

REVERSIBLE DATA HIDING USING SECURE FORCE ALGORITHM

¹Subash Nemani, ²JayachandraPrasad.Talari, ³Sumalatha.Vangala

¹Research Scholar, Dept of ECE, RGM CET,

JNTUA College of Engineering Ananthapuramu, India

²Dept of ECE, RGM CET, Nandyal, India

³Dept of ECE, JNTUA College of Engineering Ananthapuramu, India

¹nemani.470@gmail.com

Abstract: Steganography is the branch of science which deals with hiding data in cover image with reversibility. Data hiding is an interesting area in digital world. In this paper we present a secured form of reversible data hiding based on Secure Force (SF) Algorithm. SF algorithm consists of three blocks: a) Key generation Block b) Encryption block and c) Decryption block. In the first stage different keys are generated and some mathematical operations are performed such as XOR, XNOR to maintain security and then encryption and decryption are carried out to reduce the size of the cover images. SF based cover images are preferred for data hiding by simple least significant bit substitution. Our simulation results show that the presented SF algorithm performs better in PSNR of 60.25 dB for cover image of boat at a bit rate of 0.05 bpp (bits per pixel) with structural content of 0.9989.

Keywords: Reversible Data Hiding, Encryption, Secure Force Algorithm, Steganography.

1. Introduction

As there is a fast growth in the digital media always providing security and protection to the internet based communication has become a challenging issue. In recent times more attention is drawn for images to attain reversibility called as Reversible Data Hiding (RDH) is the root of steganography. It conceals text, images, audio/video formats into another file of text, image, audio/video formats. For this purpose RDH has become an interesting field of image processing. The different reversible data hiding algorithms are classified as: Spatial domain and Transform domain methods. The most common method in data hiding is least significant bit (LSB) substitution. Researchers further classified spatial domain methods into four groups. Group I as Difference Expansion, group II as Histogram modification and group III and IV as prediction and interpolation Algorithms.

In 2001, Ran-Zan Wang et al [1] implemented data hiding using genetic algorithm (GA) and least significant bit substitution and proved that the

computational time for GA is twice that of LSB substitution. Chin-Chen Chang et al [2] proposed a LSB substitution by dynamic programming strategy which reduces the computational time with optimal embedding. Thien et al [3] presented data hiding using modulus function with improved PSNR of 1.40 dB greater than GA-LSB substitution and high embedding capacity. Chang and Tseng [4] proposed a steganographic method using side match information with two, three and four-sided methods and increased the embedding capacity up to 3,89,004 bits with PSNR 41.22 dB for lena image using two-sided method. Mielikainen [5] made slight modification to LSB matching by choosing a cover pixel using binary function and performs well in distortion and can resist against steganalysis.

Tian [6] proposed data embedding using difference expansion with low distortion and high payload. XiaoTong Wang et al [7] has chosen 2-D vector map for embedding data using DE and performs better in capacity and invisibility. Tseng and Chang [8] extended Tian's method using shiftable pixel pair and improved capacity upto 2, 55,226 bits with PSNR 32.42 dB. Yongjian Hu et al [9] implemented data hiding in DE using two directions i.e; horizontal and vertical with PSNR of 46.03 dB at embedding rate 0.1 bits per pixel (bpp) for lena image. Ni et al. [10] proposed reversible data hiding using histogram minimum and maximum points to embed data up to 80kb with visual quality greater than 48 dB. Chia-Chen Lin et al [11] made modifications to histogram by embedding data in peak points and achieved high capacity of 1,15,963 bits with PSNR 43.02 dB for lena image. Yuan-Yu Tsai et al [12] developed a method for data hiding by making modification to histogram using neighboring pixel differences (NPD) with one pixel value and two pixel values and improved embedding capacity upto 59503 bits with PSNR 50.20 dB for NPD1 and 82842 bits with PSNR 47.12 dB for NPD2.

