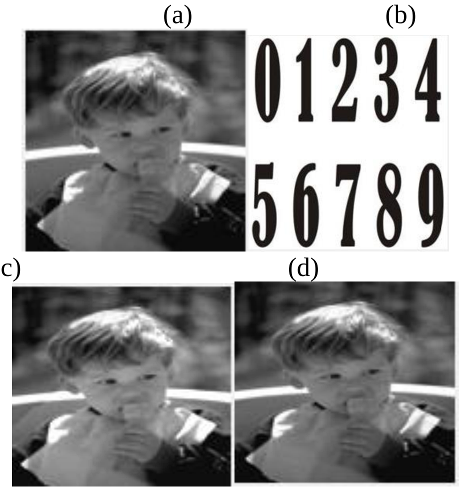

Fig. 5: Kid – (a) Original Host image, (b) Secret Image (c) Reconstructed Host image using conventional method (d) Reconstructed Host image using proposed method

Published By:
Blue Eyes Intelligence Engineering
and Sciences Publication (BEIESP)

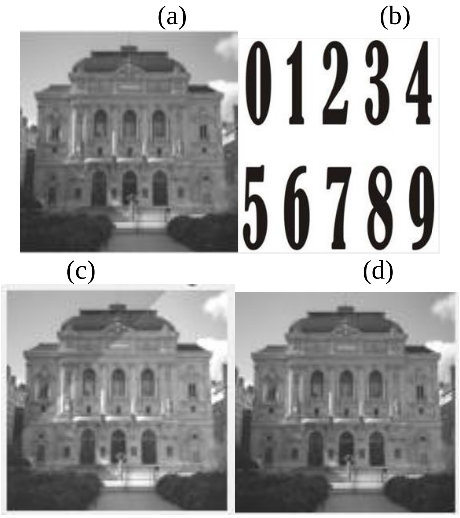

Fig. 6: Opera – (a) Original Host image, (b) Secret Image (c) Reconstructed Host image using conventional method (d) Reconstructed Host image using proposed method

Table I: Spectral energies of various bands

Cover image	LL	LH	HL	HH
S1	1.528 x 10^6	557.7	1612	167.6
Baboon	4.666 x 10^6	8579	7251	2765
Flower	3.286 x 10^6	16680	38520	10150
Kid	1.471 x 10^6	3975	910.1	269.6
Opera	4.345 x 10^6	3829	6237	854.2

Table II: Mean Squared Error (MSE) values

Cover image/Secret image	Conventional method	Proposed method
S1/E3	1.6272 x 10^4	2.2225 x 10^{-20}
Baboon/E3	4.8026 x 10^4	5.82 x 10^{-20}
Flower/E3	3.1105 x 10^4	2.3507 x 10^{-19}
Kid/E3	2.4347 x 10^4	5.3595 x 10^{-20}
Opera/E3	3.5590 x 10^4	3.7342 x 10^{-20}

Table III: Peak Signal to Noise ratio (PSNR) values

Cover image/Secret image	Conventional method	Proposed method
S1/E3	6.0163	244.6624
Baboon/E3	1.3161	240.4816
Flower/E3	3.2025	234.4188
Kid/E3	4.2664	240.8395
Opera/E3	2.6175	242.4089

Table IV: Normalized Cross Correlation (NCC) values

Cover image/Secret image	Conventional method	Proposed method
S1/E3	0.1203	0
Baboon/E3	0.1565	0
Flower/E3	0.1185	0
Kid/E3	0.1457	0
Opera/E3	0.1345	0