Tseng and Hsieh [13] implemented embedding method based on prediction error expansion using threshold value. Different predictors were discussed and their performance in terms of PSNR and payload are analyzed. Hong et al [14] implemented embedding

scheme based on modification of prediction errors (MPE) for creating vacant space to embedding data which is five time more than that of Ni et al method with PSNR greater than 48 dB. Chin-Feng Lee et al [15] combined prediction and difference expansion to increase the embedding rate without use of location map. Lixin Luo et al [16] proposed reversible watermarking technique using interpolation and achieved high visual quality of 48.82 dB with embedding capacity of 71,674 bits for Lena image. Hong and Chen [17] implemented interpolation based data hiding using reference pixel distribution mechanism with improved average image quality of 50.48 dB with average payload of 86,068 bits.

In this paper, we present a Secure Force (SF) based data hiding and results show that SF method performs well in payload and average PSNR than the state-of-art methods.

The remaining paper is organized as: Section II explains Ex-or based encryption in related work. Section III presents SF algorithm for data hiding. Simulation results were shown in Section IV and Conclusions are discussed in section V.

2. Related Work

Reversible data hiding has to satisfy the triangle rule which is payload, imperceptibility and security are major parameters to be high for a good RDH method. One of the key parameter for RDH is maintaining security which can be attained using Encryption [18-19]. It is the process of converting the image into indecipherable form which protects from malicious attacks.

Let the input image is considered as $I(i,j)$ with each pixels having its gray values $[0, 255]$ to denoted 8 bits. The bits of the pixel are denoted as: $a_{i,j,0}, a_{i,j,1}, a_{i,j,2}, \dots, a_{i,j,7}$ Such that

$$a_{i,j}(k) = \left\lfloor \frac{a_{i,j}}{2^k} \right\rfloor \bmod 2, k = 0, 1, 2, \dots, 7 \quad (1)$$

Now the encryption can be obtained for the bits of the image using Exclusive-OR operation

$$E_{i,j}(k) = a_{i,j}(k) \oplus b_{i,j}(k) \quad (2)$$

Where $b_{i,j}(k)$ are random bits generated by stream cipher using encryption key.

3. Secure Force Algorithm

In modern era, providing security for digital media has become a challenging task. Steganography is one such area where data can be embedded into the digital media with reversibility. Present steganography methods provide security by encrypting the image and then hiding data into it and decrypt the image. The problem with EX-or operation used for encryption by Zhang is,

as there is only one encryption key used by hider so there is chance of detection of the hidden data by attackers. To overcome this problem we present in this paper a Secure Force algorithm which uses multiple keys for encryption such that it is free from malicious attacks. The secure force algorithm consists of three blocks: a) Key expansion block b) Encryption block and c) Decryption block.

A. Key expansion Block

In this step we generate five different keys and perform different logical and mathematical operations, Permutation and transposition for all the keys.

B. Encryption Block

Based on the keys generated by expansion block the encryption process begins. The following are the steps for encryption.

- Consider an input image of size 512 X 512. Take an 8X8 block of sub image.
- Arrange 64 pixels elements into each of 16 pixel blocks.
- Perform xnor operation for first 16 pixel bits with key k1 and apply swapping technique.
- Perform xnor operation for last 16 pixel bits with key k1 and apply swapping technique.
- Repeat steps iii and iv for different keys till all the keys are completed.

The block diagram for encryption is as shown in Fig. 1.

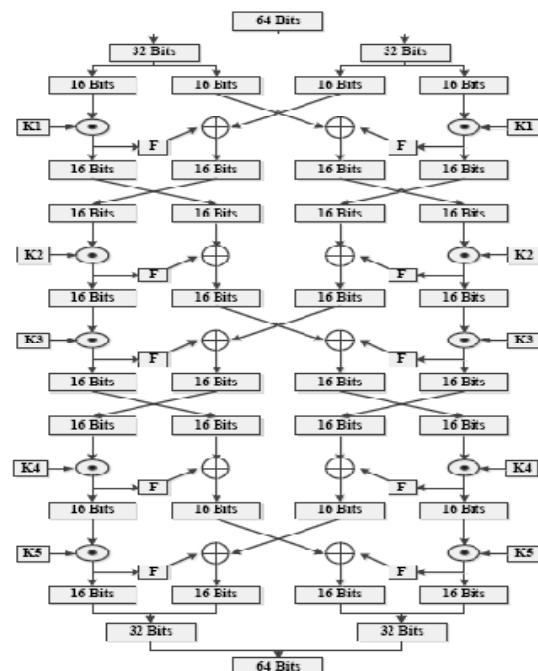


Figure 1. 64 bit encryption representation

C. Decryption

The reverse process for the above encryption block.

i) Data Hiding Algorithm

After the encryption was done by using SF algorithm the data hider starts embedding secret bits as follows:

Step1: Read the image E of size $m \times n$

Step2: The image E is Segmented into $k \times k$ size of smaller blocks as

$$(i-1).k+1 \leq m \leq i.k$$

$$(j-1).k+1 \leq n \leq j.k$$

Where i and j are positive integers.

Step 3: Divide k^2 pixels of each block as k_0 and k_1 randomly using hiding key.

Step 4: change pixels in k_0 by three positions if binary 0 is to be inserted.

$$I'_1 = \overline{I_{m,n,q}}, \quad (m,n) \in k_0 \text{ and } q=0, 1, 2$$

Step 5: change pixels in k_1 by three positions if binary 1 is to be inserted.

$$I'_1 = \overline{I_{m,n,q}}, \quad (m,n) \in k_1 \text{ and } q=0, 1, 2.$$

The rest of the encrypted bits remain unchanged.

ii) Extraction Algorithm

Once the hiding secret data is finished, the steps for extraction are:

Step 1: perform Exclusive-OR operation between decrypted image D and random sequence generator r .

Step 2: If the inserted bit is 0 and belongs to pixel k_0 , then the

3 LSB positions are decrypted as:

$$I = r \oplus D = r \oplus \overline{I_{m,n,q}} = r \oplus \overline{I \oplus r} = \overline{I}$$

Step 3: If the inserted bit is 1 and belongs to pixel k_1 , then the

bits are decrypted as in step 2.

Step 4: Perform step 2 and 3 till all the bits are extracted.

4. Simulation Results

The simulation results are shown for 512 X 512 cover images of "Lena", "Airplane", "Barbara", "Baboon", "Boat" and "Peppers" in Fig. 2.



Figure 2. Cover images for simulation

We evaluate two parameters: one is PSNR for image imperceptibility and other is Structural Content for similarity between cover image and stego image. PSNR can be calculated as:

$$PSNR = 20 \log_{10} \left(\frac{255}{MSE} \right) \quad (3)$$

Where

$$MSE = \frac{1}{MXN} \sum_{i=1}^M \sum_{j=1}^N (I(i,j) - I'(i,j))^2 \quad (4)$$

$I(i,j)$ - cover image and $I'(i,j)$ - Stego image

Structural content can be calculated as:

$$SC = \frac{\sum_{i=1}^M \sum_{j=1}^N [I(i,j)]^2}{\sum_{i=1}^M \sum_{j=1}^N [I'(i,j)]^2} \quad (5)$$

PSNR and structural content at different bit rates for DDH-DCT method and SF method are presented in Table 1. From the results we observe that PSNR for Boat is 60.25 dB at 0.05bpp which is greater than other cover images with Structural content of 1.0000.

Structural content is the similarity between cover image and stego image. Human visual system cannot distinguish the similarity if it ranges in between -1 and + 1. From the simulation results we observe that SC for the presented method is in between 0.9955 to 1.0000.

we compare the results with DDH-DCT method. This method use data embedding by encrypting the cover image using Ex-OR operation by single encryption key. To improve the security we presented SF algorithm where we use multiple secret keys for encryption and then hiding data secures from the malicious attacks. From the results we observed that the presented SF method achieved high visual quality with better embedding capacity. For cover image "Lena" we have attained better visual quality of 59.17 dB at bit rate of 0.05 bpp and still maintained PSNR 45.45 dB at 0.5 bpp. SF method out performs well for all the five

test images except for baboon in image quality compared to DDH-DCT method which is to be analyzed in future.

Average PSNR for all the cover images in SF method are greater than 50.07 dB except for baboon it is 42.46 dB at different bit rates, because baboon

contains more complex features. Embedding data in complex based images is a challenging task. In future better methodology for complex based image data hiding should be proposed to overcome the low imperceptibility.