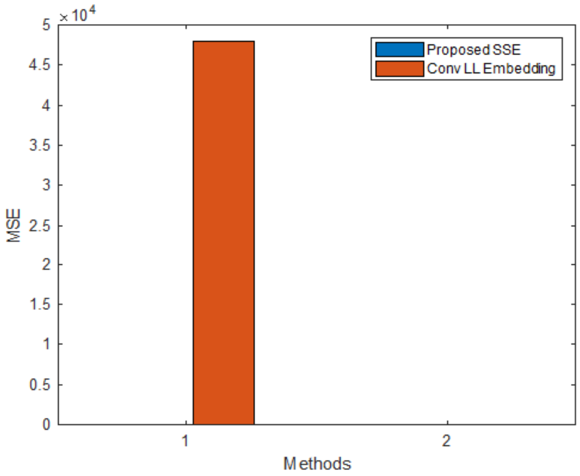

Fig. 7: MSE Plot for Baboon image

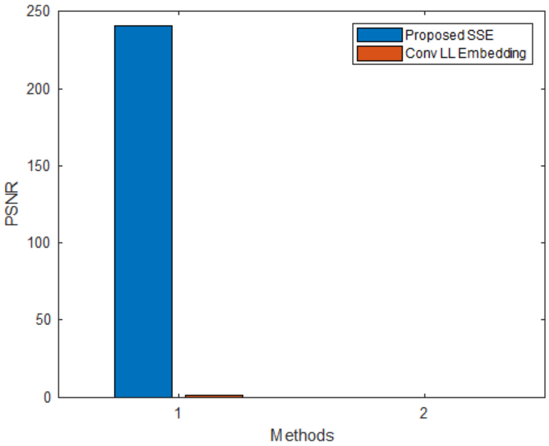

Fig.8: PSNR Plot for Baboon image

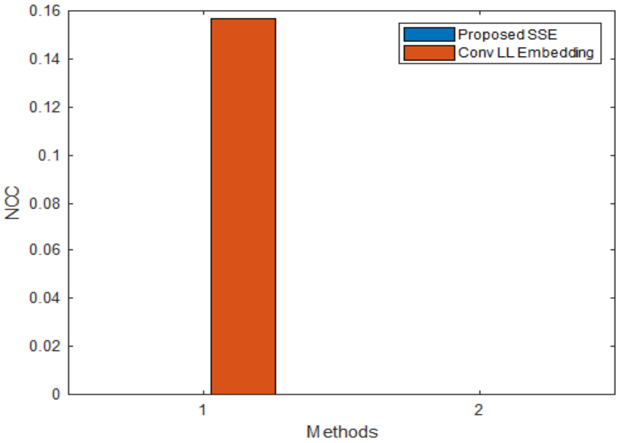

Fig.9: NCC Plot for Baboon image

V. CONCLUSION

It is observed from the experimental results that the proposed method using optimal band selection outperforms the conventional method using LL band for embedding. Therefore, we can conclude that rather than selecting LL band blindly for embedding, we can optimally select the band to preserve the host image which in turn increases the embedding efficiency and security for the cryptographic application.

Published By:
Blue Eyes Intelligence Engineering
and Sciences Publication (BEIESP)
© Copyright: All rights reserved.

REFERENCES

1. Miss. Nuzhat Ansari and Prof. Rahila Shaikh, “A Keyless Approach for RDH in Encrypted Images using Visual Cryptography”,*Procedia Computer Science (2016),* vol. 78, Dec 2015, pp. 125-131. [International Conference on Information Security & Privacy (ICISP2015)]
2. Punam Bedi, Veenu Bhasin and Tarun Yadav, “2L-DWTS – Steganography technique based on second level DWT”, *Intl. Conference on Advances in Computing, Communications and Informatics (ICACCI),* Sept. 21-24, 2016, pp. 1533-1538
3. Essam H. Houssein, Mona A. S. Ali and Aboul Ella Hassanien, “An Image Steganography Algorithm using HaarDiscrete Wavelet Transform with AdvancedEncryption System”, *Proceedings of the Federated Conference on Computer Science and Information Systems,*vol. 8., pp. 641-644, 2016
4. Xinyi Zhou, Wei Gong, WenLong Fu and LianJing Jin, “An Improved Method for LSB Based Color Image Steganography Combined with Cryptography”, *15th International Conference on Computer and Information Science (ICIS),* pp. 1-4, 2016
5. Ankush V. Dahat and Pallavi V. Chavan, “Secret Sharing Based Visual Cryptography SchemeUsing CMY Color Space”, *Procedia Computer Science,* vol.78, pp.- 563 – 570, Dec 2015 [International Conference on Information Security & Privacy (ICISP2015)]]

AUTHORS PROFILE

Ali Baig Mohammadobtained his M.E. in Electronics & Communication Engineering (Systems & Signal Processing) from Osmania University, Hyderabad, B.Tech. from Bapatla Engg. College, Bapatla (affiliated to Acharya Nagarjuna University). He is currently pursuing his Ph.D in Electronics and Communication Engineering at Acharya Nagarjuna University and working as an Assistant Professor in ECE Dept., KLEF deemed to be University. His research interests are Signal processing and Image processing.

Tummala Ranga Babuprocured his Ph.D. in Electronics and Communication Engineering from JNTUH, Hyderabad, M.Tech in ECE (Digital Electronics & Communication Systems) from JNTUA, Anantapuram, M.S.(Electronics & Control Engineering) from BITS, Pilani. He obtained his B.E. (ECE) from University of Madras. He is currently holding the position of Professor& Head of Department of Electronics & Communication Engineering., RVR & JC College of Engineering, Guntur. He is a member in various professional bodies like IEEE, IETE, ISTE, CSI, IACSIT. His research interests include Image Processing, Pattern Recognition, Embedded Systems, Digital Communication.

Published By:
Blue Eyes Intelligence Engineering
and Sciences Publication (BEIESP)