Table 1. PSNR and Structural Content at different bit rates for DDH-DCT and SF method

Cover Image	DDH-DCT method			SF method (presented)		
	PSNR(dB)	Bit rate(bpp)	SC	PSNR(dB)	Bit rate(bpp)	SC
Lena	46.75	0.5	1.000	45.45	0.5	1.0000
	47.75	0.4	1.000	47.94	0.4	1.0000
	48.78	0.3	1.000	49.22	0.3	1.0000
	51.41	0.2	1.000	52.26	0.2	1.000
	53.91	0.1	0.998	55.53	0.1	0.9995
	55.8	0.05	0.997	59.17	0.05	0.9986
Airplane	45.84	0.5	0.9999	46.43	0.5	1.0000
	47.39	0.4	1.000	48.14	0.4	1.000
	48.49	0.3	1.000	49.42	0.3	1.000
	50.95	0.2	0.994	52.52	0.2	0.9996
	53.63	0.1	1.000	56.34	0.1	1.0000
	55.53	0.05	1.000	59.06	0.05	1.0000
Barbara	37.24	0.5	0.9961	42.98	0.5	0.9987
	39.59	0.4	0.9997	45.55	0.4	0.9985
	42.48	0.3	0.9997	48.23	0.3	1.0000
	45.32	0.2	0.9992	51.3	0.2	0.9996
	49.86	0.1	1.0000	54.34	0.1	1.0000
	52.81	0.05	0.9993	58.04	0.05	0.9999
Baboon	37.29	0.5	0.996	33.54	0.5	0.9958
	39.75	0.4	0.9971	36.38	0.4	0.9955
	42.44	0.3	0.9979	39.95	0.3	0.9977
	45.58	0.2	1.000	44.29	0.2	0.9972
	50.05	0.1	0.9998	49.28	0.1	0.9972
	53.24	0.05	0.9996	51.33	0.05	0.9967
Boat	44.43	0.5	0.9985	45.11	0.5	0.9999
	46.29	0.4	1.0000	47.57	0.4	1.0000
	47.93	0.3	1.000	49.18	0.3	1.0000
	50.42	0.2	0.9956	52.13	0.2	0.9994
	52.87	0.1	1.0000	56.6	0.1	1.0000
	55.07	0.05	0.9976	60.25	0.05	0.9989
Peppers	41.44	0.5	0.9946	44.83	0.5	0.9977
	43.98	0.4	0.9951	47.23	0.4	0.9964
	46.18	0.3	0.9992	48.78	0.3	0.9997
	49.39	0.2	1.0000	51.77	0.2	1.0000
	52.01	0.1	1.0000	54.89	0.1	1.0000
	54.39	0.05	0.9983	58.19	0.05	0.9996

6. Conclusion

In this paper, a Secure Force method for data hiding was presented. At first we design the SF algorithm with Key generation, encryption and decryption blocks. Drawback in the existing encryption methods is they use EX-or Operation using single key encryption which may lead to malicious attacks. In order to improve the security we have presented a SF method using multiple keys for encryption and decryption with reduce in size of the cover image. The presented SF method outperforms well in terms of PSNR and also maintains good structural content. The results show that for the cover image Boat the maximum PSNR of 60.25 dB is attained at 0.05 bpp with structural content of 0.9989.

References

- [1] R.Z. Wang, C.F. Lin, and J.C. Lin, "Image hiding by optimal LSB substitution and genetic algorithm", *Pattern recognition*, Vol. 34, pp. 671-683, 2001.
- [2] C.C. Changa, J.Y. Hsiao and C.S. Chana, "Finding optimal least-significant-bit substitution in image hiding by dynamic programming strategy", *Pattern recognition*, Vol. 36, pp. 1583 – 1595, 2003.
- [3] C.C. Thien and J.C. Lin, "A simple and high-hiding capacity method for hiding digit-by-digit data in images based on modulus function", *Pattern recognition*, Vol. 36, pp. 2875 – 2881, 2003.
- [4] C.C. Chang and H.W. Tseng, "A steganographic method for digital images using side match", *Pattern recognition Letters*, Vol. 25, pp. 1431–1437, 2004.
- [5] J. Mielikainen, "LSB matching revisited", *IEEE signal processing letters*, Vol. 13, pp. 285-287, 2006.
- [6] J.Tian, "Reversible Data Embedding Using a Difference Expansion", *IEEE Transactions on Circuits and Systems for Video Technology*, Vol. 13, pp. 890-896, AUGUST 2003.
- [7] X.T. Wang, C.Y. Shao, X.G. Xu, and X.M. Niu, "Reversible Data-Hiding Scheme for 2-D Vector Maps Based on Difference Expansion", *IEEE Transactions on Information Forensics and security*, Vol. 2, pp. 311-320, SEPTEMBER 2007.
- [8] H.W.Tseng and C.C.Chang, "An extended difference expansion algorithm for reversible watermarking", *Image and Vision Computing*, Vol. 26, pp. 1148–1153, 2008.
- [9] Y. Hu, H.K. Lee, K.Chen, and J. Li, "Difference Expansion Based Reversible Data Hiding Using Two Embedding Directions", *IEEE Transactions on Multimedia*, Vol. 10, pp. 1500-1512, DECEMBER 2008.
- [10] Z. Ni, Y.Q. Shi, N. Ansari and W.Su, "Reversible Data Hiding", *IEEE Transactions. Circuits and Systems for Video Technology*, Vol. 16, pp. 354-362, March 2006.
- [11] C.C. Lina, W.L.Taib, C.C.Chang, "Multilevel reversible data hiding based on histogram modification of difference images", *Pattern Recognition*, Vol. 41, pp. 3582 – 3591, 2008.
- [12] Y.Y.Tsai, D.S.Tsai and C.L.Liu, "Reversible data hiding scheme based on neighboring pixel differences", *Digital Signal Processing*, Vol. 23, pp. 919-927, 2013.
- [13] H.W.Tseng and C.P.Hsieh, "Prediction-based reversible data hiding", *Information Sciences*, Vol. 179, pp. 2460–2469, 2009.
- [14] W. Hong, T.S. Chen and C.W.Shui, "Reversible data hiding for high quality images using modification of prediction errors", *The Journal of Systems and Software*, 2009.
- [15] C.F.Lee, H.L.Chen and H.K.Tso, "Embedding capacity raising in reversible data hiding based on prediction of difference expansion", *The Journal of Systems and Software*, Vol. 83, pp. 1864–1872, 2010.
- [16] L. Luo, Z.Chen, M.Chen, X.Zeng, and Z. Xiong, "Reversible Image Watermarking Using Interpolation Technique", *IEEE Transactions on Information Forensics and Security*, Vol. 5, pp. 187-193, MARCH 2010.
- [17] W.Hong and T.S.Chen, "Reversible data embedding for high quality images using interpolation and reference pixel distribution mechanism", *J. Vis. Commun. Image R*, Vol. 22, pp. 131-140, 2011.
- [18] S .Nemani, J. P. Talari and S. Vangala, "Distortionless Data Hiding for Encrypted Images: A DCT Approach", *Journal of Engineering Science and Technology Review*, Vol. 10, pp. 61-67, 2017.
- [19] X. Zhang, "Reversible Data Hiding in Encrypted Image", *IEEE Signal Processing Letters*, Vol. 18, pp. 255-258, APRIL 2011.
- [20] S.V.Manikanthan and D.Sugandhi "Interference Alignment Techniques For MIMO Multicell Based On Relay Interference Broadcast Channel" *International*

Journal of Emerging Technology in Computer Science & Electronics (IJETCSE) ISSN: 0976-1353 Volume- 7 ,Issue 1 –MARCH 2014.

[21] T.Padmapriya, Ms. N. Dhivya, Ms U. Udhayamathi, "Minimizing Communication Cost In Wireless Sensor Networks To Avoid Packet Retransmission", International Innovative Research Journal of Engineering and Technology, Vol. 2, Special Issue, pp. 38-42.

[22] K. Ramash Kumar, D.Kalyankumar, DR.V.Kirbakaran" An Hybrid Multi level Inverter Based DSTATCOM Control, Majlesi Journal of Electrical Engineering, Vol. 5. No. 2, pp. 17-22, June 2011, ISSN: 0000-0388.

[23] A Murali, K Hari Kishore, D Venkat Reddy "Integrating FPGAs with Trigger Circuitry Core System Insertions for Observability in Debugging Process" Journal of Engineering and Applied Sciences, ISSN No: 1816-949X, Vol No.11, Issue No.12, page: 2643-2650, December 2016.

